Note di algebra

Work in progress

Martino Garonzi

Versione 3.1 del 09/02/2010

“If I can still be standing on my feet then life isn’t so bad.” (Sylvester Stallone)

Indice

CAPITOLO 1

Gruppi

1. Generalità

DEFINIZIONE 1 (Semigruppi, monoidi, gruppi). *Un **semigruppo** è una coppia $(S, *)$ dove S è un insieme (detto "supporto" del semigruppo) e*

$$* : S \times S \to S, \qquad (s, t) \mapsto s * t$$

*è una funzione detta "operazione binaria interna", che sia associativa, cioè tale che $s * (t * r) = (s * t) * r$ per ogni $s, t, r \in S$. Un **monoide** è un semigruppo $(S, *)$ che possegga un elemento neutro per $*$, ovvero un elemento $e \in S$ tale che $s * e = e * s = s$ per ogni $s \in S$. Un **gruppo** è un monoide $(S, *)$ tale che per ogni $s \in S$ esiste $t \in S$ tale che $s * t = t * s = e$; un tale t si denota con s^{-1} e si dice inverso di s. Un semigruppo (risp. monoide, gruppo) S si dice **commutativo** o **abeliano** se per ogni $s, t \in S$ si ha $s * t = t * s$.*

Notazione: Un semigruppo/monoide/gruppo viene denotato con $(S, *)$ dove $*$ è l'operazione. Per alleggerire la notazione, se l'operazione è dichiarata altrimenti o sottintesa, un semigruppo/monoide/gruppo $(S, *)$ viene denotato semplicemente dal suo supporto S. A meno di dover distinguere diverse operazioni o di avere altre esigenze notazionali, l'operazione in un gruppo non verrà indicata con simboli, cosicché $x * y$ verrà piuttosto indicato con xy. In virtù della proprietà associativa, un prodotto del tipo $(xy)z = x(yz)$ verrà indicato con xyz. Riferendoci ai gruppi, piuttosto che parlare di cardinalità parleremo di "ordine".

Esempio: $(\mathbb{N} - \{0\}, +)$ è un semigruppo (commutativo) ma non un monoide.

Esempio: $(\mathbb{N}, +)$ è un monoide (commutativo) ma non un gruppo.

Esempio: $(\mathbb{Z}, +)$ è un gruppo (commutativo). L'inverso di $n \in \mathbb{Z}$ è $-n$.

Osservazione: in un monoide l'elemento neutro è unico: se e, e' sono due elementi neutri allora $e = e * e' = e'$ per definizione.

Unicità dell'inverso: in un gruppo l'inverso di un elemento è unico: se t e r sono due inversi di s allora da $rs = sr = st = ts = e$ segue $r = r(st) = (rs)t = t$. L'inverso di s si denoterà s^{-1}. Possiamo usare lo stesso argomento per dimostrare che $(s^{-1})^{-1} = s$.

Cancellatività: se in un gruppo G si ha $xy = xz$ o $yx = zx$ allora $y = z$. Infatti se $xy = xz$ allora $y = x^{-1}xy = x^{-1}xz = z$, e l'altro caso è analogo.

Esempio: l'insieme delle funzioni biiettive $\{1, 2, 3\} \to \{1, 2, 3\}$ è un gruppo con l'operazione di composizione, la sua cardinalità è 6 e non è commutativo (esercizio). Più in generale dato un insieme X, l'insieme $\mathrm{Sym}(X)$ delle funzioni biiettive $X \to X$ è un gruppo con la composizione, non commutativo a meno che $|X| \leq 2$. Se $X = \{1, 2, ..., n\}$ allora $\mathrm{Sym}(X)$ verrà denotato $\mathrm{Sym}(n)$ o S_n e chiamato "gruppo simmetrico su n oggetti". Si ha $|\mathrm{Sym}(n)| = n!$ (esercizio).

DEFINIZIONE 2 (Potenza). *Siano $(G, \cdot)$ un gruppo, $g \in G$, $n \in \mathbb{N}$. g^n è una notazione per indicare l'elemento $g \cdot g \cdot ... \cdot g$ (dove i g sono n) ottenuto iterando l'operazione. Poniamo inoltre per definizione $g^{-n} := (g^{-1})^n = (g^n)^{-1}$.*

ESERCIZIO 1. *Siano G un gruppo, $g \in G$. Mostrare che se $m \in \mathbb{N}$ allora $g^n g^m = g^{n+m}$, $(g^n)^m = g^{nm}$. In particolare l'insieme $\{g^n \mid n \in \mathbb{Z}\}$ è anch'esso un gruppo.*

DEFINIZIONE 3 (Gruppo ciclico). *Un gruppo G si dice ciclico se esiste $g \in G$ tale che ogni elemento di G è della forma g^n per un qualche n intero positivo. In tal caso g si dice generatore di G e G viene denotato con $\langle g \rangle$. Un generico gruppo ciclico finito di ordine n si indica con C_n.*

Un gruppo ciclico è abeliano perché un elemento commuta sempre con le sue potenze.

Esempio: $(\mathbb{Z}, +)$ è un gruppo ciclico.

Esempio: $(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo ciclico di ordine n.

ESERCIZIO 2. *Dato un gruppo ciclico $G = \langle g \rangle$ di ordine n, mostrare che i generatori di G sono tutti e soli gli elementi di G della forma g^m con m coprimo con n.*

Da quest'ultimo esercizio segue che il numero di generatori di G è uguale al numero di interi compresi tra 1 e n e coprimi con n. Tale numero viene usualmente indicato con $\varphi(n)$. La funzione $\varphi : \mathbb{N} \to \mathbb{N}$ si chiama "φ di Euler".

ESERCIZIO 3. *Sia $\varphi : \mathbb{N} - \{0\} \to \mathbb{N}$ la funzione di Euler. Si hanno i seguenti fatti.*

1. *Se p è primo e $n > 0$ è un intero allora $\varphi(p^n) = p^{n-1}(p-1)$.*
2. *Se m, n sono interi positivi coprimi allora $\varphi(mn) = \varphi(m)\varphi(n)$.*
3. *Se $n = {p_1}^{e_1}...{p_r}^{e_r}$ dove i p_i sono primi a due a due distinti allora*

$$\varphi(n) = (p_1 - 1){p_1}^{e_1 - 1}...(p_r - 1){p_r}^{e_r - 1}.$$

Cosicché per esempio

$$\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(5) = (2-1) \cdot 2^2 \cdot (3-1) \cdot 3^1 \cdot (5-1) = 96.$$

DEFINIZIONE 4 (Ordine di un elemento). *Dato un gruppo G e dato un suo elemento x, l'**ordine** di x in G è per definizione la cardinalità del gruppo ciclico $\langle x \rangle$, ovvero il più piccolo intero positivo n tale che $x^n = 1$ se tale n esiste, infinito altrimenti. L'ordine di x si indica con $|x|$.*

Osservazione: Se G è finito allora ogni suo elemento ha ordine finito: per vedere questo prendiamo $x \in G$ e consideriamo l'insieme delle potenze x^n di x in G; siccome G è finito tali potenze non sono infinite, quindi esistono due interi distinti $n > m$ tali che $x^n = x^m$. Moltiplicando a sinistra per $(x^{-1})^m$ otteniamo $1 = x^n(x^{-1})^m = x^{n-m}$. Quindi l'ordine di x è finito essendo minore o uguale di $n - m$.

ESERCIZIO 4. *Siano G un gruppo, $g, h \in G$ tali che $gh = hg$, e $|g| = s$, $|h| = t$ siano finiti. Mostrare che $|gh|$ divide il minimo comune multiplo tra s e t, e che se s e t sono coprimi allora $|gh| = st$.*

Notazione: se un semigruppo è abeliano l'operazione viene abitualmente indicata con $+$. Se l'operazione è indicata con $+$ l'eventuale elemento neutro è indicato con 0 (zero), altrimenti con 1 (uno).

Attenzione: questo non significa che non si possa decidere di usare la notazione additiva per semigruppi, monoidi o gruppi non abeliani.

DEFINIZIONE 5 (Omomorfismi e nuclei). *Dati due semigruppi (risp. monoidi, gruppi) $(S, *)$ ed $(T, *')$, un "**omomorfismo**" tra S ed T è una funzione $f : S \to T$ tale che $f(s * r) = f(s) *' f(r)$ per ogni $s, r \in S$, e che inoltre mandi l'eventuale elemento neutro di S nell'eventuale elemento neutro di T. Un tale f si dice "**monomorfismo**" se è insiemisticamente iniettivo, "**epimorfismo**" se è insiemisticamente suriettivo, "**isomorfismo**" se è insiemisticamente biiettivo. Se esiste un isomorfismo $S \to T$ si dice che S e T sono isomorfi e si scrive $S \cong T$. Se S, T sono (almeno) monoidi, il "**nucleo**" di f è $\ker(f) := \{s \in S \mid f(s) = 1\}$.*

Esempio: Dati due gruppi G e H, la funzione $G \to H$ che manda tutto in 1 è un omomorfismo, il suo nucleo è G e la sua immagine è $\{1\}$.

Esempio: $(\mathbb{R}, +)$ e $(\mathbb{R}_{>0}, *)$ sono gruppi abeliani. La funzione

$$f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, *) , \qquad x \mapsto e^x$$

è un isomorfismo di gruppi.

DEFINIZIONE 6 (Automorfismi). *Dato un qualsiasi gruppo G, un automorfismo di G è un isomorfismo $G \to G$. L'insieme degli automorfismi di G viene denotato con $\mathrm{Aut}(G)$, ed è un gruppo con l'operazione di composizione. Il suo elemento neutro è la funzione identità $G \to G$.*

ESERCIZIO 5. *Mostrare che $\mathrm{End}(C_n)$, l'insieme degli omomorfismi $C_n \to C_n$, è un anello rispetto a somma e composizione isomorfo a $\mathbb{Z}/n\mathbb{Z}$, e che $\mathrm{Aut}(C_n) \cong U(\mathbb{Z}/n\mathbb{Z})$, dove $U(\mathbb{Z}/n\mathbb{Z})$ è l'insieme degli elementi invertibili rispetto alla moltiplicazione dell'anello $\mathbb{Z}/n\mathbb{Z}$.*

ESERCIZIO 6. *Un omomorfismo di gruppi $f : G \to H$ è iniettivo se e solo se $\ker(f) = \{1\}$.*

ESERCIZIO 7. *Se $f : G \to H$ è un omomorfismo iniettivo di gruppi allora f conserva gli ordini degli elementi: $|f(g)| = |g|$ per ogni $g \in G$.*

ESERCIZIO 8. *Dato un omomorfismo di gruppi $f : G \to H$ si ha $f(g^{-1}) = f(g)^{-1}$ per ogni $g \in G$.*

ESERCIZIO 9. *Due gruppi ciclici di ordine n sono isomorfi. Segue che ogni gruppo ciclico di ordine n è isomorfo a $(\mathbb{Z}/n\mathbb{Z}, +)$.*

DEFINIZIONE 7 (Prodotto diretto). *Se G e H sono due gruppi allora l'insieme $G \times H$ è un gruppo con l'operazione "per componenti": $(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$. L'elemento neutro risulta essere $(1, 1)$. $G \times H$ con questa operazione si dice il prodotto diretto (esterno) di G e H. Per estensione, se $G_1, ..., G_n$ sono n gruppi l'insieme $G_1 \times ... \times G_n$ con l'operazione per componenti è un gruppo, detto il prodotto diretto (esterno) di $G_1, ..., G_n$.*

ESERCIZIO 10. *Mostrare che un prodotto diretto di gruppi abeliani è un gruppo abeliano, ma che un prodotto diretto di gruppi ciclici non è necessariamente ciclico.*

DEFINIZIONE 8 (Sottogruppi, classi laterali e quozienti). *Dato un gruppo G, un sottogruppo di G è un sottoinsieme H di G contenente 1, chiuso per l'operazione di G (cioè tale che se $a, b \in H$ allora $ab \in H$) e contenente l'inverso di ogni suo elemento. Equivalentemente si tratta di un sottoinsieme non vuoto H di G tale che per ogni $a, b \in H$ si ha $ab^{-1} \in H$. Se H è un sottogruppo di G si scrive $H \leq G$. Un laterale destro di un sottogruppo H di G è un sottoinsieme di G della forma $Hg := \{hg \mid h \in H\}$ per un $g \in G$; un laterale sinistro è un sottoinsieme di G della forma $gH := \{gh \mid h \in H\}$ per un $g \in G$. Un sottogruppo N di G si dice "sottogruppo normale (di G)" se $gng^{-1} \in N$ per ogni $g \in G$, $n \in N$, o equivalentemente $gN = Ng$, ovvero $gNg^{-1} = N$, per ogni $g \in G$. Se N è un sottogruppo normale di G si scrive $N \trianglelefteq G$. In tal caso definita in G la relazione di equivalenza "$x \sim y \Leftrightarrow xy^{-1} \in N$", possiamo dotare l'insieme quoziente G/N della struttura di gruppo data dall'operazione $(gN)(g'N) := gg'N$ (tale operazione è ben definita perché N è normale). Si tratta dell'unica struttura che rende l'applicazione canonica $G \to G/N$ un omomorfismo.*

DIMOSTRAZIONE. (delle asserzioni fatte).

- $H \leq G$ se e solo se $ab^{-1} \in H$ per ogni $a, b \in H$: supponiamo $H \leq G$, e siano $a, b \in H$; allora $b^{-1} \in H$ perché $b \in H$, e $ab^{-1} \in H$ perché H è chiuso rispetto all'operazione di G. Viceversa sia H un sottoinsieme non vuoto di G tale che $ab^{-1} \in H$ per ogni $a, b \in H$. Sia $a \in H$ (esiste perché H è non vuoto); allora prendendo $b = a$ otteniamo che $1 = aa^{-1} \in H$. Presi $x, y \in H$ scegliamo $a = x$ e $b = y^{-1}$ otteniamo $H \ni ab^{-1} = x(y^{-1})^{-1} = xy$.
- Dato $N \leq G$, $gN = Ng$ (cioè $g^{-1}Ng = N$) per ogni $g \in G$ se e solo se $gng^{-1} \in N$ per ogni $n \in N$, $g \in G$. Supponiamo che $gN = Ng$ per ogni $g \in G$, e sia $n \in N$. Allora $gn \in gN = Ng$, quindi $gn = mg$ per un opportuno $m \in N$, e $gng^{-1} = mgg^{-1} = m \in N$. Supponiamo che $gng^{-1} \in N$ per ogni $n \in N$, $g \in G$. Dato $gn \in gN$, si ha che $gn = (gng^{-1})g \in Ng$ dato che $gng^{-1} \in N$. Viceversa dato $ng \in Ng$, si ha che $ng = g(g^{-1}ng) \in gN$ dato che $g^{-1}ng \in N$.
- Se N è normale allora la posizione $(gN)(hN) = (gh)N$ definisce bene una operazione che rende G/N un gruppo. Basta osservare che $gNhN = gh(h^{-1}Nh)N = ghNN = ghN$. L'elemento neutro di G/N è N, e l'inverso di gN è $g^{-1}N$.

□

Esempio: Dato un gruppo G, $\{1\}$ e G sono sottogruppi di G. $\{1\}$ è usualmente chiamato il sottogruppo banale. Un sottogruppo H di G si dice "proprio" se $H \neq G$.

ESERCIZIO 11. *Siano G, H due gruppi. Mostrare che $G \times \{1\}$ e $\{1\} \times H$ sono sottogruppi normali di $G \times H$.*

Dati n sottogruppi $H_1, ..., H_n$ di un gruppo G, indichiamo con $H_1...H_n$ il sottoinsieme $\{h_1...h_n \mid h_i \in H_i \ \forall i = 1, ..., n\}$.

ESERCIZIO 12. *Siano H, K due sottogruppi di un gruppo G. Mostrare che $|HK| = |H| \cdot |K|/|H \cap K|$.*

ESERCIZIO 13. *Siano G un gruppo, $N_1, ..., N_t$ sottogruppi normali di G tali che $N_i \cap (N_1...N_{i-1}N_{i+1}...N_t) = \{1\}$ per ogni $i \in \{1, ..., t\}$. Mostrare che il sottogruppo*

di G generato da $N_1 \cup N_2 \cup ... \cup N_t$ coincide con $N_1...N_t$ ed è un sottogruppo normale di G isomorfo al prodotto diretto $N_1 \times N_2 \times ... \times N_t$. Un tale sottogruppo si dice "prodotto diretto interno" di $N_1, ..., N_t$.

Svolgimento: risolviamo dapprima il caso $t = 2$. Sia $H := (N_1 \cup N_2)$ il sottogruppo di G generato da N_1 e N_2. Consideriamo $N_1N_2 := \{xy \mid x \in N_1,\ y \in N_2\}$. Si tratta di un sottogruppo di G perché se $x, z \in N_1$ e $y, w \in N_2$ allora $(xy)(zw) = x(yzy^{-1})(yw) \in N_1N_2$ perché $yzy^{-1} \in N_1$ essendo N_1 normale in G, e $yw \in N_2$ essendo N_2 un sottogruppo di G; inoltre $(xy)^{-1} = y^{-1}x^{-1} = (y^{-1}x^{-1}y)y^{-1} \in N_1N_2$ perché $y^{-1}x^{-1}y \in N_1$ essendo $x^{-1} \in N_1$ e N_1 normale in G, e $y^{-1} \in N_2$. Questo prova che $N_1N_2 \leq G$. Siccome ogni sottogruppo di G contenente N_1 e N_2 deve contenere N_1N_2, si deduce che $H = N_1N_2$. N_1N_2 è normale in G perché se $g \in G$, $n_1 \in N_1$ e $n_2 \in N_2$ allora $g^{-1}n_1n_2g = (g^{-1}n_1g)(g^{-1}n_2g) \in N_1N_2$ in quanto N_1 e N_2 sono normali. Ora mostriamo che dall'ipotesi $N_1 \cap N_2 = \{1\}$ segue che ogni elemento di N_1N_2 si scrive in modo unico come n_1n_2 con $n_1 \in N_1$, $n_2 \in N_2$. Se infatti $n_1n_2 = xy$ con $x \in N_1$, $y \in N_2$ allora $N_1 \ni x^{-1}n_1 = yn_2{}^{-1} \in N_2$, quindi $x^{-1}n_1$ e $yn_2{}^{-1}$ appartengono a $N_1 \cap N_2 = \{1\}$. Segue che $x = n_1$ e $y = n_2$. Di conseguenza la funzione $f : N_1 \times N_2 \to N_1N_2$ che manda (x, y) in xy è ben definita. Per concludere basta mostrare che è un isomorfismo di gruppi. Se $(x, y), (z, w) \in N_1 \times N_2$ allora $f((x, y)(z, w)) = f(xz, yw) = xzyw$ e $f(x, y)f(z, w) = xyzw$, quindi per mostrare che f è un omomorfismo di gruppi basta mostrare che $yz = zy$, ovvero $yzy^{-1}z^{-1} = 1$, e questo segue dal fatto che $yzy^{-1} \in N_1$ e $zy^{-1}z^{-1} \in N_2$, essendo N_1, N_2 normali in G, da cui $yzy^{-1}z^{-1} \in N_1 \cap N_2 = \{1\}$. L'omomorfismo f è ovviamente suriettivo. Per mostrare che f è iniettivo basta mostrare che $\ker(f) = \{1\}$. Sia dunque $(x, y) \in \ker(f)$, cosicché $f(x, y) = xy = 1$. Siccome ogni elemento di N_1N_2 si scrive in modo unico come n_1n_2 con $n_1 \in N_1$, $n_2 \in N_2$, siccome $xy = 1 \cdot 1$ si deve avere $x = y = 1$, ovvero $(x, y) = (1, 1)$.

Passiamo ora al caso generale, e procediamo per induzione su t. Sappiamo che $(N_1 \cup ... \cup N_{t-1}) = N_1...N_{t-1}$ è isomorfo al prodotto diretto $N_1 \times ... \times N_{t-1}$, e che è un sottogruppo normale di G. Siccome $N_1...N_{t-1} \cap N_t = \{1\}$ possiamo applicare il caso $t = 2$ e concludere che $(N_1 \cup ... \cup N_t) = (N_1...N_{t-1}) \times N_t \cong N_1 \times ... \times N_t$. Questo conclude lo svolgimento dell'esercizio.

Osserviamo che l'ipotesi "$N_i \cap N_j = \{1\}$ per ogni $i \neq j$" era insufficiente: basta considerare $G := C_2 \times C_2$. G ammette tre sottogruppi normali $C_2 \times \{1\}$, $\{1\} \times C_2$, $\langle(1, 1)\rangle$, tutti isomorfi a C_2, che si intersecano a due a due in $\{1\}$, ma essi non possono generare un sottogruppo isomorfo a $C_2 \times C_2 \times C_2$.

Osserviamo inoltre che la tesi dell'esercizio restava valida se si supponeva come ipotesi che gli N_i avessero ordini coprimi: $(|N_i|, |N_j|) = 1$ per ogni $i \neq j$.

Esercizio 14. *Un'intersezione arbitraria di sottogruppi di un dato gruppo è ancora un sottogruppo.*

Esercizio 15. *Un automorfismo ϕ di G si dice interno se esiste $g \in G$ tale che $\phi(x) = g^{-1}xg$ per ogni $x \in G$. L'insieme degli automorfismi interni di G si indica con* $\mathrm{Inn}(G)$. *Mostrare che* $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Il quoziente $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ si indica con $\mathrm{Out}(G)$. Gli elementi di $\mathrm{Out}(G)$ si chiamano automorfismi esterni, sebbene non siano automorfismi nel senso proprio.

Definizione 9 (Sottogruppo generato). *Dato un gruppo G ed un suo sottoinsieme S, il sottogruppo di G generato da S è l'intersezione di tutti i sottogruppi di G contenenti S. Verrà indicato con $\langle S\rangle$.*

Per esempio se $S = \{g\}$, $\langle S \rangle$ è il sottogruppo ciclico generato da g.

ESERCIZIO 16. *Dati un gruppo G ed un suo elemento x, $|x|$ è l'ordine del sottogruppo ciclico di G generato da x.*

ESERCIZIO 17. *Ogni gruppo ciclico infinito è isomorfo a $(\mathbb{Z}, +)$.*

ESERCIZIO 18. *Sia $n \in \mathbb{N}$. L'insieme*

$$\mathrm{Stab}(n+1) := \{\sigma \in S_{n+1} \mid \sigma(n+1) = n+1\}$$

è un sottogruppo di S_{n+1} isomorfo a S_n ("Stab" sta per "stabilizzatore").

ESERCIZIO 19. *I sottogruppi e i quozienti di C_n sono ciclici. Dato un divisore d di n, esiste esattamente un sottogruppo di C_n di ordine d.*

ESERCIZIO 20. *Se n e m sono interi positivi coprimi allora $C_{nm} \cong C_n \times C_m$.*

Osservazione: Se $n \in \mathbb{Z}$ l'insieme $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ è un sottogruppo di $(\mathbb{Z}, +)$. Di più, ogni sottogruppo di $\mathbb{Z}$ è del tipo $n\mathbb{Z}$ con $n \in \mathbb{Z}$: per vedere questo prendiamo G, un sottogruppo di $\mathbb{Z}$ diverso da $\{0\}$, e definiamo d come il più piccolo intero positivo appartenente a G. È chiaro che $d\mathbb{Z} \subseteq G$. Viceversa se $g \in G$ effettuando la divisione con resto di g per d otteniamo $g = dq + r$ con $0 \leq r < d$. Ma allora $r = g - dq \in G$, quindi per minimalità di d il numero r dev'essere nullo: $r = 0$. Segue che $g \in d\mathbb{Z}$, e quindi anche $G \subseteq d\mathbb{Z}$. Segue che $G = d\mathbb{Z}$. Ricaviamo in particolare:

PROPOSIZIONE 1 (Identità di Bezout). *Siano m, n due interi, e sia $d = (m, n)$. Allora esistono interi α, β tali che $\alpha m + \beta n = d$.*

DIMOSTRAZIONE. Osserviamo che $\langle m, n \rangle \leq \mathbb{Z}$ quindi $\langle m, n \rangle = d\mathbb{Z}$ per qualche intero d. A questo punto siccome $d \in \langle m, n \rangle = \{\alpha m + \beta n \mid \alpha, \beta \in \mathbb{Z}\}$ devono esistere α, β come nell'enunciato. Inoltre siccome $m, n \in d\mathbb{Z}$ si ha che m e n sono multipli di d, ma non possono avere un fattore comune più grande di d altrimenti l'uguaglianza $\alpha m + \beta n = d$ non potrebbe sussistere. In altre parole $d = (m, n)$. □

ESERCIZIO 21. *Provare che dato un elemento g di un gruppo G, l'insieme degli interi $z \in \mathbb{Z}$ tali che $g^z = 1$ è un sottogruppo di $\mathbb{Z}$, diciamo $n\mathbb{Z}$. Mostrare che in tal caso $n = |g|$.*

ESERCIZIO 22. *[CENTRALIZZANTE]Dati un gruppo G e un suo elemento x, $C_G(x) := \{g \in G \mid gx = xg\}$ è un sottogruppo di G contenente x, e detto centralizzante di x in G.*

ESERCIZIO 23. *[NORMALIZZANTE]: dati un gruppo G ed un suo sottogruppo H, $N_G(H) := \{g \in G \mid g^{-1}Hg = H\}$ è un sottogruppo di G contenente H, e detto normalizzante di H in G.*

ESERCIZIO 24. *[CENTRO]: dato un gruppo G, mostrare che $Z(G) := \{g \in G \mid gx = xg \ \forall x \in G\}$ è un sottogruppo di G, detto centro di G. Si tratta dell'intersezione dei centralizzanti degli elementi di G. Chiaramente G è abeliano se e solo se $Z(G) = G$.*

ESERCIZIO 25. *Il nucleo di un omomorfismo di gruppi è un sottogruppo normale del dominio, e la sua immagine è un sottogruppo del codominio.*

ESERCIZIO 26. *[Primo teorema di isomorfismo per i gruppi]: dato un omomorfismo $f : G \to H$ di gruppi, esso induce un isomorfismo canonico $\tilde{f} : G/\ker(f) \to f(G)$ (quello che manda $g\ker(f)$ in $f(g)$).*

DIMOSTRAZIONE. Questo è un tipico caso in cui si deve verificare la buona definizione di qualcosa: la legge che manda $g\ker(f)$ in $f(g)$ non è ben definita finché da $g\ker(f) = g'\ker(f)$ non segue $f(g) = f(g')$ (ovvero l'immagine di una classe di $\ker(f)$ non deve dipendere dal rappresentante scelto per calcolarla). Si tratta quindi di dimostrare questa implicazione. Se $g\ker(f) = g'\ker(f)$ allora $g^{-1}g' \in \ker(f)$ per definizione, quindi $f(g^{-1}g') = 1$, e quindi $f(g) = f(g')$. □

ESERCIZIO 27. *[Secondo teorema di isomorfismo per i gruppi]: siano G un gruppo, $H \leq G$ e $N \trianglelefteq G$. Allora $HN := \{hn \mid h \in H,\ n \in N\}$ è un sottogruppo di G, N è normale in HN, $H \cap N$ è normale in H e $H/H \cap N \cong HN/N$.*

ESERCIZIO 28. *[Terzo teorema di isomorfismo per i gruppi]: siano $H \subseteq N$ due sottogruppi normali di un gruppo G. Allora esiste un isomorfismo canonico $(G/H)/(N/H) \cong G/N$.*

TEOREMA 1 (Teorema di Lagrange). *Siano G un gruppo finito e H un suo sottogruppo. Allora $|H|$ divide $|G|$.*

DIMOSTRAZIONE. Osserviamo che l'insieme $\{gH \mid g \in G\}$ delle classi laterali sinistre di H è una partizione di G. Infatti:

- Per ogni $g \in G$, gH è non vuoto (contiene g).
- L'unione dei gH è tutto G, infatti un fissato $g \in G$ appartiene a gH.
- Due diverse classi laterali g_1H, g_2H sono disgiunte. Infatti se $x \in g_1H \cap g_2H$ allora $x = g_1h_1 = g_2h_2$ per opportuni $h_1, h_2 \in H$, quindi $g_1 = g_2h_2h_1{}^{-1} \in g_2H$ e $g_2 = g_1h_1h_2{}^{-1} \in g_1H$, da cui $g_1H = g_2H$.

Osserviamo inoltre che per ogni $g \in G$ si ha $|gH| = |H|$. Infatti la funzione $H \to gH$ che manda h in gh è biiettiva. □

Segue dal teorema di Lagrange che se G è un gruppo finito e $H \leq G$ il numero $|G|/|H|$ è intero: esso si chiama indice di H in G. Più in generale:

DEFINIZIONE 10 (Indici). *Dati un gruppo G ed un suo sottogruppo H, l'indice di H in G è la cardinalità dell'insieme delle classi laterali sinistre, uguale alla cardinalità dell'insieme delle classi laterali destre. Si indica con $[G : H]$.*

In particolare se G è finito allora $|G| = |H| \cdot [G : H]$.

ESERCIZIO 29. *Dimostrare che dato un qualsiasi gruppo G, ogni suo sottogruppo di indice 2 è normale.*

PROPOSIZIONE 2 (Formula degli indici). *Sia G un gruppo, e siano $K \leq H \leq G$. Allora $[G : K]$ è finito se e solo se $[G : H]$ e $[H : K]$ sono finiti, e in tal caso*

$$[G : K] = [G : H][H : K].$$

DIMOSTRAZIONE. Sappiamo che $[G : H] = |\{gH \mid g \in G\}|$. Sia T un trasversale sinistro di H in G, ovvero un sottoinsieme di G che contiene esattamente un elemento per ogni classe laterale sinistra di H, e sia S un trasversale sinistro di K in H. Evidentemente $|T| = [G : H]$, $|S| = [H : K]$. Per provare che $[G : K] = |T||S|$ basta provare che $TS := \{ts \mid t \in T,\ s \in S\}$ è un trasversale sinistro di K in G.

Sia quindi $g \in G,\ g = th$ con $t \in T,\ h \in H$. Questo è possibile perché T è un trasversale di H e g deve appartenere a qualche classe laterale di H. Ora $h = sk$ con $s \in S,\ k \in K$. Quindi $g = (ts)k$. Ne segue che $g \in (ts)K$. Ora supponiamo che $t_1 s_1 K = t_2 s_2 K$ per qualche $t_1, t_2 \in T,\ s_1, s_2 \in S$. Equivalentemente $(t_1 s_1)^{-1} t_2 s_2 = s_1^{-1} t_1^{-1} t_2 s_2 \in K$. Sia quindi $k \in K$ tale che $s_1^{-1} t_1^{-1} t_2 s_2 = k$. Allora $t_1^{-1} t_2 = s_1 k s_2^{-1} \in H$ implica $t_1 = t_2$ perché T è trasversale di H in G. Ora $s_1^{-1} s_2 \in K$ implica $s_1 = s_2$ perché S è trasversale di K in H. Quindi $t_1 s_1 = t_2 s_2$. □

Osservazione: Se x è un elemento di un gruppo finito G allora l'ordine di x divide $|G|$ essendo $\langle x \rangle$ un sottogruppo di G di ordine uguale all'ordine di x. In particolare $x^{|G|} = 1$.

Esercizio 30. *Se m, n sono interi coprimi allora m è invertibile in $\mathbb{Z}/n\mathbb{Z}$ e viceversa (basta usare l'identità di Bezout).*

Vediamo ora un esempio elementare di applicazione di questa teoria. Se p è un primo l'insieme $\mathbb{Z}/p\mathbb{Z} - \{0\}$ è chiuso per l'operazione di moltiplicazione, perché se p divide un prodotto allora divide uno dei fattori (e quindi un prodotto di classi modulo p non nulle non può essere nullo). Inoltre ogni intero compreso tra 1 e $p-1$ è coprimo con p, quindi ogni elemento di $\mathbb{Z}/p\mathbb{Z} - \{0\}$ ammette inverso moltiplicativo. Segue che $\mathbb{Z}/p\mathbb{Z} - \{0\}$ è un gruppo moltiplicativo di ordine $p-1$. Vedremo in seguito che tale gruppo è ciclico.

Proposizione 3 (Piccolo teorema di Fermat). *Siano n un intero, p un numero primo. Allora p divide $n^p - n$.*

Osserviamo che questa proposizione non ha l'aria di essere facile da dimostrare. Ma con gli strumenti che abbiamo possiamo banalizzarla.

Dimostrazione. Naturalmente possiamo supporre che p non divida n altrimenti l'asserto è banale. Ora, si tratta di mostrare che nel campo $\mathbb{Z}/p\mathbb{Z}$ si ha $n^p = n$. n è invertibile modulo p, quindi appartiene al gruppo moltiplicativo $\mathbb{Z}/p\mathbb{Z} - \{0\}$ che ha ordine $p - 1$, da cui $n^{p-1} = 1$. Moltiplicando per n, otteniamo $n^p = n$. □

Introduciamo altre definizioni utili. Siano G un gruppo, N un suo sottogruppo normale. Un "**supplemento**" di N in G è un sottogruppo H di G tale che $HN := \{hn \mid h \in H,\ n \in N\}$ coincide con G. In questo caso si dice che H supplementa N, o che N è supplementato da H. Un "**complemento**" di N in G è un supplemento H di N in G tale che $H \cap N = \{1\}$. In questo caso si dice che H complementa N, o che N è complementato da H.

Definizione 11 (Prodotto semidiretto). *Se N e H sono due gruppi e $\varphi : H \to \mathrm{Aut}(N)$ è un omomorfismo, il "**prodotto semidiretto**" di N e H rispetto a φ, indicato con $N \rtimes H$ o con $H \ltimes N$, è il gruppo il cui supporto è il prodotto cartesiano $H \times N$, e la cui operazione è definita da $(h_1, n_1) \cdot (h_2, n_2) := (h_1 h_2, n_1{}^{h_2} n_2)$, dove se $n \in N$ e $h \in H$, n^h sta ad indicare $\varphi(h)(n)$, l'automorfismo relativo ad h applicato a n.*

Esercizio 31. *Mostrare che $N \times \{1\}$ e $\{1\} \times H$ sono sottogruppi di $N \rtimes H$, che $N \times \{1\}$ è normale complementato da $\{1\} \times H$. Mostrare che se G è un gruppo e N, H sono due suoi sottogruppi con N normale in G e complementato da H allora $G \cong N \rtimes H$. Mostrare che il prodotto semidiretto $N \rtimes H$ è un prodotto diretto se e solo se φ è l'omomorfismo che manda tutto in 1 (l'identità $N \to N$).*

ESEMPIO: Dato $n \in \mathbb{N}$ sia $D_{2n} := C_n \rtimes C_2$ dove l'operazione, detti $C_2 = \langle h \rangle$ e $C_n = \langle g \rangle$, è determinata dalla relazione $g^h = g^{-1}$, nel senso che risulta

$$(h^a g^b)(h^c g^d) = h^{a+c} h^{-c} g^b h^c g^d = h^{a+c} g^{(-1)^c b + d}.$$

Questo definisce bene il gruppo D_{2n}, che si dice "**gruppo diedrale**" di ordine $2n$. D_{2n} ammette la presentazione seguente:

$$D_{2n} = \langle g, h \mid g^n = h^2 = 1,\ g^h = g^{-1} \rangle.$$

ESEMPIO: siano N un gruppo, k un intero positivo. Allora S_k è contenuto nel gruppo degli automorfismi di N^k (il prodotto diretto di N con se stesso k volte), dato che un $\sigma \in S_k$ corrisponde all'automorfismo di N^k definito da $(n_1, ..., n_k) \mapsto (n_{\sigma(1)}, ..., n_{\sigma(k)})$. Possiamo quindi costruire il prodotto semidiretto $N^k \rtimes S_k$ relativo a tale inclusione. Più in generale se $K \leq S_k$ allora possiamo considerare il prodotto semidiretto $N^k \rtimes K$ relativo alla composizione $K \to S_k \to \mathrm{Aut}(N^k)$.

Se $K \leq S_k$ indichiamo il gruppo così costruito $N^k \rtimes K$ con $N \wr K$. Esso si dice "**prodotto intrecciato**" di N e K. Si ha $|N \wr K| = |N|^k |K|$.

2. Azioni di gruppi

Le azioni dei gruppi sono estremamente importanti.

DEFINIZIONE 12 (Azioni). *Siano G un gruppo, X un insieme. Un'azione a sinistra di G su X è una funzione $G \times X \to X$, $(g, x) \mapsto g \cdot x$ tale che:*

- *$(gh) \cdot x = g(h \cdot x)$ per ogni $g, h \in G$, $x \in X$;*
- *$1 \cdot x = x$ per ogni $x \in X$.*

In tal caso diciamo che G agisce su X a sinistra tramite l'azione data, e X si dice G-insieme. Se non ci sono ambiguità indicheremo l'immagine di (g, x) tramite l'azione con gx anziché con $g \cdot x$.

Analogamente possiamo parlare di azioni a destra. Un'azione a destra di G su X è una funzione $X \times G \to G$, $(x, g) \mapsto xg$ tale che $(x, 1) \mapsto x$ e $(xg)h = x(gh)$.

Per esempio lo spazio vettoriale $\mathbb{R}^2$ agisce sull'insieme delle rette del piano affine $\mathbb{R}^2$ traslandole: se v è un vettore e r è una retta mandiamo la coppia (v, r) in $r + v$.

DEFINIZIONE 13 (Stabilizzatori, orbite). *Dato un G-insieme X, lo stabilizzatore di $x \in X$ è $\mathrm{Stab}_G(x) := \{g \in G \mid gx = x\}$: si tratta di un sottogruppo di G. Il nucleo dell'azione è l'intersezione degli stabilizzatori. L'azione si dice fedele se il suo nucleo è $\{1\}$. L'orbita di un $x \in X$ è $o_G(x) = Gx := \{gx \mid g \in G\} \subseteq X$; le orbite formano una partizione di X. L'azione si dice transitiva se ammette una sola orbita.*

ESERCIZIO 32. *Mostrare che dare un'azione di G su X equivale a dare un omomorfismo di gruppi $f : G \to \mathrm{Sym}(X)$, confondendo gx con $f(g)(x)$. Il nucleo dell'azione coincide col nucleo di tale omomorfismo.*

Se il gruppo G agisce su un insieme X e $Y \subseteq X$ è tale che $g \cdot y \in Y$ per ogni $g \in G$, $y \in Y$ allora Y si dice "stabile" per l'azione di G su X.

Esempio: G agisce su se stesso nei seguenti modi:

- A destra per coniugio: $(g, x) \mapsto x^g := g^{-1} x g$. x^g si chiama coniugato di x tramite g. In tal caso gli stabilizzatori sono i centralizzanti e il nucleo è il centro. I sottogruppi normali sono esattamente i sottogruppi stabili rispetto a tale azione. Lo stabilizzatore di x secondo tale azione

è il centralizzante di x in G. L'orbita di x secondo tale azione si chiama classe di coniugio di x in G.
- A sinistra per moltiplicazione a sinistra: $(g, x) \mapsto gx$. Tale azione è fedele e transitiva.
- A destra per moltiplicazione a destra: $(g, x) \mapsto xg$. Tale azione è fedele e transitiva.

ESERCIZIO 33. *G agisce per coniugio sull'insieme dei suoi sottogruppi: $(g, H) \mapsto H^g := g^{-1}Hg$. Quali sono i sottogruppi la cui orbita consiste di un solo elemento?*

ESERCIZIO 34. *Dati un gruppo G e un suo sottogruppo H, G agisce per moltiplicazione a destra sui laterali destri di H ($(g, Hx) \mapsto Hxg$), e per moltiplicazione a sinistra sui laterali sinistri di H ($(g, xH) \mapsto gxH$). Quali sono i nuclei di queste azioni? E le orbite?*

ESERCIZIO 35. *[Equazione delle classi]: dati un gruppo G, un G-insieme X e $x \in X$, si ha $[G : \mathrm{Stab}_G(x)] = |Gx|$ (aiuto: considerare la funzione che manda $gx \in Gx$ nella classe $g\,\mathrm{Stab}_G(x)$ di $\mathrm{Stab}_G(x)$). Dal teorema di Lagrange segue allora la cosiddetta "equazione delle classi": $|G| = |Gx| \cdot |\mathrm{Stab}_G(x)|$.*

Le azioni di gruppi sono comode tra le altre cose per fare dei conteggi. Per esempio, sono utili per calcolare il numero di coniugati di un dato elemento o di un dato sottogruppo:

- G agisca su G per coniugio, e sia $x \in G$. Allora l'orbita di x è l'insieme dei coniugati di x in G, quindi per l'equazione delle classi x ha esattamente $[G : C_G(x)]$ coniugati in G.
- Sia $H \leq G$, e G agisca per coniugio sull'insieme dei suoi sottogruppi. Allora $\mathrm{Stab}(H) = N_G(H)$, e quindi per l'equazione delle classi H ha esattamente $[G : N_G(H)]$ coniugati in G. Per esempio se H è massimale e non normale in G allora $N_G(H) = H$ e quindi H ha tanti coniugati quant'è il suo indice in G.

Possiamo dedurre anche risultati a priori non banali:

- G agisca su se stesso per moltiplicazione a destra. Tale azione è fedele e transitiva, quindi G si immerge in $\mathrm{Sym}(G)$. Segue il teorema di Cayley, secondo cui ogni gruppo finito G si può vedere come sottogruppo di $\mathrm{Sym}(n)$ dove $n = |G|$.
- Sia $H \leq G$, e G agisca per moltiplicazione a destra sull'insieme delle classi laterali destre di H in G. In particolare $\mathrm{Stab}(H) = H$. Il nucleo dell'azione è l'intersezione dei coniugati di H in G, si denota con H_G e si chiama cuore normale di H. Si tratta del più grande sottogruppo normale di G contenuto in H. In particolare G/H_G si immerge in $\mathrm{Sym}(\{Hg \mid g \in G\}) \cong \mathrm{Sym}([G : H])$ e quindi $[G : H_G]$ divide $[G : H]!$. In particolare, da questo segue che se un sottogruppo H ha indice finito allora il suo cuore normale ha indice finito, minore o uguale di $[G : H]!$.

Da quest'ultimo punto segue la seguente:

PROPOSIZIONE 4. *Sia G un gruppo finito, e sia p il più piccolo primo che divide $|G|$. Allora ogni sottogruppo di G di indice p è normale.*

DIMOSTRAZIONE. Sia H un sottogruppo di indice p. Allora $[G : H_G]$ divide $|G|$ e $p!$, quindi deve eguagliare p, altrimenti avrebbe dei fattori primi minori di p.

Ne segue che $p = [G : H_G] = [G : H][H : H_G] = p[H : H_G]$, ovvero $[H : H_G] = 1$, cioè $H = H_G$, cioè $H \trianglelefteq G$. □

DEFINIZIONE 14 (Azioni equivalenti). *Sia G un gruppo che agisca su due insiemi X e Y. Tali due azioni si dicono equivalenti se esiste una biiezione $\varphi : X \to Y$ tale che $\varphi(xg) = \varphi(x)g$ per ogni $x \in X$, $g \in G$.*

È facile verificare che se $\varphi : X \to Y$ determina un'equivalenza di azioni di un gruppo G allora dato $x \in X$, l'immagine tramite φ dell'orbita di x è l'orbita di $\varphi(x)$, e lo stabilizzatore in G di $\varphi(x)$ è uguale allo stabilizzatore di x. Inoltre molte proprietà delle azioni sono stabili per equivalenza, come la transitività e la primitività (si vedrà in seguito cosa sia un'azione primitiva).

3. Gruppo simmetrico: proprietà e terminologia

Abbiamo denotato con S_n il gruppo simmetrico su n oggetti, ovvero il gruppo delle funzioni biiettive di un insieme di cardinalità n in sé con l'operazione di composizione. Questa definizione ha senso a meno di isomorfismi, nel senso che denotato con $\mathrm{Sym}(X)$ il gruppo delle permutazioni dell'insieme X, si ha che:

ESERCIZIO 36. *Se X e Y sono insiemi equipotenti allora* $\mathrm{Sym}(X)$ *e* $\mathrm{Sym}(Y)$ *sono gruppi isomorfi.*

Osserviamo inoltre che $\mathrm{Sym}(X)$ agisce su X nel modo "ovvio": $(\sigma, x) \mapsto \sigma(x)$. In questo modo un sottogruppo di S_n non è altro che un gruppo che agisce fedelmente su n oggetti.

Un *ciclo di lunghezza $d \leq n$ (d-ciclo)* è un elemento di S_n definito in questo modo:

$$i_1 \mapsto i_2 \mapsto i_3 \mapsto ... \mapsto i_{d-1} \mapsto i_d \mapsto i_1,$$

dove $i_1, ..., i_d \in \{1, ..., n\}$ sono a due a due distinti. Tale d-ciclo si indica con $(i_1 i_2 ... i_d)$. È convenzione comune che nell'applicare un prodotto di permutazioni ad un elemento si parta da destra, così per esempio il prodotto $(123)(234)(12)$ è uguale a (34), non a (1324). Due cicli $(i_1 ... i_d)$, $(j_1 ... j_t)$ si dicono *disgiunti* se $\{i_1, ..., i_d\} \cap \{j_1, ..., j_t\} = \emptyset$.

ESERCIZIO 37. *Due cicli disgiunti commutano.*

ESERCIZIO 38. *Ogni elemento di S_n si scrive in modo unico (a meno di scambiare l'ordine dei fattori) come prodotto (cioè composizione) di cicli disgiunti.*

*[*Suggerimento*: data $\sigma \in S_n$ considerare la relazione di equivalenza seguente in $\{1, ..., n\}$: $i \sim j$ se $\sigma^m(i) = j$ per qualche intero positivo m.]*

Se $l_1, ..., l_d$ sono le lunghezze dei cicli della decomposizione di $\sigma \in S_n$ allora la sequenza di tali lunghezze si chiama **struttura ciclica** di σ. Se σ ha nella decomposizione r_i cicli di lunghezza i per $i = 1, ..., n$ allora la struttura ciclica di σ si indica anche con $1^{r_1} 2^{r_2} ... n^{r_n}$.

ESERCIZIO 39. *Due elementi di S_n sono coniugati in S_n se e solo se hanno la stessa struttura ciclica.*

[Suggerimento: mostrare che se $\sigma \in S_n$ allora $\sigma^{-1}(i_1 ... i_d)\sigma = (\sigma(i_1) ... \sigma(i_d))$.]

Un ciclo di lunghezza 2 si chiama **trasposizione**.

ESERCIZIO 40. *Mostrare che ogni permutazione si può scrivere come prodotto di trasposizioni.*

*[*Suggerimento*: osservare che basta farlo per i cicli, e che* $(12...d) = (1d)(1\ d-1)(1\ d-2)...(13)(12)$*.]*

ESERCIZIO 41. *[Segno] Sia* $\sigma \in S_n$ *un prodotto di* k *trasposizioni. Mostrare che* $(-1)^k$ *dipende solo da* σ*. Esso viene denotato con* $\mathrm{sgn}(\sigma)$ *e chiamato segno di* σ *.*

Svolgimento: basta mostrare che una permutazione non si può scrivere contemporaneamente come prodotto di un numero dispari di trasposizioni e di un numero pari di trasposizioni. Siano dunque k, m due interi non negativi, e siano $g_1, ..., g_{2k+1}, h_1, ..., h_{2m}$ trasposizioni tali che $g_1...g_{2k+1} = h_1...h_{2m}$. Ricordando che ogni trasposizione ammette se stessa come inversa (perché se σ è una trasposizione allora $\sigma^2 = 1$) moltiplicando a destra ordinatamente per $h_{2m}, h_{2m-1}, ..., h_1$ si ottiene che $g_1...g_{2k+1}h_{2m}...h_1 = 1$. Siamo quindi ridotti a mostrare che 1 non si può scrivere come prodotto di un numero dispari di trasposizioni. Scriviamo $g_1...g_m = 1$ con $g_i = (g_{i1}, g_{i2})$ e $g_{i1} \neq g_{i2}$. Per concludere basta mostrare che ogni simbolo in $\{1, ..., n\}$ compare un numero pari di volte in $(g_{11}, g_{12}, g_{21}, g_{22}, ..., g_{m,1}, g_{m,2})$. Prendiamo per esempio il simbolo 1. Percorrendo il prodotto di trasposizioni da destra a sinistra scopriamo che se g_i muove un simbolo in 1 poi 1 dev'essere mosso da qualche g_{j_i}, e questo vale anche per le trasposizioni successive. Ne segue che 1 compare solo in trasposizioni del tipo $g_{i_1}, g_{j_{i_1}}, ..., g_{i_k}, g_{j_{i_k}}$, e quindi un numero pari di volte.

Una permutazione si dice **pari** se il suo segno è 1, **dispari** altrimenti.

ESERCIZIO 42. *Mostrare che la funzione* $S_n \to \{1, -1\}$ *che manda* σ *in* $\mathrm{sgn}(\sigma)$ *è un omomorfismo di gruppi (dove in* $\{-1, 1\}$ *c'è l'usuale prodotto di* $\mathbb{Z}$*).*

Il suo nucleo si indica con $\mathrm{Alt}(n)$ o A_n e si chiama **gruppo alterno** di grado n.

ESERCIZIO 43. *Mostrare che un ciclo di lunghezza* d *è una permutazione pari se e solo se* d *è dispari.*

ESERCIZIO 44. *Mostrare che le permutazioni pari di* S_n *sono esattamente quelle permutazioni che hanno nella struttura ciclica un numero pari di cicli di lunghezza pari.*

ESERCIZIO 45. *Mostrare che la potenza* k*-esima di un* n*-ciclo è un prodotto di* (n, k) *cicli disgiunti tutti di lunghezza* $n/(n, k)$*.*

ESERCIZIO 46. *Risolvere in* S_{10} *l'equazione* $\sigma^3 = (1234)(56)$*.*

Svolgimento: $(1234)(56)$ ha ordine 4. Elevando alla quarta otteniamo che $\sigma^{12} = 1$, quindi l'ordine di σ divide 12. D'altra parte 4 divide $|\sigma|$ (questo è un fatto generale: in ogni gruppo se un elemento x ha ordine finito allora l'ordine di ogni sua potenza divide $|x|$), quindi σ ha ordine 4 oppure 12. Per l'esercizio precedente nella struttura ciclica di σ ci deve essere la trasposizione (56), dato che è l'unica trasposizione nella struttura ciclica di σ^3, e ci deve essere una radice cubica di (1234), dato che (1234) è l'unico 4-ciclo nella struttura ciclica di σ^3. Ogni radice cubica di (1234) deve avere (1432) nella struttura ciclica. Ne segue che $\sigma = (1432)(56)\tau$ dove $\tau^3 = 1$ e gli elementi che τ coinvolge sono in $\{7, 8, 9, 10\}$. Ci sono 9 scelte possibili per τ, quindi 9 soluzioni.

4. Classificazione dei gruppi abeliani finitamente generati

Un gruppo G si dice finitamente generato se esiste $S \subseteq G$ finito tale che $G = \langle S \rangle$. Nel seguito indichiamo con $\mathbb{Z}^n$ il prodotto diretto di $\mathbb{Z}$ con se stesso n volte (è un esempio di gruppo abeliano finitamente generato). Chiamiamo "base" di $\mathbb{Z}^n$ un sottoinsieme $\{u_1, ..., u_t\}$ di $\mathbb{Z}^n$ tale che:

- $\{u_1, ..., u_t\}$ generi $\mathbb{Z}^n$;
- ogni volta che $a_1u_t + ... + a_tu_t = 0$ con $a_1, ..., a_t \in \mathbb{Z}$ si ha $a_1 = ... = a_t = 0$.

Si dimostra che ogni base di $\mathbb{Z}^n$ ha n elementi. È facile vedere che se $\{u_1, ..., u_n\}$ è una base di $\mathbb{Z}^n$ allora ogni $z \in \mathbb{Z}^n$ si scrive in modo unico come $a_1u_1 + ... + a_nu_n$ con $a_1, ..., a_n \in \mathbb{Z}$.

LEMMA 1. *Se H è un sottogruppo di $G := \mathbb{Z}^n$ allora $H \cong \mathbb{Z}^s$ con $s \leq n$ ed esistono una base $\{u_1, ..., u_n\}$ di G ed interi $\alpha_1, ..., \alpha_s$ tali che $\{\alpha_1u_1, ..., \alpha_su_s\}$ è una base di H.*

DIMOSTRAZIONE. Per induzione su n. Se $n = 1$ l'asserto è chiaro, dato che ogni sottogruppo di $\mathbb{Z}$ è del tipo $m\mathbb{Z}$ con $m \in \mathbb{Z}$. Supponiamo $n > 1$. Sia $\{w_1, ..., w_n\}$ una base di G. Dato $0 \neq h \in H$ scriviamo $h = h_1w_1 + ... + h_nw_n$ con $h_1, ..., h_n \in \mathbb{Z}$, e sia $\lambda(w_1, ..., w_n)$ il minimo h_i positivo che compare come coefficiente di qualche $h \in H$ nella base $\{w_1, ..., w_n\}$. Scegliamo $\{w_1, ..., w_n\}$ in modo che $\lambda(w_1, ..., w_n)$ sia minimo, chiamiamolo α_1. Numeriamo i w_i in modo tale che $v_1 = \alpha_1w_1 + \beta_2w_2 + ... + \beta_nw_n \in H$ per qualche $v_1 \in H$. Dividiamo β_i per α_1, ottenendo $\beta_i = \alpha_1q_i + r_i$ con $0 \leq |r_i| < \alpha_1$, e questo per ogni $i = 2, ..., n$. Sia $u_1 := w_1 + q_2w_2 + ... + q_nw_n$. Non è difficile mostrare che $\{u_1, w_2, ..., w_n\}$ è una base di G, e $v_1 = \alpha_1u_1 + r_2w_2 + ... + r_nw_n$. Ma allora $r_2 = ... = r_n = 0$ per minimalità di α_1, e quindi $v_1 = \alpha_1u_1$. Siano ora

$$G_1 := \{m_1u_1 + m_2w_2 + ... + m_nw_n \mid m_1 = 0\}, \qquad H_1 := G_1 \cap H.$$

È chiaro che $H_1 \cap \langle v_1 \rangle = \{0\}$, essendo $G_1 \cap \langle v_1 \rangle = \{0\}$. Vogliamo mostrare che $H = H_1 + \langle v_1 \rangle$.

- Dato $h \in H$ scriviamo $h = \gamma_1u_1 + \gamma_2w_2 + ... + \gamma_nw_n$, e $\gamma_1 = \alpha_1q + r_1$ con $0 \leq |r_1| < \alpha_1$. Allora $H \ni h - qv_1 = r_1u_1 + \gamma_2w_2 + ... + \gamma_nw_n$, perché $v_1 \in H$, quindi $r_1 = 0$ per minimalità di α_1. Quindi $h - qv_1 \in H_1$.

Ora $G_1 \cong \mathbb{Z}^{n-1}$ e $\{w_2, ..., w_n\}$ è una sua base, quindi per ipotesi induttiva $H_1 \leq G_1$ è isomorfo a $\mathbb{Z}^{s-1}$ con base $\{\alpha_2u_2, ..., \alpha_su_s\}$ per qualche $\alpha_2, ..., \alpha_s \in \mathbb{Z}$. Ne segue che $H \cong \mathbb{Z}^s$ con base $\{\alpha_1u_1, \alpha_2u_2, ..., \alpha_su_s\}$. □

TEOREMA 2. *Sia G un gruppo abeliano finitamente generato. Allora esistono potenze di primi $q_1, ..., q_t$ e interi $n, n_1, ..., n_t$ tali che*

$$G \cong \mathbb{Z}^n \times {C_{q_1}}^{n_1} \times ... \times {C_{q_t}}^{n_t}.$$

DIMOSTRAZIONE. Sia G un gruppo abeliano (con notazione additiva) finitamente generato, e sia $S = \{s_1, ..., s_n\} \subseteq G$ un insieme finito di n elementi che generi G. La funzione $\mathbb{Z}^n \to G$ definita dalla legge $e_i \mapsto s_i$ (dove $\{e_1, ..., e_n\}$ è la base canonica di $\mathbb{Z}^n$) estesa per linearità (ovvero $\sum_i a_ie_i \mapsto \sum_i a_is_i$) è un omomorfismo suriettivo di gruppi, quindi detto H il suo nucleo si ha $G \cong \mathbb{Z}^n/H$. Usando il lemma 1 possiamo scrivere $G = \langle u_1 \rangle \oplus ... \oplus \langle u_n \rangle$ e $H = \langle \alpha_1u_1 \rangle \oplus ... \oplus \langle \alpha_su_s \rangle$, e

da questo segue che

$$\begin{aligned} G/H &= \langle u_1\rangle \oplus ... \oplus \langle u_n\rangle / \langle \alpha_1 u_1\rangle \oplus ... \oplus \langle \alpha_s u_s\rangle \cong \\ &\cong \langle u_1\rangle/\langle \alpha_1 u_1\rangle \oplus ... \oplus \langle u_n\rangle/\langle \alpha_s u_s\rangle \oplus \langle u_{s+1}\rangle \oplus ... \oplus \langle u_n\rangle \cong \\ &\cong \mathbb{Z}/\alpha_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/\alpha_s\mathbb{Z} \oplus \mathbb{Z}^{n-s}. \end{aligned}$$

Per concludere basta osservare che in generale $\mathbb{Z}/m\mathbb{Z} \cong C_m$ e se $m = {p_1}^{a_1}...{p_t}^{a_t}$ è la fattorizzazione in primi di n allora $C_m \cong C_{{p_1}^{a_1}} \times ... \times C_{{p_t}^{a_t}}$. □

In pratica, questo teorema dice che i gruppi abeliani finitamente generati sono esattamente i prodotti diretti finiti di gruppi ciclici.

Esercizio 47. *Mostrare che esistono solo quattro gruppi abeliani di ordine* 36 *a meno di isomorfismi.*

5. p-gruppi e Teoria di Sylow

Sia p un numero primo. Un p-gruppo è un gruppo G ogni cui elemento ha ordine una potenza di p.

Lemma 2. *Sia G un gruppo finito di ordine divisibile per il primo p. Allora esiste $x \in G$ di ordine p.*

Dimostrazione. Se troviamo un elemento di G di ordine una potenza di p abbiamo finito, perché se $|x| = p^t$ allora $|x^{p^{t-1}}| = p$. Per fare questo basta trovare un elemento di G di ordine divisibile per p, perché se $|x| = mp^t$ allora $|x^m| = p^t$. Per induzione su $|G|$, basta trovare un sottogruppo proprio H o un quoziente proprio G/N di G il cui ordine divide p. Se G è abeliano allora è chiaro, perché se $x \in G$ ha ordine non divisibile per p allora possiamo applicare l'ipotesi induttiva su $G/\langle x\rangle$. Supponiamo quindi G non abeliano, cioè $G \neq Z(G)$. Se $Z(G) \neq 1$ allora concludiamo per ipotesi induttiva su $Z(G)$ o su $G/Z(G)$, quindi possiamo supporre $Z(G) = 1$. L'equazione delle classi per l'azione di coniugio fornisce l'uguaglianza

$$|G| = 1 + \sum_i [G : C_G(y_i)],$$

dove gli y_i sono rappresentanti di classi di coniugio distinte e non centrali (ciò perché G è l'unione disgiunta di $Z(G)$ più le orbite degli elementi non centrali, e per l'equazione delle classi la cardinalità dell'orbita di y_i è uguale all'indice del centralizzante di y_i), in particolare $G \neq C_G(y_i)$ per ogni i. Siccome p divide $|G|$, p deve non dividere qualche $[G : C_G(y_i)]$, quindi p divide qualche $|C_G(y_i)|$. Concludiamo per ipotesi induttiva. □

Esercizio 48. *Se G è un gruppo finito allora G è un p-gruppo se e solo se il suo ordine è una potenza di p (usare il lemma 2).*

Esercizio 49. *Usare l'equazione delle classi come fatto nella dimostrazione del lemma 2 per dimostrare che se G è un p-gruppo finito non banale allora il centro di G è non banale: $Z(G) \neq \{1\}$.*

Esercizio 50. *Usare l'esercizio precedente per dimostrare che dato un primo p, ogni gruppo di ordine p^2 è abeliano.*

A livello notazionale, quando si parla di gruppi finiti "p-gruppo" sta ad indicare un qualsiasi gruppo il cui ordine sia una potenza di un primo. Esempi di p-gruppi sono D_8, C_9, $C_4 \times C_8$, Q_8.

ESERCIZIO 51. *Fissati un primo p e un naturale n, quanti sono i gruppi abeliani di ordine p^n?*

Sia G un gruppo finito, e sia p un divisore primo di $|G|$. Un p-sottogruppo di Sylow (o p-Sylow) di G è un sottogruppo H di G il cui ordine è p^t, la massima potenza di p che divide $|G|$. Andiamo a mostrare il seguente:

TEOREMA 3. *Siano G un gruppo finito, p un divisore primo di $|G|$, e p^t la massima potenza di p che divide $|G|$.*

1. *Per ogni intero k tale che p^k divide $|G|$, esiste un sottogruppo di G di ordine p^k. In particolare esiste un p-Sylow di G.*
2. *Due qualsivoglia p-Sylow di G sono coniugati in G, e il loro numero divide l'indice di ogni p-Sylow ed è congruo a 1 modulo p.*
3. *Ogni sottogruppo di G che è un p-gruppo è contenuto in un p-Sylow di G.*

Prima di addentrarci nella dimostrazione mostriamo il seguente lemma:

LEMMA 3. *Sia p un numero primo. Se un p-sottogruppo H di un gruppo G normalizza un p-Sylow P di G allora $H \subseteq P$.*

DIMOSTRAZIONE. Indichiamo con $N_G(P)$ il normalizzante di P in G. Per definizione $P \trianglelefteq N_G(P)$ e per ipotesi $H \subseteq N_G(P)$. Ora HP è un sottogruppo di $N_G(P)$ dato che P è normale in $N_G(P)$, e $HP/P \cong H/H \cap P$ è un p-gruppo perché il suo ordine divide quello di H. Ma allora anche HP è un p-gruppo, e $|HP| = |HP/P||P| = |P|$ per massimalità di P (che è un p-Sylow). Quindi $HP/P = 1$, ovvero $H \subseteq P$. □

Ora dimostriamo il teorema 3.

Procediamo per induzione su $|G|$ per dimostrare il primo punto. Possiamo supporre che p divida gli indici dei centralizzanti degli elementi non centrali, perché altrimenti potremmo applicare l'ipotesi induttiva ad un opportuno centralizzante. Ma allora dall'equazione delle classi

$$|G| = |Z(G)| + \sum_i [G : C_G(y_i)]$$

deduciamo che p divide $|Z(G)|$. Sia x un elemento di $Z(G)$ di ordine p (che esiste per il lemma 2). Allora per ipotesi induttiva $G/\langle x\rangle$ ammette un sottogruppo $H/\langle x\rangle$ di ordine p^{k-1}, quindi $|H| = |H/\langle x\rangle||\langle x\rangle| = p^{k-1}p = p^k$.

Sia ora Π l'insieme dei p-Sylow di G, e sia $P \in \Pi$. Sia Σ un'orbita di Π per l'azione di coniugio di G, e partizioniamo Σ in P-orbite. La cardinalità di tali orbite è una potenza di p perché P è un p-gruppo. Osserviamo che se $P \in \Sigma$ allora $\{P\}$ è una P-orbita, ed è l'unica P-orbita con un solo elemento perché se $\{P_0\}$ è una P-orbita allora P normalizza P_0 e quindi dal lemma 3 si ha $P \subseteq P_0$ da cui $P = P_0$ essendo $|P| = |P_0|$. Segue che:

- se $P \in \Sigma$ allora $|\Sigma| \equiv 1 \mod (p)$.
- se $P \notin \Sigma$ allora $|\Sigma|$ è una potenza di p.

Quindi non appena Σ contiene qualche p-Sylow P (cioè $\Sigma \neq \emptyset$) si deve avere $\Sigma = \Pi$. In altre parole l'azione di coniugio di G sull'insieme Π dei P-Sylow è transitiva, e questo prova la prima parte del secondo punto. Inoltre abbiamo visto che $|\Pi| = |\Sigma| \equiv 1 \mod (p)$. Per mostrare che $|\Pi|$ divide $|G|/p^t$ basta osservare che se $P \in \Pi$ allora $|\Pi| = [G : N_G(P)]$ deve dividere $[G : P]$ dato che $P \subseteq N_G(P)$.

Sia ora H un p-sottogruppo di G. Partizioniamo Π in H-orbite. Siccome ogni H-orbita ha un numero di elementi che è una potenza di p, e la cardinalità di Π è congrua a 1 modulo p, deve esistere una H-orbita che consiste di un solo elemento, P. Segue che H normalizza P, cioè $H \subseteq P$ in virtù del lemma 3. Questo termina la dimostrazione del teorema 3.

Esercizio svolto: mostriamo che un gruppo G tale che $|G| = 231$ ha centro non banale. Sia allora Z il centro di G. Siccome $231 = 3 \cdot 7 \cdot 11$ esistono un 3-Sylow H, un 7-Sylow K e un 11-Sylow N. Il numero di 7-Sylow divide 33 ed è congruo a 1 modulo 7, quindi è 1. Siccome i 7-Sylow sono coniugati, l'unico 7-Sylow deve essere un sottogruppo normale di G. Analogamente c'è un solo 11-Sylow (l'unico numero congruo a 1 modulo 11 che divide 21 è 1) che quindi è normale. Il numero dei 3-Sylow invece può essere 1 oppure 7. Se c'è un solo 3-Sylow allora è normale e quindi G ammette tre sottogruppi normali di ordini 3, 7 e 11, quindi è il prodotto diretto interno di tali tre sottogruppi, che sono ciclici (hanno ordine primo), quindi G risulta abeliano e $Z = G$. Ricordiamo infatti che sottogruppi di ordine coprimo hanno intersezione banale (facile esercizio) e che, come già visto, il sottogruppo generato da un insieme di sottogruppi normali che si intersecano banalmente a due a due è il loro prodotto diretto interno.

L'alternativa è che i 3-Sylow siano 7. Per l'equazione delle classi il numero dei coniugati del particolare 3-Sylow H è uguale all'indice del normalizzante $N_G(H)$, quindi vale 33. In particolare $N_G(H)$ contiene un sottogruppo di ordine 11 (un suo 11-Sylow), che è anche sottogruppo di G, per cui si tratta proprio dell'11-Sylow di G. Analogamente al caso in cui c'era un solo 3-Sylow, deduciamo che $N_G(H)$ è il prodotto diretto interno di H e N. In particolare N centralizza H (cioè ogni elemento di N commuta con ogni elemento di H), e quindi l'11-Sylow N centralizza ogni sottogruppo di Sylow di G. Proviamo allora a dimostrare che $Z = N$. Basterebbe $N \subseteq Z$, ma siccome il centro non può essere un sottogruppo massimale, Z non può avere indice primo. Infatti:

LEMMA 4. *Il centro di un gruppo non è un sottogruppo massimale.*

DIMOSTRAZIONE. Sia Z il centro del gruppo G. Supponiamo per assurdo Z sottogruppo massimale. Sia $g \in G - Z$. Il centralizzante di g in G contiene Z e g, quindi coincide con G. In altre parole $g \in Z$, assurdo. □

Osserviamo ora che vale il seguente:

LEMMA 5. *Siano H e K due sottogruppi di un gruppo G tali che $HK = KH$ (questo succede in particolare se uno tra H e K è normale in G). Allora HK è un sottogruppo di G, e il suo ordine è $|H| \cdot |K|/|H \cap K|$.*

Segue che HKN è un sottogruppo di G di ordine 231, infatti K e N sono normali e $H \cap K = H \cap N = K \cap N = \{1\}$. Quindi $HKN = G$. Segue che ogni elemento di G si scrive come hkn con $h \in H$, $k \in K$, $n \in N$. Ma sappiamo che N centralizza H, K e N, quindi deve centralizzare tutto G; in altre parole $N \subseteq Z$, e quindi $N = Z$ (ogni sottogruppo proprio di G contenente propriamente N è massimale).

6. Gruppi nilpotenti

Se Ω è un fissato insieme, un Ω-gruppo è un gruppo G dotato di una funzione $\alpha : G \times \Omega \to G$ tale che per ogni fissato $\omega \in \Omega$ la funzione $G \to G$, $g \mapsto \alpha(g, \omega)$ è un

endomorfismo di G. Indicheremo $\alpha(g,\omega)$ con g^ω se non ci sono confusioni possibili. Un Ω-sottogruppo di un Ω-gruppo G è un sottogruppo H di G tale che $h^\omega \in H$ per ogni $\omega \in \Omega$. Un Ω-omomorfismo tra due Ω-gruppi G, H è un omomorfismo $f : G \to H$ tale che $f(g)^\omega = f(g^\omega)$ per ogni $\omega \in \Omega$. Per gli Ω-gruppi valgono i principali teoremi sui gruppi: il nucleo di un Ω-omomorfismo è un Ω-sottogruppo normale del dominio, l'immagine di un Ω-omomorfismo è un Ω-sottogruppo del codominio.

Dato un Ω-gruppo G, una Ω-serie di composizione per G è una sequenza

$$1 = G_0 \lhd G_1 \lhd ... \lhd G_l = G.$$

Se i G_i sono distinti l'intero l si dice lunghezza di tale serie. I quozienti G_i/G_{i-1} si dicono i fattori della serie. Osserviamo che ogni G_i è sub-normale in G, ovvero esiste una serie che va da G_i a G.

- se $\Omega = \emptyset$ si parlerà semplicemente di serie di composizione;
- se $\Omega = \mathrm{Inn}(G)$, il sottogruppo di $\mathrm{Aut}(G)$ che consiste degli automorfismi del tipo $x \to g^{-1}xg$ con $g \in G$, con la regola $g^\omega := \omega(g)$, si parlerà di serie normale; gli $\mathrm{Inn}(G)$-sottogruppi sono esattamente i sottogruppi normali;
- se $\Omega = \mathrm{Aut}(G)$ si parlerà di serie caratteristica;
- se $\Omega = \mathrm{End}(G)$ si parlerà di serie pienamente invariante.

Esercizio 52. *Mostrare che per ogni gruppo G si ha un isomorfismo canonico $G/Z(G) \cong \mathrm{Inn}(G)$ [Suggerimento: considerare l'azione di coniugio di G in sé].*

Due Ω-serie S, T di un Ω-gruppo G si dicono Ω-isomorfe se esiste una biiezione tra l'insieme dei fattori di S e l'insieme dei fattori di T tale che fattori corrispondenti sono Ω-isomorfi. Un raffinamento di una Ω-serie S è una Ω-serie T tale che ogni termine di T è anche un termine di S.

Teorema 4 (Jordan-Holder). *Se S è una Ω-serie di composizione e T è una Ω-serie di un Ω-gruppo G allora T ammette un raffinamento che è una serie di composizione Ω-isomorfa a S. In particolare due serie di composizione di G sono Ω-isomorfe.*

Nel caso $\Omega = \emptyset$, questo teorema dice in pratica che ogni gruppo finito ammette un insieme di ben definiti "fattori semplici", paragonabili ai numeri primi per i numeri naturali. Tuttavia, conoscere i fattori di composizione di un gruppo non è sufficiente per conoscere il gruppo. Per esempio:

Esercizio 53. *: Mostrare che S_3 e C_6 hanno gli stessi fattori di composizione.*

Dato un gruppo G, un suo sottogruppo H si dice centrale se è contenuto nel centro di G. Se $K \leq H \leq G$ e K è normale in G, si dice che H/K è centrale se è contenuto nel centro di G/K.

Definizione 15 (Gruppi nilpotenti). *Un gruppo G si dice nilpotente se ammette una serie normale finita a fattori centrali. La minima lunghezza di una tale serie si dice classe di nilpotenza di G, e si indica con* $\mathrm{cl}(G)$.

Un esempio di serie centrale è la serie $1 = G_0 \trianglelefteq G_1 \trianglelefteq ...$ definita da $G_i/G_{i-1} := Z(G/G_{i-1})$. In questa serie G_i verrà denotato con $\zeta_i G$. Si dimostra che la finitezza di tale serie è equivalente alla nilpotenza di G, e quindi che G è nilpotente se e solo se $\zeta_c G = G$ per qualche intero c.

Lemma 6. *Sia G un gruppo.*

(1) *Se G è nilpotente e semplice allora è ciclico di ordine primo.*
(2) *Se G è nilpotente e non banale allora ha centro non banale.*
(3) *Se G è nilpotente e $1 \neq N \lhd G$ allora $N \cap Z(G) \neq \{1\}$.*
(4) *Se G è nilpotente, un sottogruppo normale minimale di G è centrale.*
(5) *Se G è nilpotente e A è un sottogruppo normale, abeliano di G e massimale con queste proprietà allora $A = C_G(A)$.*
(6) *Un p-gruppo finito è nilpotente.*
(7) *Sottogruppi, immagini e prodotti diretti finiti di gruppi nilpotenti sono nilpotenti.*

Dimostrazione.

(1) Dato che G è nilpotente e semplice la sola serie normale possibile, cioè $1 \trianglelefteq G$, dev'essere centrale, ovvero $G \subseteq Z(G)$, in altre parole G è abeliano. Essendo G semplice ed abeliano non ammette sottogruppi propri e quindi è ciclico, finito di ordine primo.
(2) Se $Z(G) = 1$ allora non esistono serie centrali finite, dato che il primo fattore dev'essere 1.
(3) Sappiamo che $\zeta_c G = G$ per qualche intero c, e quindi $N \cap \zeta_i G \neq 1$ per qualche intero i; scegliamolo minimale con questa proprietà. Ora siccome $\zeta_i G$ commuta con G modulo $\zeta_{i-1}G$, si ha $[\zeta_i G, G] \leq \zeta_{i-1}G$, e quindi $[N \cap \zeta_i G, G] \leq N \cap \zeta_{i-1}G = 1$, in altre parole $N \cap \zeta_i G \leq Z(G) = \zeta_1 G$. Dato che $N \cap \zeta_i G \neq 1$, abbiamo finito.
(4) Segue dal precedente osservando che $N \cap Z(G)$ è un sottogruppo normale di G contenuto in N.
(5) Poiché A è abeliano, $A \leq C := C_G(A)$. Se per assurdo $A \neq C$ allora C/A è un sottogruppo normale non banale di G/A che è nilpotente, e quindi esiste $xA \in (C/A) \cap \zeta(G/A)$ con $x \notin A$. Ora $\langle x, A\rangle$ è abeliano e normale in G dato che $\langle x, A\rangle/A \leq \zeta(G/A)$.
(6) Se G è un p-gruppo finito di ordine > 1 allora per quanto visto sui p-gruppi finiti $Z(G) \neq \{1\}$, quindi per ipotesi induttiva possiamo supporre che $G/Z(G)$ sia nilpotente. L'anti-immagine di una serie centrale di $G/Z(G)$ tramite la proiezione $G \to G/Z(G)$ costituisce una serie centrale di G.
(7) Abbreviamo con SNFC la dicitura "serie normale finita a fattori centrali". L'intersezione dei componenti una SNFC di un gruppo nilpotente G con un sottogruppo H è una SNFC di H. L'immagine di una SNFC di un gruppo nilpotente G tramite un omomorfismo suriettivo $G \to H$ è una SNFC di H. Se G e H sono nilpotenti allora per ottenere una SNFC di $G \times H$ basta fare il prodotto diretto ordinatamente dei componenti di una SNFC di G e una SNFC di H.

□

Proposizione 5. *Sia G un gruppo finito. Le seguenti asserzioni sono equivalenti:*

(1) *G è nilpotente.*
(2) *Ogni sottogruppo massimale di G è normale.*
(3) *G è il prodotto diretto dei suoi sottogruppi di Sylow.*

Dimostrazione. (1) $\Rightarrow$ (2). Supponiamo G nilpotente, e sia $1 = N_0 \lhd N_1 \lhd ... \lhd N_l = G$ una sua serie centrale. Se H è un sottogruppo massimale di G allora esiste un $0 \leq i < l$ tale che $N_i \leq H$ e $N_{i+1} \not\leq H$. Ne segue che H/N_i è un sottogruppo

massimale di G/N_i, che è nilpotente con serie centrale $1 = N_i/N_i \lhd N_{i+1}/N_i \lhd ... \lhd N_l/N_i = G/N_i$. Possiamo allora supporre $i = 0$. Ora $N_1H = HN_1 = G$ contenendo N_1 elementi che non stanno in H, e quindi i coniugati di H sono relativi ad elementi di N_1, che è centrale. Ne segue che i coniugati di H coincidono con H, e quindi H è normale.

(2) $\Rightarrow$ (3). Supponiamo che ogni sottogruppo massimale di G sia normale. Dobbiamo mostrare che G è il prodotto diretto dei suoi sottogruppi di Sylow, e per questo basterà mostrare che ogni sottogruppo di Sylow è normale, dato che in tal caso il loro prodotto è diretto (il loro ordine è coprimo) e deve coincidere con G per questioni di cardinalità. Sia allora per assurdo P un p-Sylow non normale di G. Allora $N_G(P) \neq G$ e quindi esiste $M \leq G$ massimale - e quindi normale - tale che $P \leq N_G(P) \leq M$. Ora se $g \in G - M$ (che esiste perché M è proprio) allora $g^{-1}Pg$ è un p-Sylow di G contenuto in M, quindi è un p-Sylow di M e $g^{-1}Pg = m^{-1}Pm$ per qualche $m \in M$. Ma allora $gm^{-1} \in N_G(P) \leq M$, ovvero $g \in M$, assurdo.

(3) $\Rightarrow$ (1). I p-gruppi finiti sono nilpotenti e quindi lo sono anche i loro prodotti diretti finiti. □

Segue che un gruppo nilpotente finito è esattamente un prodotto diretto finito di p-gruppi finiti.

7. Sottogruppi normali minimali

Sia G un gruppo. Un sottogruppo normale minimale di G è un sottogruppo normale $N \neq 1$ di G che non contiene propriamente sottogruppi normali non banali di G. Se G è finito esiste almeno un sottogruppo normale minimale di G: un qualunque sottogruppo normale di ordine minimo. Per la stessa ragione ogni sottogruppo normale di un gruppo finito ne contiene uno minimale.

Un sottogruppo sub-normale di G è un sottogruppo H di G tale che esistono dei sottogruppi $N_0, ..., N_t$ di G tali che

$$H = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_t = G.$$

Un sottogruppo sub-normale minimale di G è un sottogruppo sub-normale non banale di G che non contiene propriamente sottogruppi sub-normali non banali di G. È chiaro che un sottogruppo sub-normale minimale di G è semplice: per questo basta osservare che ogni sottogruppo normale è sub-normale e che la relazione di sub-normalità è transitiva.

Un sottogruppo H di un gruppo G si dice **caratteristico** se per ogni automorfismo ϕ di G si ha $\phi(H) \subseteq H$, ovvero $\phi(H) = H$.

Esercizio 54. *: Mostrare che ogni sottogruppo di un gruppo ciclico finito è caratteristico.*

Esercizio 55. *Mostrare che se un gruppo finito G ammette un solo p-Sylow, allora tale p-Sylow è caratteristico.*

Lemma 7. *Se $K \leq H \leq G$, K è caratteristico in H e H è normale in G allora K è normale in G.*

Dimostrazione. Basta osservare che se $g \in G$ allora il coniugio tramite g è un automorfismo di H. □

Sia $\mathrm{soc}(G)$ (lo zoccolo di G) il sottogruppo di G generato dai sottogruppi normali minimali di G.

Esercizio 56. *Mostrare che* $\mathrm{soc}(G)$ *è il prodotto diretto interno dei sottogruppi normali minimali di* G*.*

Esercizio 57. *Mostrare che* $\mathrm{soc}(G)$ *è un sottogruppo caratteristico di* G*, in particolare normale.*

Proposizione 6. *Sia* G *un gruppo finito e sia* S *un sottogruppo sub-normale di* G*. Allora* $\mathrm{soc}(G) \leq N_G(S)$*.*

Dimostrazione. Procediamo per induzione sull'ordine $|G|$. Possiamo supporre che $S \neq G$. Allora esiste un sottogruppo normale N di G tale che $N \neq G$ e S è sub-normale in N. Sia M un sottogruppo normale minimale di G: dobbiamo mostrare che M centralizza S in G. Possiamo supporre $N \cap M \neq 1$ perchè altrimenti M centralizza N e quindi banalmente normalizza S. Ma dire $N \cap M \neq 1$ significa dire $M \leq N$, perché M è normale minimale. Siccome M è normale in G e contenuto in N esso contiene un sottogruppo normale minimale di N e quindi $M \cap \mathrm{soc}(N) \neq 1$. Ora $\mathrm{soc}(N)$ è caratteristico in N e N è normale in G, quindi $\mathrm{soc}(N) \trianglelefteq G$ (lemma 7), e quindi $M \leq \mathrm{soc}(N)$ per minimalità di M. Per ipotesi induttiva $\mathrm{soc}(N)$ normalizza S, quindi anche M normalizza S. □

Possiamo ora dimostrare il teorema di struttura per i sottogruppi normali minimali di un gruppo finito.

Teorema 5. *Sia* G *un gruppo finito. I sottogruppi normali minimali di* G *sono del tipo* $N = \prod_{g \in G} S^g$ *dove* S *è un sottogruppo sub-normale minimale di* G*.*

Dimostrazione. Sia N un sottogruppo normale minimale di G, e sia S un sottogruppo sub-normale minimale di G contenuto in N (tale S esiste perché G è finito). Per la proposizione 6 S è un sottogruppo normale minimale di N. Osserviamo inoltre che se $g \in G$ allora S^g è normale in N, infatti se $n \in N$ allora $(S^g)^n = S^{gn} = S^{(gng^{-1})g} = S^g$ poiché $gng^{-1} \in N$ e $S \trianglelefteq N$. Segue che se $S^g \neq S^h$ allora $S^g \cap S^h = 1$ (S^g è semplice, e $S^g \cap S^h \trianglelefteq S^g$), quindi il sottogruppo generato dai coniugati di S è il loro prodotto diretto interno (infatti commutano a due a due, dovendo essere $[S^g, S^h] \subseteq S^g \cap S^h$ in N). Inoltre tale sottogruppo è contenuto in N perché N è normale in G, ed è normale in G perché il coniugio permuta i coniugati di S; siccome N è normale minimale in G, si deve allora avere $N = \prod_{g \in G} S^g$. □

8. Gruppi risolubili

Un gruppo G si dice risolubile se ammette una serie finita a fattori abeliani, del tipo

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_t = G.$$

In altre parole ogni quoziente N_i/N_{i-1} è abeliano. Il numero t viene detto lunghezza della serie. La minima lunghezza di una tale serie si dice lunghezza derivata di G.

Esercizio 58. *Mostrare che ogni gruppo nilpotente è risolubile.*

Sia G' il sottogruppo derivato di G, ovvero quello generato dai commutatori, gli elementi di G della forma $[a, b] := a^{-1}b^{-1}ab$ con $a, b \in G$. Allora la serie $G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq ...$ è a fattori abeliani. Si dimostra che G è risolubile se e solo se la serie $G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq ...$ è finita, cioè esiste un intero n tale che $G^{(n)} = 1$ (dove $G^{(n)}$ è definito per ricorsione tramite $G^{(0)} = G$ e $G^{(n+1)} = (G^{(n)})'$). Inoltre la lunghezza derivata di G è esattamente il minimo intero n che verifica $G^{(n)} = 1$.

ESERCIZIO 59. *G' è un sottogruppo caratteristico di G, in particolare normale.*

ESERCIZIO 60. *Se $N \trianglelefteq G$ allora G/N è abeliano se e solo se $G' \leq N$.*

ESERCIZIO 61. *Se $N \trianglelefteq G$ e i gruppi N e G/N sono risolubili allora G è risolubile.*

Se G è un gruppo, un "**fattore di composizione**" di G è H/K dove H e K sono sottogruppi sub-normali di G, $K \trianglelefteq H$ e H/K è semplice. H/K è un "**fattore principale**" di G se $K \trianglelefteq G$ e H/K è un sottogruppo normale minimale di G/K.

LEMMA 8 (Legge modulare di Dedekind). *Siano H, K, L tre sottogruppi di un gruppo G con $K \subseteq H$ e $L \trianglelefteq G$. Allora $(H \cap L)K = H \cap KL$.*

DIMOSTRAZIONE. L'inclusione $\subseteq$ segue dal fatto che $H \cap L \subseteq H \cap KL$ e $K \subseteq H \cap KL$. Sia ora $h = lk \in H \cap KL$, con $k \in K$ e $l \in L$ (possiamo scrivere un elemento di KL nella forma lk perché L è normale in G). Allora $l = k^{-1}h \in H \cap L$. □

LEMMA 9. *Siano G un gruppo, A un suo sottogruppo normale e abeliano, H un supplemento di A in G. Allora H è massimale se e solo se $A/H \cap A$ è un fattore principale di G. Inoltre in questo caso $[G : H] = [A : H \cap A]$.*

DIMOSTRAZIONE. Osserviamo che $H \cap A \trianglelefteq H$ perché A è normale in G, e $H \cap A \trianglelefteq A$ perché A è abeliano, quindi $H \cap A \trianglelefteq G$ essendo $HA = G$. Supponiamo H massimale, e sia $L \trianglelefteq G$ tale che $H \cap A < L \leq A$. Basta allora mostrare che $A = L$. Si ha che $G = HL$ perché $L \not\leq H$, quindi $A = (HL) \cap A = (H \cap A)L = L$ per la legge modulare di Dedekind. Viceversa supponiamo che $A/H \cap A$ sia un fattore principale di G, e sia $H < K \leq G$; basta così mostrare che $K = G$. Si ha che $K = K \cap (HA) = H(K \cap A) > H$, quindi $H \cap A < K \cap A \trianglelefteq G$ ($K \cap A$ è normale in G perché normalizzato da H e da A), quindi $A = K \cap A$, cioè $A \leq K$. Segue $G = K$ dato che $G = HA \leq K$. □

PROPOSIZIONE 7. *Sia G un gruppo risolubile finito.*

1. *Ogni fattore di composizione di G ha ordine primo.*
2. *Ogni fattore principale di G è un p-gruppo abeliano elementare per qualche primo p.*
3. *L'indice di ogni sottogruppo massimale di G è una potenza di un primo.*

DIMOSTRAZIONE.

1. Sia H/K un fattore di composizione di G. Allora H in quanto sottogruppo di G è risolubile, e H/K in quanto quoziente di H è risolubile. Ne segue che H/K è risolubile e semplice, quindi è abeliano e quindi è ciclico di ordine primo.
2. Dato che la risolubilità è stabile per passaggio al quoziente, basta mostrare che i sottogruppi normali minimali di G sono p-gruppi abeliani elementari per qualche primo p. Ma nella sezione 7 abbiamo visto che un sottogruppo normale minimale N è il prodotto dei coniugati di un sottogruppo sub-normale minimale S, e un sottogruppo sub-normale minimale di G è semplice e risolubile, quindi ciclico di ordine p primo: $S \cong C_p$. Segue che $N = \prod_{g \in G} S^g \cong C_p{}^{[G:N_G(S)]}$ è un p-gruppo abeliano elementare.
3. Sia M un sottogruppo massimale di G. Possiamo supporre che M contenga $\mathrm{soc}(G)$, perché in caso contrario esiste un sottogruppo normale minimale N non contenuto in M, da cui $G = MN$ e $G/N = MN/N \cong$

$M/M \cap N$, quindi

$$[G : M] = \frac{|G|}{|M|} = \frac{|G|}{|G||M \cap N|/|N|} = \frac{|N|}{|N \cap M|}$$

è una potenza di un primo perché $|N|$ lo è. Procediamo per induzione su $|G|$. Dato che $1 \neq \mathrm{soc}(G) \subseteq M$, si ha che $[G : M] = [G/\mathrm{soc}(G) : M/\mathrm{soc}(G)]$ per ipotesi induttiva è una potenza di un primo.

□

Attenzione: se G è un gruppo nilpotente (in particolare risolubile), in generale la sua classe di nilpotenza e la sua lunghezza derivata sono due numeri distinti. Esistono gruppi con lunghezza derivata 2 e classe di nilpotenza arbitrariamente grande. Nel seguito faremo un esempio di un tale gruppo.

Intanto diamo una nuova caratterizzazione dei gruppi nilpotenti. Dato un gruppo G e due suoi sottogruppi H, K definiamo

$$[H, K] := \langle \{[h, k] \mid h \in H,\ k \in K\} \rangle.$$

Per esempio $[G, G] = G'$.

Rimarchiamo qualche utile proprietà dei commutatori. Siano x, y, z elementi di G, siano H, K sottogruppi di G.

- $[x, y]^{-1} = [y, x]$.
- $[xy, z] = [x, z]^y [y, z]$.
- $[z, xy] = [z, y][z, x]^y$.
- $N \leq G$ è normale in G se e solo se $[N, G] \subseteq N$.
- H e K commutano modulo $N \trianglelefteq G$ se e solo se $[H, K] \subseteq N$.

La seconda proprietà elencata dice che fare il commutatore con z a destra è un 1-cociclo (si veda più avanti per la definizione di 1-cociclo). Questo implica in modo immediato che H e K normalizzano $[H, K]$: si tratta di usare la seconda proprietà con $x \in H$, $z \in K$ e y in uno tra H e K.

Dato G, definiamo una catena di sottogruppi di G come segue: $G^1 := G$, $G^{n+1} := [G^n, G]$. La catena

$$G = G^1 \trianglerighteq G^2 \trianglerighteq ... \trianglerighteq G^n \trianglerighteq ...$$

è una serie centrale. Abbiamo il seguente risultato:

Proposizione 8. *Un gruppo finito G è nilpotente se e solo se esiste $n \in \mathbb{N}$ tale che $G^n = 1$. In questo caso la classe di nilpotenza di G coincide col più piccolo intero r tale che $G^{r+1} = 1$.*

Dimostrazione. Posposta. □

Per esempio, un gruppo G è nilpotente con classe di nilpotenza 2 se e solo se $G' \subseteq Z(G)$ (ovvio, dato che $G^2 = [G, G] = G'$). In questo caso se $x, y \in G$ si ha $(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}$.

Dimostrazione. Per induzione: ricordando che i commutatori stanno nel centro abbiamo

$$x^2 y^2 [y, x] = x^2 y x^{-1} y x = x[x, y] y^2 x = x y^2 x [x, y] = xyxy = (xy)^2.$$

Supponiamo di aver dimostrato il risultato per $n - 1$. Allora ricordando che l'operazione di commutazione $(x, y) \mapsto [x, y]$ è bilineare, nel senso che $[xz, y] = [x, y][z, y]$

e $[x, yz] = [x, y][x, z]$ (per la seconda proprietà di cui sopra, ricordando che in questo caso i commutatori sono nel centro), si ha:

$$\begin{aligned}(xy)^n &= (xy)^{n-1}xy = x^{n-1}y^{n-1}[y,x]^{\binom{n-1}{2}}xy = \\ &= x^{n-1}y^{n-1}xy[y,x]^{\binom{n-1}{2}} = x^{n-1}xy^{n-1}[y^{n-1},x]y[y,x]^{\binom{n-1}{2}} = \\ &= x^n y^n [y,x]^{n-1}[y,x]^{\binom{n-1}{2}} = x^n y^n [y,x]^{\binom{n}{2}}.\end{aligned}$$

□

Sia ora G un p-gruppo, con $|G| = p^n$. Allora $\mathrm{cl}(G) \leq n$, perché i centri successivi male che vada hanno ordine p. In realtà possiamo dire meglio. Nel seguito sia $n > 1$.

LEMMA 10. $|G^1/G^2| \geq p^2$. *In particolare* $\mathrm{cl}(G) \leq n - 1$.

DIMOSTRAZIONE. Supponiamo per assurdo che $|G^1/G^2| = p$. Siano $\overline{G} := G/G^3$ e $\overline{Z} := G^2/G^3$. Allora $\overline{Z} \subseteq Z(\overline{G})$. Sia $g \in \overline{G} - \overline{Z}$. Allora g ha ordine p modulo G^2, quindi $\overline{G} = \overline{Z}\langle\overline{g}\rangle$, quindi $\overline{G}$ è abeliano, cioè $G^3 = G^2$. Quindi siccome G è nilpotente si deve avere $G^2 = 1$, cioè $G' = 1$. Ma allora

$$p^n = |G| = |G/G'| = |G^1/G^2| = p,$$

contraddizione. □

Facciamo ora un esempio di un p-gruppo G di lunghezza derivata 2 e classe di nilpotenza p. Sia $H = \langle g\rangle \cong C_p$, e sia $K = \langle\sigma\rangle \cong C_p \leq \mathrm{Sym}(p)$, con $\sigma = (1\ ...\ p)$. Consideriamo il prodotto semidiretto $G := H^p \rtimes K$ con l'azione di σ che fa slittare ogni componente di uno a destra. In questo modo $|G| = p^{p+1}$, quindi $\mathrm{cl}(G) \leq p$. D'altra parte la lunghezza derivata di G è 2 (ricordiamo infatti che se $N \trianglelefteq G$ allora $l(G) \leq l(N) + l(G/N)$). Mostrare che $G^p \neq 1$ è sufficiente per dedurre che $\mathrm{cl}(G) = p$. Sia allora $x := (g, 1, ..., 1) \in N = H^p$. È un facile conto dimostrare che allora l'elemento

$$[x, \sigma, \sigma, ..., \sigma]$$

ha g nell'ultima posizione quando i σ sono al più $p - 1$. In particolare questo vale se i σ sono $p - 1$, da cui quello che vogliamo.

8.1. Gruppi di ordine p^3. Classifichiamo i gruppi di ordine p^3. Sia G un gruppo di ordine p^3. Se G è abeliano allora il teorema di struttura dei gruppi abeliani finiti implica che G è isomorfo ad uno dei seguenti tre gruppi: C_{p^3}, $C_{p^2} \times C_p$, $C_p \times C_p \times C_p$.

Supponiamo ora G non abeliano. G è nilpotente e come abbiamo visto G^1/G^2 ha ordine $\geq p^2$, per cui $|G^1/G^2| = p^2$ perché $G^2 = G' \neq 1$. Segue che l'indice di nilpotenza di G è 2, quindi se $x, y \in G$ abbiamo che $(xy)^p = x^p y^p [y,x]^{\binom{p}{2}}$.

Supponiamo $p \neq 2$. Distinguiamo due casi.

(1) G contiene un elemento a di ordine p^2. Allora $\langle a\rangle \lhd G$. Esiste un complemento di $\langle a\rangle$? Sia b un elemento di G non appartenente a $\langle a\rangle$. Se b ha ordine p allora $\langle b\rangle$ complementa $\langle a\rangle$. Supponiamo che b abbia ordine p^2. L'intersezione $\langle a\rangle \cap \langle b\rangle$ è un gruppo ciclico $\langle c\rangle$ di ordine p, e possiamo scegliere a e b in modo che $a^p = c = b^p$. Allora $(ab^{-1})^p = a^p (b^{-1})^p [b,a]^{\binom{p}{2}} = c \cdot c^{-1}[b,a]^{\binom{p}{2}} = [b,a]^{\binom{p}{2}}$. Ora siccome $p \neq 2$, si ha che p divide $\binom{p}{2}$ e quindi $[b,a]^{\binom{p}{2}} = 1$ dato che $[b,a] \in G^2$ e G^2 è

ciclico di ordine p. Ne segue che ab^{-1} è un elemento di ordine p che non sta in $\langle a\rangle$, quindi $\langle ab^{-1}\rangle$ complementa $\langle a\rangle$.

Abbiamo dimostrato che esiste $x \in G$ tale che $\langle x\rangle$ complementa $\langle a\rangle$ in G, ovvero $G = \langle a\rangle \rtimes \langle x\rangle$. Ricordiamo che $|a| = p^2$ e $|x| = p$. Ora $A := \mathrm{Aut}(\langle a\rangle) \cong \mathrm{Aut}(C_{p^2}) \cong C_{p^2-p}$ ha esattamente un p-Sylow, quindi $\langle x\rangle$ è il p-Sylow di A, e $a^x = a^{1+p}$. Conosciamo l'azione di x su $\langle a\rangle$, quindi conosciamo il prodotto semidiretto $\langle a\rangle \rtimes \langle x\rangle$.

(2) Ogni elemento non banale di G ha ordine p. Sia N un sottogruppo normale massimale di G. Allora $|N| = p^2$ a meno che ogni sottogruppo normale non banale e proprio di G sia ciclico di ordine p, ma in questo caso G dev'essere monolitico (non appena ammette due sottogruppi normali di ordine p il loro prodotto è normale di ordine p^2) e questo è assurdo perché G/N ha ordine p^2 quindi deve ammettere sottogruppi normali propri non banali. Segue che N ha ordine p^2 ed ogni suo elemento ha ordine p, quindi $N \cong C_p \times C_p$. Ora è chiaro che se $x \in G - N$ allora $\langle x\rangle$ è un complemento di N, quindi $G = N \rtimes \langle x\rangle$, e l'azione di $\langle x\rangle$ è fedele altrimenti sarebbe banale e G risulterebbe abeliano. $\langle x\rangle$ è quindi un p-Sylow di $\mathrm{Aut}(N) \cong GL(2,p)$, dato che l'ordine di $GL(2,p)$ è $p(p-1)^2(p+1)$ e x ha ordine p. Quindi a meno di passare ad un coniugato di $\langle x\rangle$ in $GL(2,p)$ (cioè a meno di cambiare base di riferimento dello spazio vettoriale $C_p \times C_p = {\mathbb{F}_p}^2$) possiamo scrivere

$$G \cong (C_p \times C_p) \rtimes \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle.$$

Supponiamo $p = 2$. Allora esiste in G un elemento a di ordine 4 perché se tutti gli elementi non banali di G avessero ordine 2 allora G sarebbe abeliano (esercizio). Se esiste un complemento $\langle b\rangle$ di $\langle a\rangle$ in G allora b ha ordine 2 e siccome $\mathrm{Aut}(\langle a\rangle) \cong C_2$ l'azione di b su a è l'inversione (al solito a non può essere centrale altrimenti G sarebbe abeliano), da cui segue subito che $G \cong D_8$, il gruppo diedrale di ordine 8.

Esiste un gruppo G di ordine 8 con un sottogruppo normale, ciclico di ordine 4 e non complementato? Sì, ne esiste esattamente uno a meno di isomorfismi, è il gruppo dei quaternioni. Si tratta del sottogruppo di $GL(2,\mathbb{C})$ generato dagli elementi

$$a := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad b := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Questo gruppo si denota con Q_8. $\langle a\rangle$, $\langle b\rangle$, $\langle ab\rangle$ sono massimali e quindi normali (Q_8 è un 2-gruppo), e $\langle -1\rangle$ è il centro. Non ci sono altri sottogruppi non banali, quindi in Q_8 ogni sottogruppo è normale, e Q_8 non è abeliano (per esempio $ab = -ba$).

9. Sottogruppi notevoli

Definizione 16 (Sottogruppo di Frattini). *Sia G un gruppo. Il sottogruppo di Frattini di G è l'intersezione dei sottogruppi massimali di G, e viene indicato con $\Phi(G)$.*

Osserviamo che $\Phi(G)$ non è supplementato, in quanto se $H < G$ allora H è contenuto in un qualche sottogruppo massimale M e quindi $\Phi(G)H \leq M$.

Proposizione 9 (Argomento di Frattini). *Siano G un gruppo finito, N un suo sottogruppo normale, P un p-sottogruppo di Sylow di N. Allora $N_G(P)$ supplementa N in G.*

DIMOSTRAZIONE. Dato $g \in G$, il coniugato P^g di P è un p-sottogruppo di Sylow di N, quindi esiste $n \in N$ tale che $P^g = P^h$, ovvero $gn^{-1} \in N_G(P)$. Ma allora $g \in N_G(P)n \subseteq N_G(P)N$. □

Il sottogruppo di Frattini di un gruppo finito è nilpotente (si vedano gli esercizi).

DEFINIZIONE 17 (Sottogruppo di Fitting). *Sia G un gruppo finito. Per ogni divisore primo p di $|G|$ definiamo $O_p(G)$ come l'intersezione dei p-sottogruppi di Sylow di G. Si tratta di sottogruppi caratteristici di G. Il sottogruppo di Fitting di G (denotato con $F(G)$) è il prodotto diretto interno degli $O_p(G)$.*

Osserviamo che $F(G)$ è nilpotente in quanto gli $O_p(G)$ sono normali in $F(G)$, e sono i suoi p-sottogruppi di Sylow. In realtà, $F(G)$ è il "più grande" sottogruppo normale nilpotente di G:

PROPOSIZIONE 10. *Siano G un gruppo finito, N un suo sottogruppo normale nilpotente. Allora $N \leq F(G)$.*

DIMOSTRAZIONE. Poiché N è nilpotente, basta mostrare che ogni p-sottogruppo di Sylow di N è contenuto in $F(G)$. Sia P un p-Sylow di N. Allora P è caratteristico in N e N è normale in G, quindi $P \trianglelefteq G$ e quindi, dato un p-Sylow Q di G contenente P, si ha $P = P^g \subseteq Q^g$ per ogni $g \in G$. Siccome i p-Sylow di G sono a due a due coniugati, si ottiene che $P \subseteq O_p(G) \subseteq F(G)$. □

9.1. Fattori principali di Frattini. Osserviamo che un sottogruppo normale minimale di G è in particolare un fattore principale di G. Diciamo che un fattore principale H/K di G è "Frattini" (o "di Frattini") se $H/K \subseteq \Phi(G/K)$. In caso contrario H/K si dice "non-Frattini".

OSSERVAZIONE 1. *Siano G un gruppo ed N un suo sottogruppo normale minimale abeliano. Allora i supplementi di N in G sono complementi.*

DIMOSTRAZIONE. Sia M un supplemento di N in G. Allora $M \cap N$ è un sottogruppo normale di N (perché N è abeliano) e di M (perché N è normale) e quindi di G essendo $G = MN$. Siccome N non è contenuto in M ed è normale minimale si ottiene $M \cap N = 1$. □

PROPOSIZIONE 11. *Se N è un sottogruppo normale minimale di un gruppo finito G, si hanno i seguenti fatti:*

1. *Se N è Frattini allora è abeliano.*
2. *Se N è abeliano allora è complementato se e solo se è non-Frattini.*

DIMOSTRAZIONE.

1. Il Frattini in quanto nilpotente non può contenere sottogruppi semplici non abeliani.
2. Se N è non-Frattini allora esiste un massimale che non lo contiene, quindi lo supplementa, quindi lo complementa (per l'osservazione 1); viceversa se N è complementato allora ogni suo complemento è massimale (per il lemma 9) e non lo contiene.

□

10. Estensioni di gruppi

Dati due gruppi H e K e un omomorfismo $K \to \mathrm{Aut}(H)$, esiste un gruppo G che ammetta un sottogruppo normale N tale che $N \cong H$ e $G/N \cong K$, e l'azione di K su N corrisponda all'azione di coniugio in G? Tale G si dice estensione di N tramite K. Come dev'essere fatto un tale G?

Osserviamo che se $N \trianglelefteq G$ ammette un complemento H in G allora $|G| = |H| \cdot |N|$ ed ogni elemento $g \in G$ si scrive in modo unico come $g = hn$ con $h \in H$ e $n \in N$. Come si comportano tali componenti di G rispetto al prodotto? Se $h_1 n_1, h_2 n_2 \in G$ con $h_1, h_2 \in H$ e $n_1, n_2 \in N$ si ha

$$(h_1 n_1)(h_2 n_2) = h_1 h_2 {n_1}^{h_2} n_2.$$

Questo suggerisce un'idea per costruire un'estensione di N in cui i complementi di N siano isomorfi ad H: il prodotto semidiretto $N \rtimes H$ relativo ad un dato omomorfismo $H \to \mathrm{Aut}(N)$.

10.1. Il teorema di Schur-Zassenhaus.

Teorema 6 (Schur-Zassenhaus). *Siano G un gruppo finito, N un sottogruppo normale di G tale che*

$$(|N|, [G : N]) = 1.$$

Allora:

1. *N ha un complemento in G.*
2. *Se uno tra N e G/N è risolubile allora due qualsivoglia complementi di N in G sono coniugati.*

Dimostrazione. Osserviamo che sotto l'ipotesi $(|N|, [G : N]) = 1$, un complemento di N in G non è altro che un sottogruppo di G di ordine $[G : N]$.

Trattiamo dapprima il caso in cui N è abeliano. Un 1-cociclo (o "derivazione") è una mappa $\varphi : G \to N$ tale che $\varphi(xy) = \varphi(x)^y \varphi(y)$ per ogni $x, y \in G$. È facile vedere che se $\varphi : G \to N$ è un 1-cociclo allora si ha:

- $\varphi(1) = 1$;
- $K := \{g \in G \mid \varphi(g) = 1\} \leq G$;
- $\varphi(x) = \varphi(y)$ se e solo se $Kx = Ky$;
- $|\varphi(G)| = [G : K]$.

Sia $\mathfrak{T}$ l'insieme di tutti i trasversali di N in G, e siano $S, T \in \mathfrak{T}$. Definiamo

$$d(S, T) := \prod_{s^{-1}t \in N} s^{-1}t \in N.$$

Allora si ha per $S, T, U \in \mathfrak{T}$:

- $d(S, T)d(T, U) = d(S, U)$;
- $d(S, T)^g = d(Sg, Tg)$;
- $d(S, Sn) = n^{[G:N]}$ per ogni $n \in N$.

Osserviamo che per dimostrare la prima di queste ultime tre proprietà si deve usare il fatto che N è abeliano.

Ora fissiamo $T \in \mathfrak{T}$, e definiamo $\vartheta : G \to N$ tramite la posizione $\vartheta(g) := d(T, Tg)$. Le proprietà elencate implicano che ϑ è un 1-cociclo suriettivo. Infatti:

$$\begin{aligned} \vartheta(g_1 g_2) &= d(T, Tg_1 g_2) = d(T, Tg_2) d(Tg_2, Tg_1 g_2) = \\ &= d(T, Tg_1)^{g_2} d(T, Tg_2) = \vartheta(g_1)^{g_2} \vartheta(g_2). \end{aligned}$$

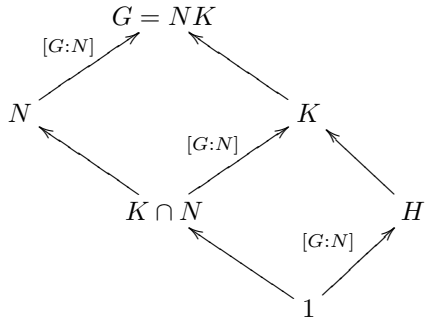
ϑ è suriettivo perché se $n \in N$ allora poiché $(|N|, [G : N]) = 1$, una opportuna potenza di $\vartheta(n) = n^{[G:N]}$ è uguale a n. $H := \{g \in G \mid d(T, Tg) = 1\}$ è un sottogruppo di G. Siccome ϑ è suriettivo, $|N| = |\vartheta(G)| = [G : H]$, cioè $|H|$ è un sottogruppo di G di ordine $[G : N]$, quello che vogliamo.

Sia ora K un altro complemento di N in G. In particolare $K \in \mathfrak{T}$, quindi detto $m := d(K, T)$ esiste $n \in N$ con $\vartheta(n) = m$. Mostriamo che $K^n = H$. Poiché $|K^n| = |H|$, per fare questo è sufficiente mostrare che $K^n \subseteq H$, ovvero $\vartheta(x^n) = 1$ per ogni $x \in K$. Osserviamo che $m^x = d(K, T)^x = d(Kx, Tx) = d(K, Tx) = d(K, T)d(T, Tx) = m \cdot \vartheta(x)$. Quindi

$$\begin{aligned} \vartheta(x^n) &= \vartheta(n^{-1}xn) = \vartheta(n^{-1}x)^n\vartheta(n) = \vartheta(n^{-1}x)m = \\ &= \vartheta(n^{-1})^x\vartheta(x)m = (\vartheta(n)^{-1})^x m\vartheta(x) = (m^x)^{-1}m\vartheta(x) = 1. \end{aligned}$$

Mettiamoci nel caso generale (N non necessariamente abeliano). Procediamo per induzione su $|G|$. Distinguiamo due casi.

(1) Esiste un sottogruppo proprio K di G tale che $KN = G$. Allora $|K \cap N|$ divide $|N|$ e $|K : K \cap N| = [G : N]$. Per ipotesi induttiva esiste un complemento H di $K \cap N$ in K. Si ha il seguente diagramma di inclusioni:



H è allora un sottogruppo di G di ordine $[G : N]$.

(2) $NK \neq G$ per ogni sottogruppo proprio K di G. In particolare N è contenuto in ogni sottogruppo massimale di G, quindi $N \subseteq \Phi(G)$ e N è nilpotente. $Z := Z(N) \neq 1$ è un sottogruppo caratteristico di N, quindi è un sottogruppo normale di G. Possiamo supporre che $Z \neq N$ perché abbiamo già risolto il caso in cui N è abeliano. Ma allora per ipotesi induttiva esiste un complemento H/Z di N/Z in G/Z, cosicché $HN = G$, assurdo.

Per mostrare che nel caso generale i complementi sono a due a due coniugati procediamo per induzione su $|G|$. Siano H, K due complementi di N in G, e sia L un qualunque sottogruppo normale non banale di G. È facile vedere che HL/L è un complemento di NL/L in G/L, quindi per ipotesi induttiva $HL/L = (KL/L)^g$ per qualche $g \in G$. Quindi $HL = (KL)^g = K^gL^g = K^gL$. Sia $X := HL$, cosicché $H, K^g \subseteq X$. Siccome $[X : X \cap N]$ divide $[G : N]$ e $|X \cap N|$ divide $|N|$, si ha per ipotesi che $(|N|, |X \cap N|) = 1$, e H e K^g sono complementi di $X \cap N$ in X. Possiamo quindi supporre per l'ipotesi induttiva che $X = G$. Cioè possiamo supporre che $HL = G$ per ogni sottogruppo normale non banale L di G. In particolare N è un sottogruppo normale minimale di G. Siccome $\mathrm{soc}(N)$ è caratteristico in N, esso è normale in G, quindi $\mathrm{soc}(N) = N$. Segue che se N è risolubile allora è abeliano - caso già trattato - e allora possiamo supporre che N non sia risolubile. Per l'ipotesi

segue allora che G/N è risolubile. Sia M/N un sottogruppo normale minimale di G/N. Allora M/N è un p-gruppo dove p è un primo che non divide $|N|$. Ora $M = M \cap G = M \cap HN = (M \cap H)N$, quindi $M \cap H$ è un p-sottogruppo di Sylow di M. Per la stessa ragione $M \cap K$ è un p-Sylow di M. Quindi $M \cap H$ e $M \cap K$ sono coniugati in M: esiste $m \in M$ tale che $M \cap H = (M \cap K)^m = M \cap K^m = L$. Osserviamo che $X := N_G(L)$ contiene H e K^m. Per ipotesi induttiva possiamo supporre che $X = G$, e L è normale in G. Ma allora $HL = G$. Questo contraddice il fatto che $L \subseteq H$, dato che $H \neq G$. □

Osserviamo una cosa importante: l'ipotesi che si fa nel secondo punto del teorema di Schur-Zassenhaus (che almeno uno tra N e G/N sia risolubile) è automaticamente verificata in virtù del teorema di Feit-Thompson (si vedano gli esercizi).

11. "Inversione" del teorema di Lagrange e teoria di Hall

Sia G un gruppo finito di ordine n, e sia m un divisore di n. Domanda: è vero che esiste sempre un sottogruppo di ordine m?

- La teoria di Sylow ci dice che la risposta è sì se m è una potenza di un primo.
- La risposta è sì se G è nilpotente (perché prodotto diretto di p-gruppi).
- Il più piccolo caso interessante è $n = 12$ (il primo intero che non è una potenza di un primo e che è diviso da un quadrato). A_4 è un gruppo di ordine 12 che non contiene sottogruppi di ordine 6 (si vedano gli esercizi).

Sia π un insieme di numeri primi. Un numero n si dice un π-numero se ogni divisore primo di n appartiene a π. Indichiamo con π' l'insieme dei primi fuori da π. Sia G un gruppo finito. Un sottogruppo H di G si dice un π-sottogruppo di Hall (o π-Hall) se $|H|$ è un π-numero e $[G : H]$ è un π'-numero.

Osservazione: in generale non esistono π-sottogruppi di Hall. Per esempio siano $G = A_5$, $\pi = \{3, 5\}$. Allora un π-Hall H di G se esistesse avrebbe ordine 15, cioè indice 4. Ma siccome G è semplice, $H_G = \{1\}$ e quindi $G = G/H_G$ si immergerebbe in $\mathrm{Sym}(\{Hg \mid g \in G\}) = S_4$, assurdo dato che $|S_4| = 24$.

Abbiamo invece un comportamento molto buono nel caso risolubile.

Teorema 7. *Sia G un gruppo risolubile finito, e sia π un insieme di primi. Allora:*

1. *G contiene π-sottogruppi di Hall.*
2. *Due qualsivoglia π-sottogruppi di Hall di G sono coniugati.*

Dimostrazione. Proviamo il primo punto per induzione sull'ordine di G. Sia N un sottogruppo normale minimale di G. Allora dato che G è risolubile, N è un p-gruppo abeliano elementare per un opportuno primo p. Per ipotesi induttiva G/N contiene un π-sottogruppo di Hall H/N. Se $p \in \pi$ allora H è un π-Hall di G; altrimenti $p \in \pi'$ e quindi per il teorema di Schur-Zassenhaus N ha un complemento in H, sia esso K. Allora $[G : K] = [G : H] \cdot |N|$ è un π'-numero, quindi K è un π-Hall di G.

Proviamo anche il secondo punto per induzione sull'ordine di G. Siano H, K due π-Hall di G, e sia N un sottogruppo normale minimale di G. Allora HN/N e KN/N sono π-Hall di G/N, quindi esiste $g \in G$ tale che $(HN/N) = (KN/N)^g$, da cui $HN = (KN)^g$. Come prima, N è un p-gruppo. Se $p \in \pi$ allora $HN = H$

e $KN = K$, quindi abbiamo finito. Se $p \in \pi'$ allora $HN = K^g N$ e H, K^g sono complementi di N in HN. Quindi per il teorema di Schur-Zassenhaus, H e K^g sono coniugati, e quindi anche H e K lo sono. □

11.1. Applicazione: i gruppi di ordine 2010. Nel seguito mostriamo che a meno di isomorfismi i gruppi di ordine 2010 sono dodici.

LEMMA 11. *C'è un unico gruppo di ordine* 15 *a meno di isomorfismi, quello ciclico. Si ha* $\mathrm{Aut}(C_{15}) \cong C_4 \times C_2$.

DIMOSTRAZIONE. Se G è un gruppo di ordine 15 allora per i teoremi di Sylow i sottogruppi di Sylow di G sono normali, quindi G è il prodotto diretto di C_3 e C_5 e quindi $G \cong C_{15}$. Per quanto riguarda il gruppo degli automorfismi, basta ricordare che $\mathrm{Aut}(C_{15}) = U(\mathbb{Z}/15\mathbb{Z})$ e fare i conti. □

LEMMA 12. *I gruppi di ordine* 30 *a meno di isomorfismi sono* C_{30}, D_{30}, $D_{10} \times C_3$ *e* $S_3 \times C_5$.

DIMOSTRAZIONE. Ricordiamo che il gruppo diedrale D_{2n} ammette la presentazione

$$D_{2n} = \langle g, h \mid g^n = 1,\ g^h = g^{-1} \rangle.$$

Sia G un gruppo di ordine 30. Allora G è risolubile (un gruppo finito non risolubile deve avere ordine almeno 60, dato che il più piccolo gruppo semplice non abeliano ha ordine 60: basta ragionare sui fattori di composizione). Possiamo quindi usare la teoria di Hall. Esiste un sottogruppo H di G di ordine 15 (un $\{3,5\}$-Hall), cioè indice 2, quindi normale, e $H \cong C_{15}$ (lemma 11). H è complementato (un complemento è generato da un qualsiasi elemento di ordine 2), sia $T = \langle t \rangle$ un complemento. Allora $G = H \rtimes T$ e basta elencare le possibilità per l'omomorfismo $\phi : T \to \mathrm{Aut}(H) \cong C_4 \times C_2$ (vd. lemma 11) per conoscere G. Ci sono 4 possibilità per l'immagine di t in $\mathrm{Aut}(H) \cong C_4 \times C_2$: l'identità o un elemento di ordine 2. Scriviamo $H = \langle h \rangle$. Le possibilità sono:

(1) $\phi(t) = 1$. In tal caso H è centrale e quindi $G \cong C_{30}$.
(2) $\phi(t)(h) = h^{-1}$. In tal caso $G \cong D_{30}$ (basta ricordare la presentazione di D_{2n}).
(3) $\phi(t)(h) = h^4$. In tal caso $\phi(t)$ fissa h^5 e inverte h^3, quindi $G \cong D_{10} \times C_3$.
(4) $\phi(t)(h) = h^{11}$. In tal caso $\phi(t)$ fissa h^3 e inverte h^5, quindi $G \cong S_3 \times C_5$ (ricordo che $D_6 \cong S_3$).

□

Ora preso G di ordine 2010 sappiamo che il 67-Sylow N (ciclico di ordine 67) è normale e complementato da H di ordine 30, quindi $G = N \rtimes H$. Rimane da determinare l'omomorfismo $H \to \mathrm{Aut}(N) \cong C_{66}$, la cui immagine è contenuta in C_6. G è risolubile poiché N e $G//N$ lo sono. Osserviamo che se A e B sono due gruppi finiti il numero di omomorfismi $A \to B$ è uguale al numero di sottogruppi normali C di A tali che A/C è isomorfo ad un sottogruppo di B. Osserviamo che per la teoria di Hall per un gruppo risolubile il cui ordine non ha fattori primi multipli (come il nostro G) esiste al più un sottogruppo normale di un fissato ordine. Si hanno quattro casi.

(1) $H = C_{30}$. Ci sono 4 omomorfismi possibili $C_{30} \to C_6$ (corrispondenti ai quattro sottogruppi di C_{30} di indici $1, 2, 3, 6$).

(2) $H = D_{30}$. Ci sono 2 omomorfismi possibili $D_{30} \to C_6$ (corrispondenti ai sottogruppi di indici 1 e 2), infatti il sottogruppo di D_{30} di indice 3 non è normale e il sottogruppo di indice 6 è normale ma il relativo quoziente non è ciclico (è isomorfo a S_3).
(3) $H = D_{10} \times C_3$. Ci sono 4 omomorfismi possibili $D_{10} \times C_3 \to C_6$ (corrispondenti ai sottogruppi di indici $1, 2, 3, 6$, che sono tutti normali di quoziente ciclico).
(4) $H = S_3 \times C_5$. Ci sono 2 omomorfismi possibili $S_3 \times C_5 \to C_6$ (corrispondenti ai sottogruppi di indici 1 e 2), infatti il sottogruppo di indice 3 non è normale e il sottogruppo di indice 6 è normale ma il relativo quoziente non è ciclico (è isomorfo a S_3).

In totale quindi i casi possibili sono 12.

12. Gruppi transitivi e primitivi

Nel seguito sia G un gruppo finito. G agisca sull'insieme X, e denotiamo l'azione con $(x, g) \mapsto x^g$. Tale azione si dice transitiva se per ogni $x, y \in X$ esiste $g \in G$ tale che $x^g = y$. Equivalentemente, l'azione ammette una sola orbita. L'azione si dice primitiva se è transitiva e nessuna partizione non banale di X è stabilizzata da G, ovvero per ogni partizione $\mathcal{R}$ di X che non sia banale (le partizioni banali di X sono $\{X\}$ e $\{\{x\} \mid x \in X\}$) e per ogni $g \in G$ si ha

$$\{Rg \mid R \in \mathcal{R}\} \neq \mathcal{R}.$$

Si osservi che se $|X| > 2$ allora la richiesta che l'azione sia transitiva è superflua (e se $|X| = 2$ l'azione banale $x^g = x$ è primitiva), infatti la partizione in orbite è sempre stabilizzata. Se G non è primitivo, gli elementi di una partizione di X non stabilizzata si dicono blocchi di imprimitività.

Si dice che G è transitivo (risp. primitivo) se ammette un'azione fedele transitiva (risp. primitiva) su un certo insieme X. In tal caso la cardinalità di X si chiama grado di transitività (risp. primitività) di G. Si noti che G può avere molti gradi di transitività o di primitività. Per esempio A_5 è primitivo dei seguenti gradi: 5, 6 e 10 (si tratta dei possibili indici dei sottogruppi massimali di A_5). Se n è un grado di transitività (risp. primitività) di G si dice che G è n-transitivo (risp. n-primitivo).

LEMMA 13. *Il gruppo G agisca sull'insieme X, e valga $|X| > 2$. Tale azione non è primitiva se e solo se esiste un sottoinsieme proprio A di X con almeno 2 elementi tale che $Ag = A$ oppure $Ag \cap A = \emptyset$ per ogni $g \in G$.*

DIMOSTRAZIONE. Supponiamo che l'azione non sia primitiva, e sia $\mathcal{R}$ una partizione non banale stabilizzata. Siccome la partizione è non banale, esiste $A \in \mathcal{R}$ tale che $|A| \geq 2$ e $A \neq X$. Dal fatto che la partizione è stabilizzata segue quanto asserito.

Supponiamo che esista A come nell'enunciato. Allora la partizione $\{Ag \mid g \in G\}$ di X è stabilizzata da G. □

Osserviamo che G è 2-primitivo o 2-transitivo se e solo se $|G| = 2$, infatti la fedeltà implica l'esistenza di un omomorfismo iniettivo $G \to S_2$ e la transitività implica che $G \neq \{1\}$.

PROPOSIZIONE 12. *Sia G un gruppo con più di due elementi. G è transitivo (risp. primitivo) se e solo se ammette un sottogruppo (risp. sottogruppo massimale) H con cuore normale identico: $H_G = \{1\}$, e in tal caso l'azione di G per moltiplicazione a destra dei laterali destri di H è transitiva (risp. primitiva). I gradi di transitività (risp. primitività) di G sono gli indici dei sottogruppi (risp. sottogruppi massimali) con cuore normale identico.*

DIMOSTRAZIONE. Proviamo la prima parte.

($\Leftarrow$) Poiché $H_G = \{1\}$, l'azione di G sui laterali destri di H è fedele. È transitiva in quanto se $x, y \in G$ allora Hx viene mandato in Hy moltiplicando a destra per $y^{-1}x$. Supponiamo ora H massimale, e mostriamo che l'azione è primitiva. Per assurdo non lo sia, e consideriamo $A \subseteq X$ come nel lemma 13. A meno di scambiare A con un opportuno Ag possiamo supporre che $H \in A$. Sia $K := \{g \in G \mid Ag = A\}$. È facile vedere che K è un sottogruppo di G contenente H, quindi $K = H$ oppure $K = G$ per massimalità di H.

- Se $K = H$ allora $Ag \cap A = \emptyset$ se $g \in G - H$, quindi $A = \{M\}$, assurdo in quanto $|A| \geq 2$.
- Se $K = G$ allora tutti i laterali destri di H sono contenuti in A, ovvero $A = X$, assurdo in quanto A è un sottoinsieme proprio di X.

($\Rightarrow$) Consideriamo $x \in X$, e sia $H := \mathrm{Stab}_G(x)$. Supponiamo che l'azione sia transitiva. Osserviamo che G agisce sui laterali destri di H per moltiplicazione a destra nello stesso modo in cui agisce su X, nel senso che la funzione

$$\varphi : X \to \{Hg \mid g \in G\}, \qquad x^g \mapsto Hg$$

determina un'equivalenza tra queste due azioni. In altre parole **un gruppo ammette un'azione fedele transitiva di grado d se e solo se ammette un sottogruppo di indice d con cuore normale identico**. Siccome $\mathrm{Stab}_G(x^g) = \mathrm{Stab}_G(x)^g$ se l'azione è transitiva allora l'intersezione dei coniugati di H (cioè il cuore normale di H) coincide con l'intersezione degli stabilizzatori, cioè col nucleo dell'azione, $\{1\}$. Supponiamo ora che G sia primitivo su X. Come appena visto $H = \mathrm{Stab}_G(x)$ ha cuore normale identico; mostriamo che è un sottogruppo massimale. Sia K un sottogruppo di G contenente H. La funzione φ di cui sopra determina un'azione primitiva di G sui laterali destri di H. Siccome G è unione di laterali destri di K, la scrittura di K come unione di laterali destri di H determina una partizione dell'insieme dei laterali destri di H stabilizzata da G, quindi ci sono due casi possibili:

- Tale partizione consiste di ogni laterale destro di H preso singolarmente; ma in tal caso $K = H$.
- Tale partizione consiste del solo insieme dei laterali destri di H; ma in tal caso $K = G$.

Per giustificare l'ultima osservazione dell'asserto basta notare che l'indice di un sottogruppo coincide col numero dei suoi laterali destri. □

Introduciamo ora un po' di terminologia. Il gruppo G agisca sull'insieme X. L'azione si dice semiregolare se $\mathrm{Stab}_G(x) = \{1\}$ per ogni $x \in X$. L'azione si dice regolare se è semiregolare e transitiva.

Osserviamo che se l'azione di G su X è regolare allora l'equazione delle classi dice esattamente che $|G| = |X|$.

LEMMA 14. *Sia G un gruppo primitivo su X, e sia N un sottogruppo normale non banale di G. Allora l'azione indotta di N su X è transitiva.*

DIMOSTRAZIONE. Consideriamo la partizione di X in N-orbite. Essa è stabilizzata da G, quindi se N non è transitivo su X allora ogni N-orbita consiste di un solo elemento. Ma allora $N = \{1\}$ per la fedeltà dell'azione, assurdo. □

LEMMA 15. *Sia G un gruppo primitivo sull'insieme X, e sia H un sottogruppo transitivo di G. Allora $C_G(H)$ è semiregolare.*

DIMOSTRAZIONE. Bisogna mostrare che se $g \in C_G(H)$ fissa un $x_0 \in X$ allora $g = 1$, e per questo basta mostrare che $gx = x$ per ogni $x \in X$ per la fedeltà. Supponiamo che g fissi x_0, cioè $gx_0 = x_0$. Sia $x \in X$ e sia $h \in H$ tale che $hx = x_0$ (esiste per la transitività di H). Allora da $gh = hg$ segue

$$gx = h^{-1}ghx = h^{-1}gx_0 = h^{-1}x_0 = h^{-1}hx = x.$$

□

PROPOSIZIONE 13. *Sia G un gruppo primitivo sull'insieme X. Allora G ammette al più due sottogruppi normali minimali. Se ne ammette due, essi sono non-abeliani.*

DIMOSTRAZIONE. Sia N un sottogruppo normale minimale di G. Se N è abeliano allora $N \subseteq C_G(N)$ quindi $C_G(N)$ è regolare contenendo il sottogruppo transitivo N (lemmi 14 e 15). Ma allora anche N è regolare, dato che se $x \in X$ si ha $\mathrm{Stab}_N(x) \subseteq \mathrm{Stab}_{C_G(N)}(x) = \{1\}$, quindi dall'equazione delle classi si ha $|C_G(N)| = |X| = |N|$ e in particolare $N = C_G(N)$. Se $\overline{N}$ è un altro sottogruppo normale minimale di G allora essendo $[N, \overline{N}] \subseteq N \cap \overline{N} = 1$ (per minimalità) si ha che $\overline{N}$ centralizza N, ovvero $\overline{N} \subseteq C_G(N) = N$. Quindi $\overline{N} = N$ per minimalità, assurdo. Ciò dimostra che se N è abeliano allora esso è il solo sottogruppo normale minimale.

Supponiamo ora N non abeliano. Sia $\overline{N}$ un sottogruppo normale minimale distinto da N. Abbiamo già osservato che $\overline{N}$ è transitivo e centralizza N, quindi coincide con $C_G(N)$. Ne segue che $\mathrm{soc}(G) = N \times C_G(N)$. □

Deduciamo che se G è un gruppo primitivo allora lo zoccolo $\mathrm{soc}(G)$ è di uno dei tipi seguenti:

- (I) un sottogruppo normale minimale abeliano;
- (II) un sottogruppo normale minimale non abeliano;
- (III) il prodotto di due sottogruppi normali minimali non abeliani.

Segue che se lo zoccolo di un gruppo primitivo è abeliano allora ogni sottogruppo massimale con cuore normale identico lo complementa. In particolare un gruppo finito primitivo e risolubile ha come grado una potenza di un primo.

ESERCIZIO 62. *Siano H e K due gruppi finiti non banali. Mostrare che $G := H \times K$ è primitivo se e solo se H e K sono due gruppi semplici non abeliani tra loro isomorfi. In particolare se $G = \prod_{i=1}^{r} H_i$ è primitivo allora $r = 1$ oppure $r = 2$, e in quest'ultimo caso $H_1 \cong H_2$ sono semplici non abeliani.*

Svolgimento: H e K sono due sottogruppi normali di G che si centralizzano a vicenda, quindi sono regolari. In particolare siccome ogni loro sottogruppo normale è un sottogruppo normale di G, esso è transitivo, quindi coincide con H o con K

(perché H e K sono regolari). Ne segue che H e K sono semplici. Dato $x \in X$, $\mathrm{Stab}_G(x)$ è un complemento comune a H e K, quindi $H \cong K$.

Per mostrare il viceversa basta fare uso della seguente proposizione.

PROPOSIZIONE 14. *Sia S un gruppo semplice non abeliano, e sia $G := S \times S$. Ogni sottogruppo massimale M di G è di uno dei tipi seguenti:*

$$S \times K, \qquad K \times S, \qquad \Delta_\alpha := \{(x, x^\alpha) \mid x \in S\},$$

dove K è un sottogruppo massimale di S e $\alpha \in \mathrm{Aut}(S)$.

DIMOSTRAZIONE. Sia M un sottogruppo massimale di $G = S_1 \times S_2 = S \times S$, e supponiamo che non sia del tipo $K \times S$ o $S \times K$ con K sottogruppo massimale di S. Chiamiamo $\pi_1 : G \to S_1$, $\pi_2 : G \to S_2$ le due proiezioni. Siano $M_1 = \pi_1(M)$, $M_2 = \pi_2(M)$. Siccome $M \leq M_1 \times M_2$ e M è massimale e non del tipo $K \times S$ o $S \times K$, si deve avere che $M_1 = M_2 = S$. In altre parole le restrizioni $\pi_1|_M$, $\pi_2|_M$ sono suriettive. Questo implica che

$$H := \{s \in S \mid (1, s) \in M\}$$

è un sottogruppo normale di S, dato che se $g \in S$ esiste $h \in S$ tale che $(h, g) \in M$ (per la suriettività di π_2) e $(1, s^g) = (1, s)^{(h,g)} \in M$. Siccome $1 \times S$ non è contenuto in M, si deve avere $H = \{1\}$. Indichiamo con $\alpha : S \times S$ la funzione che manda s nell'elemento t tale che $(s, t) \in M$ (esso è unico poiché $H = \{1\}$). È facile vedere che $\alpha \in \mathrm{Aut}(S)$.

Per mostrare che Δ_α è effettivamente un sottogruppo massimale di $S \times S$ prendiamo $(x, y) \notin \Delta_\alpha$ e consideriamo $L := \langle \Delta_\alpha, (x, y) \rangle$. Per concludere basta mostrare che $L = S \times S$. L contiene $(x, x^\alpha)(x, y)^{-1} = (1, x^\alpha y^{-1}) \neq (1, 1)$. Poiché $\Delta_\alpha \subseteq L$, le proiezioni $\pi_i|_L$ sono suriettive, quindi $\{s \in S \mid (1, s) \in L\}$ è un sottogruppo normale di S diverso da $\{1\}$, e questo implica che $L \supseteq 1 \times S$. Simmetricamente si ha $L \supseteq S \times 1$, quindi $L = S \times S$. □

È facile vedere che il sottogruppo massimale Δ_α di $S \times S$ ha cuore normale identico.

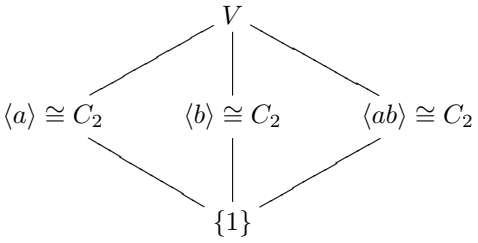
13. Reticolo dei sottogruppi di alcuni gruppi piccoli

Il reticolo dei sottogruppi di un dato gruppo G non è altro che l'insieme dei sottogruppi di G parzialmente ordinato dall'inclusione. In questo paragrafo vedremo i reticoli di alcuni gruppi piccoli.

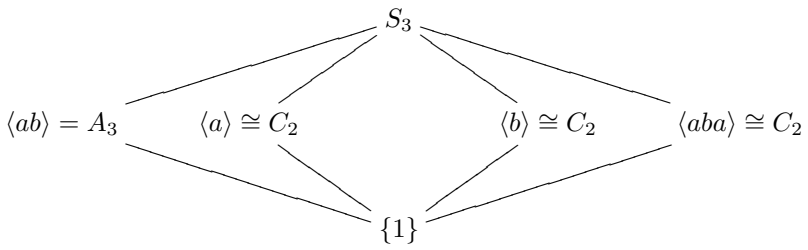
- $V := C_2 \times C_2$, il gruppo di Klein di ordine 4, si può descrivere nel seguente modo: $V = \{1, a, b, ab\}$ con le relazioni

  $$|a| = |b| = |ab| = 2.$$

  Ogni suo sottogruppo proprio non banale è ciclico di ordine 2, quindi il reticolo dei sottogruppi è il seguente:



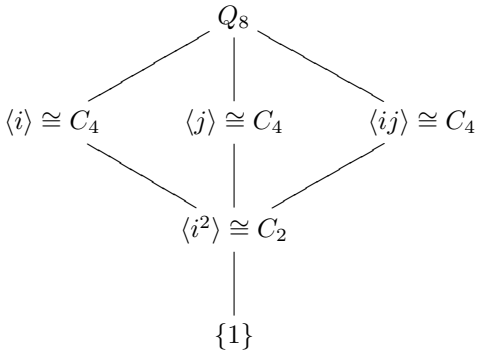
- S_3, il gruppo simmetrico su 3 oggetti. Ogni suo sottogruppo proprio non banale è ciclico e massimale di indice primo, quindi il reticolo dei sottogruppi è il seguente:



- Q_8, il gruppo dei quaternioni di ordine 8 si può descrivere nel seguente modo: $Q_8 = \{1, i, j, ij, i^2, ji, i^3, j^3\}$ con le relazioni:

$$i^2 = j^2 = (ij)^2,\ |i| = |j| = |ij| = 4.$$

I sottogruppi ciclici $\langle i\rangle$, $\langle j\rangle$ e $\langle ij\rangle$ hanno indice 2 quindi sono massimali e normali, e l'unico elemento non banale che non genera uno di questi tre sottogruppi è i^2, contenuto in ognuno. È facile dedurre che il reticolo dei sottogruppi è il seguente:

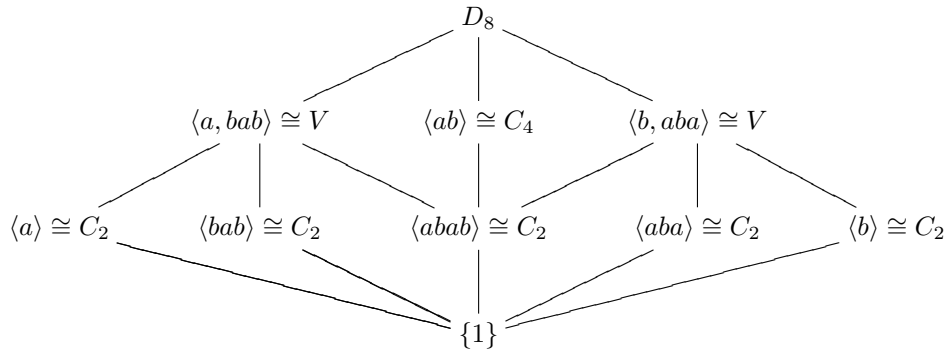


- D_8, il gruppo diedrale di ordine 8 si può descrivere nel seguente modo: $D_8 = \{1, a, b, ab, ba, aba, bab, abab\}$ con le relazioni

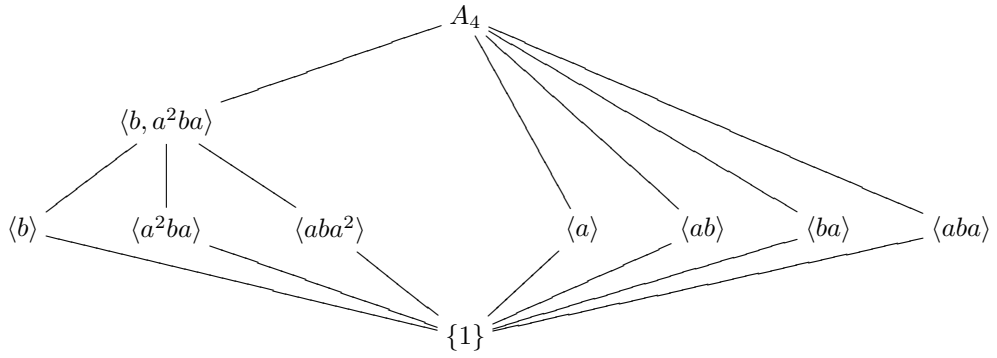
$$|a| = |b| = 2,\ |ab| = 4.$$

Certamente ci sono esattamente cinque sottogruppi di ordine 2, corrispondenti a a, b, aba, bab, $abab$. Inoltre $\langle baba\rangle = \langle abab\rangle < \langle ab\rangle = \langle ba\rangle$. Tramite una verifica diretta notiamo che gli unici due elementi che aggiunti a $\langle a\rangle$ generano un sottogruppo proprio di D_8 sono bab e $abab$. Consideriamo $\{1, a, bab, abab\}$. Si verifica facilmente che questo è un gruppo, ed è del tipo $\{1, x, y, xy\}$ ove $|x| = |y| = |xy| = 2$. Di conseguenza è un gruppo di Klein. Non ci sono sottogruppi propri tra esso e D_8. Simmetricamente

per b, otteniamo il seguente reticolo:



- A_4, il gruppo alterno su quattro oggetti, è generato dalle permutazioni $a := (1\ 2\ 3)$ di ordine 3, $b := (1\ 2)(3\ 4)$ di ordine 2. Gli elementi di struttura ciclica 2^2 insieme a 1 formano un sottogruppo V massimale isomorfo al gruppo di Klein $C_2 \times C_2$, e ogni 3-ciclo genera un sottogruppo ciclico massimale. Di conseguenza il reticolo è il seguente:



14. I gruppi alterni

Denotiamo con S_n il gruppo delle permutazioni di n oggetti - detto "gruppo simmetrico su n oggetti" -, e con A_n il sottogruppo di S_n che consiste delle permutazioni pari - detto "gruppo alterno su n oggetti". Si tratta del nucleo dell'omomorfismo $S_n \to C_2$ che manda ogni permutazione nel suo segno (1 se pari, -1 se dispari).

LEMMA 16. *A_n è generato dai 3-cicli.*

DIMOSTRAZIONE. La struttura ciclica di un elemento di A_n ha come unico vincolo la presenza di un numero pari di cicli di lunghezza pari (cioè cicli dispari). Ogni ciclo di lunghezza dispari è un prodotto di 3-cicli, infatti se k è un dispari allora $(123...k) = (123)(345)(567)...(k-4\ k-3\ k-2)(k-2\ k-1\ k)$. Inoltre i calcoli $(123)(124) = (13)(24)$ e $(12345)(12678) = (1345)(2678)$ hanno un'ovvia generalizzazione che dimostra che i prodotti di un numero pari di cicli di lunghezza pari possono essere realizzati come prodotti di cicli di lunghezza dispari. □

LEMMA 17. *Sia H un sottogruppo di S_n non contenuto in A_n. Allora $A_n \cap H$ ha indice 2 in H.*

DIMOSTRAZIONE. Sia $g \in H$ una permutazione dispari. Allora la funzione $A_n \cap H \longrightarrow H - (A_n \cap H)$ data dalla moltiplicazione per g è biiettiva. □

PROPOSIZIONE 15 (Classi di coniugio di A_n). *Sia $x \in A_n$. Siano $Cl_{A_n}(x)$ e $Cl_{S_n}(x)$ rispettivamente le classi di coniugio di x in A_n e in S_n. Allora $Cl_{A_n}(x) \neq Cl_{S_n}(x)$ se e solo se la struttura ciclica di x consiste di cicli di lunghezze dispari a due a due distinte. In particolare se $n \geq 5$ allora due qualsiasi 3-cicli di A_n sono coniugati.*

DIMOSTRAZIONE. Siano $C_{S_n}(x)$ e $C_{A_n}(x)$ rispettivamente i centralizzanti di x in S_n e in A_n. Per l'equazione delle classi

$$|A_n| = |C_{A_n}(x)| \cdot |Cl_{A_n}(x)|, \qquad |S_n| = |C_{S_n}(x)| \cdot |Cl_{S_n}(x)|,$$

quindi poiché $|S_n| = 2|A_n|$, $C_{A_n}(x) = C_{S_n}(x)$ se e solo se $Cl_{A_n}(x) \neq Cl_{S_n}(x)$. In altre parole, la classe di coniugio di x "si spezza" (ovvero $Cl_{A_n}(x) \neq Cl_{S_n}(x)$) se e solo se x non è centralizzato da permutazioni dispari. Supponiamo allora che x non sia centralizzato da permutazioni dispari, e sia $x = x_1x_2...x_k$ la decomposizione di x in prodotto di cicli disgiunti. Siccome ogni x_i centralizza x, ogni x_i ha lunghezza dispari (ovvero è una permutazione pari). Se x_i e x_j hanno la stessa lunghezza - chiamiamola t - allora esiste un ciclo y di lunghezza $2t$ tale che $y^2 = x_ix_j$ (l'esempio $x_i = (123)$, $x_j = (456)$, $y = (142536)$ è di immediata generalizzazione), quindi y è una permutazione dispari che centralizza x, assurdo. Segue che $x_1, ..., x_k$ hanno lunghezze dispari a due a due distinte. Viceversa, supponiamo che $x_1, ..., x_k$ abbiano lunghezze dispari a due a due distinte, e $y \in S_n$ centralizzi x. Poiché $x^y = {x_1}^y...{x_k}^y$ e gli x_i hanno lunghezze distinte, y centralizza ogni x_i, e quindi possiamo scrivere $y = y_1...y_k$ dove per ogni $i = 1, ..., k$ i punti coinvolti in y_i sono gli stessi coinvolti in x_i, e y_i centralizza x_i. Supponiamo che x_i muova il punto 1. Allora l'immagine di 1 determina completamente y_i: per esempio se $x_i = (12...m)$ e $1^{y_i} = 3$ allora $2^{y_i} = 4$, $3^{y_i} = 5$ e così via: per conoscere y_i basta scrivere due righe, sopra $12...m$ e sotto $34...m12$, e osservare che ogni elemento della prima riga va nell'elemento della seconda che occupa la stessa posizione. Segue che i possibili y_i sono tanti quante le possibili immagini di 1, ovvero n. Quindi siccome gli n elementi di $\langle x_i \rangle$ centralizzano x_i, essi sono i soli centralizzanti di x_i che coinvolgono punti che anche x_i coinvolge, e quindi $y_i \in \langle x_i \rangle$ per ogni $i = 1, ..., k$. In particolare gli y_i sono pari, quindi anche y è pari. □

ESERCIZIO 63. *Osservare che le classi di coniugio di un gruppo formano una partizione del gruppo, e che ogni sottogruppo normale è unione di classi di coniugio. Elencare le classi di coniugio di A_5, e dedurre che A_5 è un gruppo semplice.*

TEOREMA 8. *A_n è un gruppo semplice non abeliano se $n \geq 5$.*

DIMOSTRAZIONE. Proviamo il risultato per induzione su n. La base dell'induzione è $n = 5$, per questo si veda l'esercizio qui sopra. Supponiamo il risultato vero per A_{n-1} e proviamolo per A_n. Sia N un sottogruppo normale non banale di A_n. Dato $x \in \{1, ..., n\}$, indichiamo con $\mathrm{Stab}_{A_n}(x)$ il gruppo delle permutazioni di A_n che fissano x, cioè lo stabilizzatore di x per l'azione di permutazione. È chiaro che $\mathrm{Stab}_{A_n}(x) \cong A_{n-1}$. $N \cap \mathrm{Stab}_{A_n}(x)$ è un sottogruppo normale di $\mathrm{Stab}_{A_n}(x)$, quindi è $\mathrm{Stab}_{A_n}(x)$ oppure $\{1\}$. Nel primo caso N contiene almeno un 3-ciclo e quindi $N = A_n$ per la proposizione 15. Possiamo supporre quindi che $N \cap \mathrm{Stab}_{A_n}(x) = \{1\}$ per ogni $x \in \{1, ..., n\}$, in altre parole ogni permutazione non

banale di N è senza punti fissi. Mostriamo che questo non può accadere. Sia g un elemento non banale di N. Se g ammettesse nella struttura ciclica due cicli di lunghezza diversa allora esisterebbe una potenza di g non identica con un punto fisso. Se g non è un n-ciclo e la classe di coniugio di g in A_n è uguale alla sua classe di coniugio in S_n allora (si veda la proposizione 15) coniugando opportunamente troviamo l'elemento $g' \in N$ tale che se $g = g_1...g_k$ è la decomposizione di g in cicli disgiunti allora $g' = {g_1}^{-1}g_2...g_k$ e quindi $gg' \in N$ ammetterebbe un punto fisso. Resta da considerare il caso in cui g è un ciclo di lunghezza n, diciamo (a meno di cambiare nomi ai simboli) $(12...n)$. Coniugando con $(12)(34)$ otteniamo che $(214356...n) \in N$, quindi $(214356...n)(123456...n) \in N$ ha 1 come punto fisso. Abbiamo esaurito i casi, quindi siamo giunti ad una contraddizione. □

Ricordiamo che il gruppo degli automorfismi di un gruppo G è il gruppo $\mathrm{Aut}(G)$ degli isomorfismi $G \to G$ con l'operazione di composizione. L'azione di G su se stesso per coniugio determina un omomorfismo $G \to \mathrm{Aut}(G)$ il cui nucleo è $Z(G)$, il centro di G, quindi se $Z(G) = \{1\}$ allora G si immerge in $\mathrm{Aut}(G)$. Questo è il caso del gruppo alterno: se $n \geq 5$ allora $Z(A_n) = \{1\}$ (A_n è semplice non abeliano) e quindi $A_n \leq \mathrm{Aut}(A_n)$. Osserviamo che S_n agisce su A_n per coniugio, questo determina un omomorfismo $S_n \to \mathrm{Aut}(A_n)$ che è iniettivo in quanto il solo sottogruppo normale proprio non banale di S_n è A_n se $n \geq 5$ (si vedano gli esercizi). Mostriamo che se $n = 5$ oppure $n \geq 7$ allora $\mathrm{Aut}(A_n) = S_n$.

LEMMA 18. *Se $n \geq 5$ allora A_n non può agire non banalmente su meno di n oggetti.*

DIMOSTRAZIONE. Se l'asserto non fosse vero allora esisterebbe un omomorfismo iniettivo $A_n \to S_{n-1}$, ma questo è impossibile in quanto se $n \geq 5$ allora $n!/2$ non divide $(n-1)!$. □

LEMMA 19. *A_n agisca nel modo usuale su $\{1,...,n\}$. Se $n = 5$ oppure $n \geq 7$ allora ogni sottogruppo di A_n isomorfo a A_{n-1} è lo stabilizzatore di un qualche $i \in \{1,...,n\}$.*

DIMOSTRAZIONE. Dobbiamo provare che se $A_{n-1} \cong H \leq A_n$ allora $H = \mathrm{Stab}_{A_n}(i)$ per un $i \in \{1,...,n\}$. Sia $\varphi : A_{n-1} \to H \leq A_n$ l'isomorfismo dato. Risolviamo il caso $n = 7$ separatamente:

- $n = 7$. Se $A_6 \cong H \leq A_7$ non è lo stabilizzatore di un punto allora siccome ogni orbita non banale di H ha almeno 6 punti (per il lemma 18), l'azione di H su $\{1,2,3,4,5,6,7\}$ dev'essere transitiva. Ma 7 non divide $|H| = 6!/2$, quindi per l'equazione delle classi H non può agire transitivamente su 7 punti.

Mostriamo che ogni 3-ciclo di H (cioè, l'immagine di un 3-ciclo di A_{n-1} tramite φ) viene mandato in un 3-ciclo di A_n. Per questo osserviamo che se $c \in A_{n-1}$ è un 3-ciclo allora $\varphi(c)$ centralizza un $A_{n-4} \cong K \leq H$, quindi per il lemma 18 se $n-4 \geq 5$ (cioè $n \geq 9$) K è un sottogruppo di A_n di centro identico con un'orbita $\mathcal{O}$ di $n-t \geq n-4$ punti e centralizzato da un elemento di ordine 3, $\varphi(c)$. $\varphi(c)$ fissa ogni elemento $\mathcal{O}$, nel qual caso è un 3-ciclo (dovendo muovere al più 4 elementi), oppure muove qualche elemento di $\mathcal{O}$. In quest'ultimo caso non può muovere elementi di $\mathcal{O}$ fuori da $\mathcal{O}$, essendo il coniugio con $\varphi(c)$ l'identità in K, quindi deve muovere tutti gli elementi di $\mathcal{O}$, perché se per esempio fissa 1 e muove 2 allora dato $f \in K$ che manda 1 in 2 si ha che $f^{\varphi(c)}$ non manda 1 in 2, quindi è diverso da f. Ne segue

che 3 divide $n-t$ e $\varphi(c)$ è un prodotto di $(n-t)/3$ 3-cicli disgiunti. A_{n-4} agisce su tali 3-cicli permutandoli, quindi agisce fedelmente su $(n-t)/3$ elementi; per il lemma 18 si ha allora $(n-t)/3 \geq n-4$, cioè $12-2n \geq t \geq 0$, da cui $n \leq 6$, assurdo. Rimangono da discutere i casi $n = 5, 8$.

- $n = 5$. Gli elementi di ordine 3 sono proprio i 3-cicli.
- $n = 8$. Basta osservare che gli elementi di A_8 di struttura ciclica $(3^2, 1^2)$ non centralizzano gli elementi di ordine 2. (pospost)

Ora osserviamo che dati $(123), (124) \in A_{n-1} \cong H$, essi generano $A_4 \leq A_{n-1}$ e quindi $\varphi((123))$ e $\varphi((124))$ sono due 3-cicli di A_n che generano A_4, quindi sono del tipo $(abc), (abd)$. Siccome φ è iniettiva, le immagini di $(123), (124), ..., (1\ 2\ n-1)$ sono allora tutte del tipo (abx) cogli x a due a due distinti. Ma allora H è contenuto nello stabilizzatore in A_n dell'elemento di $\{1, ..., n\}$ che non è mosso da tali (abx), ed avendo il suo stesso ordine deve coincidere con esso. □

TEOREMA 9. *Se $n \geq 5$ e $n \neq 6$ allora* $\mathrm{Aut}(A_n) = S_n$.

DIMOSTRAZIONE. Sia ϕ un automorfismo di A_n. Dato $i \in \{1, ..., n\}$, osserviamo che $\phi(\mathrm{Stab}(i))$ è un sottogruppo di A_n isomorfo ad A_{n-1}, quindi per il lemma 19 è lo stabilizzatore di un certo punto, chiamiamolo k_i. L'applicazione $i \mapsto k_i$ è ben definita perché da $\mathrm{Stab}(x) = \mathrm{Stab}(y)$ segue $x = y$, ed è iniettiva perché da $\phi(\mathrm{Stab}(i)) = \phi(\mathrm{Stab}(j))$ segue $i = j$. Si tratta quindi di una biiezione di $\{1, ..., n\}$ in sé. In altre parole $i \mapsto k_i$ definisce un elemento di S_n, sia esso σ. Indichiamo con σ anche l'automorfismo di A_n dato dal coniugio $g \mapsto \sigma^{-1} g \sigma$. Consideriamo $\psi = \sigma^{-1} \circ \phi \in \mathrm{Aut}(A_n)$. Per concludere è sufficiente mostrare che ψ è l'identità, e per questo basta mostrare che ψ fissa i 3-cicli (poiché essi generano A_n). Siccome $\phi(\mathrm{Stab}(i)) = \mathrm{Stab}(\sigma(i))$, dato $g \in A_n$ gli elementi g e $\psi(g)$ muovono gli stessi punti (perché fissano gli stessi punti), quindi in particolare ψ agisce sui 3-cicli fissandoli o invertendoli (ci sono infatti solo due 3-cicli che muovono tre dati punti). Per assurdo, ψ inverta il 3-ciclo (123). Se ψ fissa (124) allora

$$\begin{aligned}(243) &= (132)(124) = \psi((123))\psi((124)) = \\ &= \psi((123)(124)) = \psi((13)(24)),\end{aligned}$$

altrimenti ψ inverte (124) e quindi

$$\begin{aligned}(243) &= (132)(124) = \psi((123))\psi((142)) = \\ &= \psi((123)(142)) = \psi((143)).\end{aligned}$$

In entrambi i casi ψ manda un elemento che muove 1 in un elemento che non lo muove, assurdo. □

E come è fatto $\mathrm{Aut}(A_6)$? Siccome A_n è caratteristico in S_n (per ogni $n \geq 1$) si ha $\mathrm{Aut}(A_n) = \mathrm{Aut}(S_n)$, e quindi siamo ridotti a calcolare $\mathrm{Aut}(S_6)$.

ESERCIZIO 64. *Mostrare che $Z(S_n) = Z(A_n) = 1$ se $n \geq 4$, e quindi* $\mathrm{Inn}(A_n) \cong A_n$ *e* $\mathrm{Inn}(S_n) \cong S_n$ *se $n \geq 4$. [Ragionare sulle classi di coniugio.]*

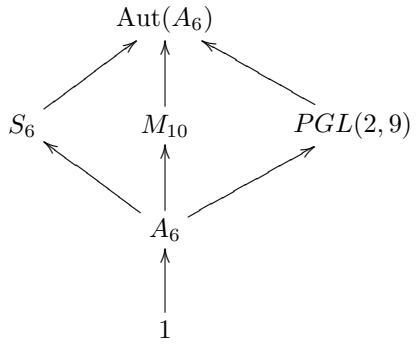
Se esiste un automorfismo di S_6 non interno allora per quanto visto nelle precedenti dimostrazioni esso deve mandare uno stabilizzatore di un punto in un sottogruppo transitivo di S_6 isomorfo a S_5. Costruiamo un tale sottogruppo. S_5 agisca per coniugio sull'insieme dei suoi sei 5-Sylow: tale azione è transitiva e determina un'immersione di S_5 in S_6. Sia H l'immagine di tale immersione: H è un sottogruppo transitivo di S_6 isomorfo a S_5. S_6 agisca per moltiplicazione a

destra sull'insieme dei laterali destri di H: tale azione è transitiva e fedele, quindi determina un omomorfismo iniettivo $S_6 \to S_6$, che quindi è un isomorfismo, cioè un automorfismo di S_6. Tale automorfismo non è interno perché manda H - che è transitivo - nello stabilizzatore del laterale H, quindi in un sottogruppo non transitivo.

ESERCIZIO 65. *Usando gli argomenti usati nelle dimostrazioni precedenti mostrare che se* $\phi \in \mathrm{Aut}(S_6)$ *manda* 3*-cicli in* 3*-cicli allora* $\phi \in \mathrm{Inn}(S_6)$.

Ora, se $\phi \in \mathrm{Aut}(S_6)$ manda un 3-ciclo in un 3-ciclo allora manda ogni 3-ciclo in un 3-ciclo in quanto i 3-cicli in S_6 sono a due a due coniugati e ogni automorfismo manda elementi coniugati in elementi coniugati. Mostriamo che se $\phi, \theta \in \mathrm{Aut}(S_6) - \mathrm{Inn}(S_6)$ allora $\phi\theta \in \mathrm{Inn}(S_6)$: per questo basta mostrare che $\phi\theta$ manda 3-cicli in 3-cicli. Osserviamo che ϕ e θ definiscono una biiezione tra i 3-cicli di S_6 e i 3^2-cicli (cioè gli elementi di struttura ciclica $(3,3)$) di S_6 (perché in S_6 i 3-cicli sono 40, tanti quanti i 3^2-cicli), quindi devono mandare i 3^2-cicli nei 3-cicli: di conseguenza $\phi\theta$ manda 3-cicli in 3-cicli. Questo dimostra che $\mathrm{Out}(S_6)$ è un gruppo non banale in cui ogni prodotto di due elementi non identici fa 1. È un facile esercizio mostrare che un tale gruppo deve avere due soli elementi, e quindi $\mathrm{Out}(S_6) \cong C_2$.

Siccome $[S_6 : A_6] = 2$, segue che $[\mathrm{Aut}(A_6) : A_6] = 4$, quindi $\mathrm{Out}(A_6)$ è un gruppo di ordine 4. In effetti si ha $\mathrm{Out}(A_6) \cong C_2 \times C_2$ (dimostrazione posposta). Il reticolo dei sottogruppi normali di $\mathrm{Aut}(A_6)$ risulta essere il seguente:



Cosa siano M_{10} (un gruppo di Mathieu) e $PGL(2,9)$ (un gruppo proiettivo lineare) si vedrà più avanti.

15. I sottogruppi massimali di S_n

In questo paragrafo vogliamo fornire una classificazione dei sottogruppi massimali di S_n. Per questo enunceremo senza dimostrarlo il teorema di O'Nan Scott.

Nel seguito S_n agisca nel modo usuale su $X := \{1, ..., n\}$. Una prima classificazione grossolana - che ci porta ad accorgerci che il vero problema sono i sottogruppi primitivi - è la seguente:

- **Il gruppo alterno**: A_n è un sottogruppo di S_n di indice 2, quindi è massimale.
- **Sottogruppi intransitivi**. Si tratta di quei sottogruppi di S_n la cui azione su X non è transitiva. Osserviamo che se $X = X_1 \cup ... \cup X_t$ è una partizione di X allora i sottogruppi $H_i := \mathrm{Stab}(X - X_i)$ commutano a

due a due e $H_i \cong \mathrm{Sym}(X_i)$. Ne segue che generano un sottogruppo di S_n della forma $S_{n_1} \times S_{n_2} \times ... \times S_{n_t}$, che è intransitivo per costruzione. È un facile esercizio mostrare che se tale sottogruppo è massimale allora $t = 2$. Siamo quindi ridotti a domandarci quando un sottogruppo della forma $S_k \times S_{n-k}$ è massimale. Risulta che un tale sottogruppo è massimale se e solo se $n - k \neq k$. Se $n = 2k$ allora esiste un sottogruppo della forma $S_k \wr C_2$ massimale e contenente $S_k \times S_k$, l'azione è data dallo scambio.

È un facile esercizio mostrare che se H è un sottogruppo intransitivo di S_n allora è contenuto in qualche sottogruppo intransitivo della forma $S_{n_1} \times ... \times S_{n_t}$ (basta considerare la partizione in H-orbite).

- **Sottogruppi imprimitivi**. Si tratta di quei sottogruppi di S_n la cui azione su X è transitiva ma non primitiva. Si dimostra che tali sottogruppi corrispondono alle fattorizzazioni di n, nel senso seguente: se $n = ab$ con a, b interi positivi maggiori di 1 allora il prodotto intrecciato $S_a \wr S_b$ agisce fedelmente su $ab = n$ oggetti, nel modo seguente: si partiziona $\{1, ..., n\}$ in b blocchi di a punti ciascuno, ogni copia di S_a permuta i punti di un blocco e S_b permuta i blocchi. Quindi $S_a \wr S_b$ si immerge in S_n, e corrisponde in effetti ad un sottogruppo massimale di S_n. $S_a \wr S_b$ è un sottogruppo imprimitivo di S_n, i blocchi di imprimitività sono dati dai sottoinsiemi di punti mossi dalle copie di S_a.
- **Sottogruppi primitivi**. Si tratta di quei sottogruppi di S_n la cui azione su X è primitiva. Nel seguito approfondiremo la struttura di tali sottogruppi.

15.1. Azione prodotto. Un primo esempio di sottogruppo primitivo di S_n è dato da un particolare prodotto intrecciato. Supponiamo che $n = k^m$, con k, m interi positivi maggiori di 1. Allora $S_k \wr S_m$ è primitivo sui k^m punti dell'insieme $\{1, ..., k\}^m$ tramite l'azione definita come segue:

$$((\sigma_1, ..., \sigma_m)\tau)(a_1, ..., a_m) := (\sigma_1(a_{\tau(1)}), ..., \sigma_m(a_{\tau(m)})).$$

Tale azione viene chiamata "**azione prodotto**", per distinguerla dall'azione imprimitiva di $S_k \wr S_m$ su km punti. Ne segue che S_m ammette un sottogruppo primitivo del tipo $S_k \wr S_m$. Si dimostra che tale sottogruppo è massimale se $k \geq 5$ e 4 non divide k^{m-1}.

15.2. Gruppi affini. Siano p un primo, n un intero positivo, $\mathbb{F}_p$ il campo con p elementi e $V := {\mathbb{F}_p}^n$ lo spazio vettoriale di dimensione n su $\mathbb{F}_p$. Consideriamo il gruppo $(T, +)$ (isomorfo a $(V, +)$) delle traslazioni di V, cioè $T := \{t_v \mid v \in V\}$ dove $t_v(w) := w + v$ per $w \in V$. Consideriamo inoltre il gruppo $GL(n, p)$ degli isomorfismi lineari dell'$\mathbb{F}_p$-spazio vettoriale V, identificabile al gruppo delle matrici invertibili $n \times n$ a coefficienti in $\mathbb{F}_p$ previa la scelta di una base di V. Siccome $GL(n, p) = \mathrm{Aut}(V)$, possiamo formare il prodotto semidiretto $G := AGL(n, p) := GL(n, p) \ltimes T$ (detto **gruppo affine** di V), dove $g \in GL(n, p)$ agisce su t_v secondo la regola ${t_v}^g := t_{g^{-1}(v)}$. G agisce fedelmente e transitivamente su V nel seguente modo: $v^{gt_w} := g^{-1}(v) + w$.

Esercizio 66. *Il gruppo G agisca transitivamente sull'insieme X. Mostrare che le seguenti affermazioni sono equivalenti:*

(1) *L'azione è primitiva.*
(2) *Lo stabilizzatore di un punto è un sottogruppo massimale.*

(3) *Lo stabilizzatore di ogni punto è un sottogruppo massimale.*

In virtù di questo esercizio, per mostrare che l'azione di G è primitiva siamo ridotti a mostrare che Stab(0) è un sottogruppo massimale. Abbiamo che $\mathrm{Stab}(0) = \{ft_v \in G \mid v = 0\} \cong GL(n,p)$. Sia $0 \neq w \in V$, e sia $g \in GL(n,p)$. Per concludere basta mostrare che Stab(0) e gt_w generano tutto G. L'operazione in G è così definita: $(ft_v) \cdot (gt_w) := (fg)(t_{g^{-1}(v)+w})$. Abbiamo quindi che se $h \in GL(n,p)$:

$$(hf^{-1}g^{-1}) \cdot (gt_w) \cdot f = ht_{f^{-1}(w)}.$$

Per ottenere un generico ht_u basta quindi scegliere una $f \in GL(n,p)$ che mandi u in w.

Segue che $GL(n,p) \ltimes T$ si immerge in S_{p^n} come sottogruppo primitivo.

15.3. Sottogruppi di tipo diagonale. Sia T un gruppo semplice non abeliano, e sia $U := \mathrm{Aut}(T)$. Sappiamo che l'azione di coniugio ci permette di identificare T ad un sottogruppo normale di U, cosicché $T \trianglelefteq U$. Dato un intero positivo k, consideriamo il prodotto intrecciato $U \wr S_k = B \rtimes S_k$, dove $B = U^k$. Sia C il sottogruppo di B che consiste delle k-ple $(u_1, ..., u_k)$ tali che $u_1 \equiv ... \equiv u_k \mod (T)$. Allora è facile vedere che $T^k \leq C$ e che $C/T^k \cong \mathrm{Out}(T)$. Inoltre dato che C è S_k-invariante si ha $L := C \rtimes S_k \leq B \rtimes S_k$. La diagonale $\Delta_U := \{(u, u, ..., u) \mid u \in U\}$ è un sottogruppo di C che commuta con S_k, quindi $H := \Delta_U \times S_k \leq L$ e si tratta di un sottogruppo di L di indice $|T|^{k-1}$ (infatti $|\Delta_U| = |U| = |\mathrm{Aut}(T)| = |T| \cdot |\mathrm{Out}(T)| = |C|/|T|^{k-1}$). Inoltre H è un sottogruppo massimale di L con cuore normale identico, quindi L è primitivo di grado $n := |T|^{k-1}$, e questo determina un sottogruppo primitivo di S_n, non sempre massimale.

15.4. Gruppi almost simple. Un gruppo G si dice "almost simple" se esiste un gruppo semplice non abeliano T tale che $T \leq G \leq \mathrm{Aut}(T)$. Se M è un sottogruppo massimale di G con cuore normale identico allora G agisce sui laterali destri di M e quindi è primitivo di grado $n := [G : M]$, e si immerge in S_n come sottogruppo primitivo, non sempre massimale.

15.5. Il teorema di O'Nan Scott. Il teorema di O'Nan Scott dà una classificazione dei sottogruppi massimali di S_n.

Teorema 10 (O'Nan Scott). *Sia n un intero positivo. Sia H un sottogruppo proprio di S_n diverso da A_n. Allora H è un sottogruppo di uno o più dei seguenti sottogruppi:*

(1) *un sottogruppo intransitivo $S_m \times S_k$ dove $m + k = n$;*
(2) *un sottogruppo imprimitivo $S_m \wr S_k$ dove $mk = n$;*
(3) *un prodotto intrecciato primitivo $S_k \wr S_m$ dove $k^m = n$;*
(4) *un gruppo affine $AGL(d,p)$;*
(5) *un sottogruppo di tipo diagonale;*
(6) *un gruppo almost simple.*

16. Esercizi sui gruppi

Raccogliamo in questo paragrafo i vari esercizi assegnati nel capitolo, più alcuni altri.

Esercizio 1: Siano G un gruppo, $g \in G$. Mostrare che se $n, m \in \mathbb{N}$ allora $g^n g^m = g^{n+m}$, $(g^n)^m = g^{nm}$. In particolare l'insieme $\{g^n \mid n \in \mathbb{N}\}$ è anch'esso un gruppo.

Esercizio 2: Dato un gruppo ciclico $G = \langle g \rangle$ di ordine n, mostrare che i generatori di G sono tutti e soli gli elementi di G della forma g^m con m coprimo con n.

Esercizio 3: Sia $\varphi : \mathbb{N} - \{0\} \to \mathbb{N}$ la funzione di Euler. Si hanno i seguenti fatti.

(1) Se p è primo e $n > 0$ è un intero allora $\varphi(p^n) = p^{n-1}(p-1)$.
(2) Se m, n sono interi positivi coprimi allora $\varphi(mn) = \varphi(m)\varphi(n)$.
(3) Se $n = {p_1}^{e_1}...{p_r}^{e_r}$ dove i p_i sono primi a due a due distinti allora

$$\varphi(n) = (p_1 - 1){p_1}^{e_1-1}...(p_r - 1){p_r}^{e_r-1}.$$

Esercizio 4: Siano G un gruppo, $g, h \in G$ tali che $gh = hg$, e $|g| = s$, $|h| = t$ siano finiti. Mostrare che $|gh|$ divide il minimo comune multiplo tra s e t, e che se s e t sono coprimi allora $|gh| = st$.

Esercizio 5: Mostrare che $\mathrm{End}(C_n)$, l'insieme degli omomorfismi $C_n \to C_n$, è un anello rispetto a somma e composizione isomorfo a $\mathbb{Z}/n\mathbb{Z}$, e che $\mathrm{Aut}(C_n) \cong U(\mathbb{Z}/n\mathbb{Z})$, dove $U(\mathbb{Z}/n\mathbb{Z})$ è l'insieme degli elementi invertibili rispetto alla moltiplicazione dell'anello $\mathbb{Z}/n\mathbb{Z}$.

Esercizio 6: Un omomorfismo di gruppi $f : G \to H$ è iniettivo se e solo se $\ker(f) = \{1\}$.

Esercizio 7: Se $f : G \to H$ è un omomorfismo iniettivo di gruppi allora f conserva gli ordini degli elementi: $|f(g)| = |g|$ per ogni $g \in G$.

Esercizio 8: Dato un omomorfismo di gruppi $f : G \to H$ si ha $f(g^{-1}) = f(g)^{-1}$ per ogni $g \in G$.

Esercizio 9: Due gruppi ciclici di ordine n sono isomorfi. Segue che ogni gruppo ciclico di ordine n è isomorfo a $(\mathbb{Z}/n\mathbb{Z}, +)$.

Esercizio 10: Mostrare che un prodotto diretto di gruppi abeliani è un gruppo abeliano, ma che un prodotto diretto di gruppi ciclici non è necessariamente ciclico.

Esercizio 11: Mostrare che $G \times \{1\}$ e $\{1\} \times H$ sono sottogruppi normali di $G \times H$.

Esercizio 12: Siano H, K due sottogruppi di un gruppo G. Mostrare che $|HK| = |H| \cdot |K| / |H \cap K|$.

Esercizio 13: Siano G un gruppo, $N_1, ..., N_t$ sottogruppi normali di G tali che $N_i \cap (N_1...N_{i-1}N_{i+1}...N_t) = \{1\}$ per ogni $i \in \{1, ..., t\}$. Mostrare che il sottogruppo di G generato da $N_1 \cup N_2 \cup ... \cup N_t$ coincide con $N_1...N_t$ ed è un sottogruppo normale di G isomorfo al prodotto diretto $N_1 \times N_2 \times ... \times N_t$. Un tale sottogruppo si dice "prodotto diretto interno" di $N_1, ..., N_t$.

Esercizio 14: Un'intersezione arbitraria di sottogruppi di un dato gruppo è ancora un sottogruppo.

Esercizio 15: Un automorfismo ϕ di G si dice interno se esiste $g \in G$ tale che $\phi(x) = g^{-1}xg$ per ogni $x \in G$. L'insieme degli automorfismi interni di G si indica con $\mathrm{Inn}(G)$. Mostrare che $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Esercizio 16: Dati un gruppo G ed un suo elemento x, $|x|$ è l'ordine del sottogruppo ciclico di G generato da x.

Esercizio 17: Ogni gruppo ciclico infinito è isomorfo a $(\mathbb{Z}, +)$.

Esercizio 18: Sia $n \in \mathbb{N}$. L'insieme

$$\mathrm{Stab}(n+1) := \{\sigma \in S_{n+1} \mid \sigma(n+1) = n+1\}$$

è un sottogruppo di S_{n+1} isomorfo a S_n ("Stab" sta per "stabilizzatore").

Esercizio 19: I sottogruppi e i quozienti di C_n sono ciclici. Dato un divisore d di n, esiste esattamente un sottogruppo di C_n di ordine d.

Esercizio 20: Se n e m sono interi positivi coprimi allora $C_{nm} \cong C_n \times C_m$.

Esercizio 21: Provare che dato un elemento g di un gruppo G, l'insieme degli interi $z \in \mathbb{Z}$ tali che $g^z = 1$ è un sottogruppo di $\mathbb{Z}$, diciamo $n\mathbb{Z}$. Mostrare che in tal caso $n = |g|$.

Esercizio 22: Dati un gruppo G e un suo elemento x, $C_G(x) := \{g \in G \mid gx = xg\}$ è un sottogruppo di G contenente x, e detto centralizzante di x in G.

Esercizio 23: Dati un gruppo G ed un suo sottogruppo H, $N_G(H) := \{g \in G \mid g^{-1}Hg = H\}$ è un sottogruppo di G contenente H, e detto normalizzante di H in G.

Esercizio 24: dato un gruppo G, mostrare che $Z(G) := \{g \in G \mid gx = xg \ \forall x \in G\}$ è un sottogruppo di G, detto centro di G. Si tratta dell'intersezione dei centralizzanti degli elementi di G. Chiaramente G è abeliano se e solo se $Z(G) = G$.

Esercizio 25: Il nucleo di un omomorfismo di gruppi è un sottogruppo normale del dominio, e la sua immagine è un sottogruppo del codominio.

Esercizio 26 (Primo teorema di isomorfismo per i gruppi): Dato un omomorfismo $f : G \to H$ di gruppi, esso induce un isomorfismo canonico $\tilde{f} : G/\ker(f) \to f(G)$ (quello che manda $g\ker(f)$ in $f(g)$).

Esercizio 27 (Secondo teorema di isomorfismo per i gruppi): Siano G un gruppo, $H \leq G$ e $N \trianglelefteq G$. Allora $HN := \{hn \mid h \in H,\ n \in N\}$ è un sottogruppo di G, N è normale in HN, $H \cap N$ è normale in H e $H/H \cap N \cong HN/N$.

Esercizio 28 (Terzo teorema di isomorfismo per i gruppi): Siano $H \subseteq N$ due sottogruppi normali di un gruppo G. Allora esiste un isomorfismo canonico $(G/H)/(N/H) \cong G/N$.

Esercizio 29 Dimostrare che dato un qualsiasi gruppo G, ogni suo sottogruppo di indice 2 è normale.

Esercizio 30: Se m, n sono interi coprimi allora m è invertibile in $\mathbb{Z}/n\mathbb{Z}$ e viceversa (basta usare l'identità di Bezout).

Esercizio 31: Mostrare che $N \times \{1\}$ e $\{1\} \times H$ sono sottogruppi di $N \rtimes H$, che $N \times \{1\}$ è normale complementato da $\{1\} \times H$. Mostrare che se G è un gruppo e N, H sono due suoi sottogruppi con N normale in G e complementato da H allora $G \cong N \rtimes H$. Mostrare che il prodotto semidiretto $N \rtimes H$ è un prodotto diretto se e solo se φ è l'omomorfismo che manda tutto in 1 (l'identità $N \to N$).

Esercizio 32: Mostrare che dare un'azione di G su X equivale a dare un omomorfismo di gruppi $f : G \to \mathrm{Sym}(X)$, confondendo gx con $f(g)(x)$. Il nucleo dell'azione coincide col nucleo di tale omomorfismo.

Esercizio 33: G agisce per coniugio sull'insieme dei suoi sottogruppi: $(g, H) \mapsto H^g := g^{-1}Hg$. Quali sono i sottogruppi la cui orbita consiste di un solo elemento?

Esercizio 34: Dati un gruppo G e un suo sottogruppo H, G agisce per moltiplicazione a destra sui laterali destri di H ($(g, Hx) \mapsto Hxg$), e per moltiplicazione a sinistra sui laterali sinistri di H ($(g, xH) \mapsto gxH$). Quali sono i nuclei di queste azioni? E le orbite?

Esercizio 35 (Equazione delle classi): Dati un gruppo G, un G-insieme X e $x \in X$, si ha $[G : \mathrm{Stab}_G(x)] = |Gx|$ (aiuto: considerare la funzione che manda $gx \in Gx$ nella classe $g\,\mathrm{Stab}_G(x)$ di $\mathrm{Stab}_G(x)$). Dal teorema di Lagrange segue allora la cosiddetta "equazione delle classi": $|G| = |Gx| \cdot |\,\mathrm{Stab}_G(x)|$.

Esercizio 36: Se X e Y sono insiemi equipotenti allora $\mathrm{Sym}(X)$ e $\mathrm{Sym}(Y)$

sono gruppi isomorfi.

Esercizio 37: In S_n, due cicli disgiunti commutano.

Esercizio 38: Ogni elemento di S_n si scrive in modo unico (a meno di scambiare l'ordine dei fattori) come prodotto (cioè composizione) di cicli disgiunti. [*Suggerimento*: data $\sigma \in S_n$ considerare la relazione di equivalenza seguente in $\{1, ..., n\}$: $i \sim j$ se $\sigma^m(i) = j$ per qualche intero positivo m.]

Esercizio 39: Due elementi di S_n sono coniugati in S_n se e solo se hanno la stessa struttura ciclica. [Suggerimento: mostrare che se $\sigma \in S_n$ allora $\sigma^{-1}(i_1...i_d)\sigma = (\sigma(i_1)...\sigma(i_d))$.]

Esercizio 40: Mostrare che ogni permutazione si può scrivere come prodotto di trasposizioni. [*Suggerimento*: osservare che basta farlo per i cicli, e che $(12...d) = (1d)(1\ d-1)(1\ d-2)...(13)(12)$.]

Esercizio 41 (Segno): Sia $\sigma \in S_n$. Scriviamo σ come prodotto di k trasposizioni. Mostrare che $(-1)^k$ dipende solo da σ. Esso viene denotato con $\mathrm{sgn}(\sigma)$ e chiamato segno di σ.

Esercizio 42: Mostrare che la funzione $S_n \to \{1, -1\}$ che manda σ in $\mathrm{sgn}(\sigma)$ è un omomorfismo di gruppi (dove in $\{-1, 1\}$ c'è l'usuale prodotto di $\mathbb{Z}$).

Esercizio 43: Un ciclo di lunghezza d è una permutazione pari se e solo se d è dispari.

Esercizio 44: Mostrare che le permutazioni pari di S_n sono esattamente quelle permutazioni che hanno nella struttura ciclica un numero pari di cicli di lunghezza pari.

Esercizio 45: Mostrare che la potenza k-esima di un n-ciclo è un prodotto di (n, k) cicli disgiunti tutti di lunghezza $n/(n, k)$.

Esercizio 46: Risolvere in S_{10} l'equazione $\sigma^3 = (1234)(56)$.

Esercizio 47: Mostrare che esistono solo quattro gruppi abeliani di ordine 36 a meno di isomorfismi.

Esercizio 48: Se G è un gruppo finito allora G è un p-gruppo se e solo se il suo ordine è una potenza di p (usare il lemma 2).

Esercizio 49: Usare l'equazione delle classi come fatto nella dimostrazione del lemma 2 per dimostrare che se G è un p-gruppo finito non banale allora il centro di G è non banale: $Z(G) \neq \{1\}$.

Esercizio 50: Usare l'esercizio precedente per dimostrare che dato un primo p, ogni gruppo di ordine p^2 è abeliano.

Esercizio 51: Fissati un primo p e un naturale n, quanti sono i gruppi abeliani di ordine p^n?

Esercizio 52: Mostrare che per ogni gruppo G si ha un isomorfismo canonico $G/Z(G) \cong \mathrm{Inn}(G)$ [Suggerimento: considerare l'azione di coniugio di G in sé].

Esercizio 53: Mostrare che S_3 e C_6 hanno gli stessi fattori di composizione.

Esercizio 54: Mostrare che ogni sottogruppo di un gruppo ciclico finito è caratteristico.

Esercizio 55: Mostrare che se un gruppo finito G ammette un solo p-Sylow, allora tale p-Sylow è caratteristico.

Esercizio 56: Mostrare che $\mathrm{soc}(G)$ è il prodotto diretto interno dei sottogruppi normali minimali di G.

Esercizio 57: Mostrare che $\mathrm{soc}(G)$ è un sottogruppo caratteristico di G, in particolare normale.

Esercizio 58: Mostrare che ogni gruppo nilpotente è risolubile.

Esercizio 59: G' è un sottogruppo caratteristico di G, in particolare normale.

Esercizio 60: Se $N \trianglelefteq G$ allora G/N è abeliano se e solo se $G' \leq N$.

Esercizio 61: Se $N \trianglelefteq G$ e i gruppi N e G/N sono risolubili allora G è risolubile.

Esercizio 63: Osservare che le classi di coniugio di un gruppo formano una partizione del gruppo, e che ogni sottogruppo normale è unione di classi di coniugio. Elencare le classi di coniugio di A_5, e dedurre che A_5 è un gruppo semplice.

Esercizio 64: Mostrare che $Z(S_n) = Z(A_n) = 1$ se $n \geq 4$, e quindi $\mathrm{Inn}(A_n) \cong A_n$ e $\mathrm{Inn}(S_n) \cong S_n$ se $n \geq 4$. [Ragionare sulle classi di coniugio.]

Esercizio 65: Mostrare che se $\phi \in \mathrm{Aut}(S_6)$ manda 3-cicli in 3-cicli allora $\phi \in \mathrm{Inn}(S_6)$.

Esercizio 66: Il gruppo G agisca transitivamente sull'insieme X. Mostrare che le seguenti affermazioni sono equivalenti:

(1) L'azione è primitiva.
(2) Lo stabilizzatore di un punto è un sottogruppo massimale.
(3) Lo stabilizzatore di ogni punto è un sottogruppo massimale.

Esercizio: Dimostrare che nessun gruppo può essere scritto come unione insiemistica di due suoi sottogruppi propri. Dare un esempio di un gruppo che è scrivibile come unione insiemistica di tre sottogruppi propri.

Esercizio: Sia n un intero positivo. Calcolare $\mathrm{Aut}(C_n)$ e confrontare il risultato con l'enunciato della proposizione 33.

Esercizio: Sia G un gruppo finito e sia T un suo sottogruppo normale e ciclico. Mostrare che ogni sottogruppo di T è un sottogruppo normale di G.

Esercizio: Mostrare che l'unico sottogruppo normale proprio di S_n è A_n se $n \geq 5$ [usare il fatto che A_n è un gruppo semplice se $n \geq 5$].

Esercizio: Mostrare che A_4 ha un unico sottogruppo normale proprio non banale, e che esso ha ordine 4.

Esercizio: Mostrare che $A_n = \{\sigma^2 \mid \sigma \in S_n\}$.

Esercizio: Sia n un intero positivo. Costruire un omomorfismo iniettivo $S_n \to A_{n+2}$.

Esercizio: Dimostrare che un gruppo semplice non abeliano non ha sottogruppi di indice 2, 3 o 4.

Esercizio: Dimostrare che non esistono gruppi semplici di ordine 300.

Esercizio: Dimostrare che non esistono gruppi semplici di ordine 144. Si tratta di un caso particolare del teorema di Burnside: ogni gruppo finito il cui ordine è diviso da al più due primi è risolubile.

Esercizio: Ogni gruppo ciclico finito ha una serie a fattori di ordine primo.

Esercizio: Dimostrare che le seguenti asserzioni sono equivalenti:

- Ogni gruppo finito di ordine dispari è risolubile.
- Ogni gruppo finito semplice non abeliano ha ordine pari.

Tali asserzioni equivalenti sono in effetti vere (teorema di Feit-Thompson).

Esercizio: Siano H, K, N tre sottogruppi di un gruppo G, con $N \trianglelefteq G$. Mostrare che H e K commutano modulo N (ovvero le loro immagini tramite la proiezione $G \to G/N$ commutano) se e solo se $[H, K] \subseteq N$.

Esercizio: Siano G un gruppo, Z il suo centro. Mostrare che se G/Z è ciclico allora $G = Z$.

Esercizio: Siano p un numero primo, G un p-gruppo finito. Mostrare che G ammette un sottogruppo di indice p. [Suggerimento: procedere per induzione su $|G|$ usando il fatto che $Z(G) \neq 1$.]

Esercizio: Siano p un numero primo, G un p-gruppo finito. Allora G ha una serie a fattori di ordine p. [Suggerimento: usare l'esercizio precedente.]

Esercizio: Dare un esempio di un gruppo infinito senza elementi di ordine infinito tale che l'insieme degli ordini dei suoi elementi sia infinito.

Esercizio: Sia G un gruppo. Ricordiamo che $\Phi(G)$ denota il sottogruppo di Frattini di G. Mostrare che:

- $\Phi(G)$ è un sottogruppo caratteristico di G.
- Dato un sottogruppo normale minimale abeliano N di G, N ammette un complemento in G se e solo se non è contenuto in $\Phi(G)$. Se N non è abeliano questo non è vero: fornire un controesempio.
- Se G è finito allora $\Phi(G)$ è nilpotente [Suggerimento: basta mostrare che ogni p-Sylow di $\Phi(G)$ è normale. Dato un p-Sylow P di $\Phi(G)$, considerare il normalizzante in G di P, $N_G(P)$, e usare l'argomento di Frattini].

DEFINIZIONE 18 (Gruppo di Frobenius). *Un gruppo G si dice gruppo di Frobenius se esiste un sottogruppo H di G tale che $H \cap H^g = \{1\}$ per ogni $g \in G - H$.*

Esercizio: Mostrare che un gruppo di Frobenius è un gruppo che agisce fedelmente, transitivamente e non regolarmente, e tale che ogni elemento non banale non ha più di un punto fisso.

Esercizio: Sia G un gruppo di Frobenius, e sia $H \leq G$ tale che $H \cap H^g = \{1\}$ per ogni $g \in G - H$. Allora esiste un sottogruppo normale N di G di cui H è un complemento in G. [Suggerimento: togliere da G i coniugati di H e aggiungere 1.]

Esercizio: Sia G un gruppo finito semplice non abeliano. Mostrare che G ammette un sottogruppo proprio non abeliano. [Suggerimento: ragionare sui centralizzanti degli elementi non banali. E usare l'esercizio precedente.]

Esercizio: Mostrare che se un gruppo abeliano agisce fedelmente e transitivamente allora l'azione è regolare.

Esercizio: S_5 agisca sull'insieme dei sottoinsiemi di $\{1, 2, 3, 4, 5\}$ di cardinalità 2, nel modo seguente: $\sigma(\{a, b\}) := \{\sigma(a), \sigma(b)\}$ per $\sigma \in S_5$. Mostrare che tale azione è fedele e transitiva e determinare i suoi stabilizzatori. Questo determina un sottogruppo transitivo di S_{10}: mostrare che non è massimale.

Esercizio: Mostrare che se $\sigma \in S_n$ è un n-ciclo allora il suo centralizzante in S_n è $\langle\sigma\rangle$. Generalizzazione: se σ è un prodotto di r t-cicli disgiunti allora il suo centralizzante in S_n è del tipo $(C_t \wr S_{r/t}) \times S_{n-rt}$.

CAPITOLO 2

Categorie

1. Anelli e moduli: cenni

Cominciamo col ricordare definizioni e proprietà di anelli e moduli, che saranno la base per i nostri esempi fondamentali.

DEFINIZIONE 19 (Anelli). *Un anello commutativo unitario è una terna* $(A, +, \cdot)$ *dove* A *è un insieme,* e $+$ *("somma"),*$\cdot$ *("prodotto" o "moltiplicazione") sono due operazioni binarie di* A *tali che:*

- $(A, +)$ *è un gruppo commutativo (il cui elemento neutro verrà chiamato zero e denotato con* 0*);*
- $(A, \cdot)$ *è un monoide commutativo (il cui elemento neutro verrà chiamato uno e denotato con* 1*);*
- $a(b + c) = ab + ac$ *per ogni* $a, b, c \in A$*;*
- $(a + b)c = ac + bc$ *per ogni* $a, b, c \in A$*.*

Un sottoinsieme R *di* A *si dice sottoanello di* A *se* R *contiene* 0 *e* 1 *ed è chiuso rispetto alle operazioni* $+$*,* $\cdot$*.*

Gli elementi invertibili o unità di A *sono quegli* $a \in A$ *tali che esista in* A *un loro inverso moltiplicativo, ovvero un* $b \in A$ *tale che* $ab = ba = 1$*. L'insieme degli elementi invertibili di* A *viene denotato con* $U(A)$*.*

D'ora in poi se non viene specificato altrimenti ogni anello sarà unitario e commutativo.

ESEMPIO: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ con somma e prodotto usuali sono anelli.

ESERCIZIO 67. *Mostrare che l'insieme degli elementi invertibili di un dato anello forma un gruppo per la moltiplicazione.*

DEFINIZIONE 20 (Ideali). *Sia* A *un anello commutativo. Un ideale di* A *è un sottoinsieme* I *di* A *tale che:*

- $(I, +)$ *è un sottogruppo di* $(A, +)$*;*
- *se* $x \in I$ *e* $a \in A$ *allora* $ax \in I$*.*

Un ideale I *di* A *si dice primo se le condizioni seguenti sono soddisfatte:*

- $1 \notin I$*;*
- *se* $x, y \in A$ *e* $xy \in I$ *allora* $x \in I$ *oppure* $y \in I$*.*

In altre parole, un ideale primo è un ideale di A *il cui complementare in* A *contiene* 1 *ed è "moltiplicativo" (cioè chiuso rispetto al prodotto). Questo modo di vedere torna utile quando si parla di localizzazione.*

Un ideale I *di* A *si dice massimale se è diverso da* A *e non ci sono ideali di* A *diversi da* A *contenenti propriamente* I*.*

ESERCIZIO 68. *Se* I *è un ideale di* A *e* $1 \in I$ *allora* $I = A$*.*

Esercizio 69. *Se A è un anello e $a \in A$ allora $(a) := \{ab \mid b \in A\}$ è un ideale di A, detto "principale generato da a". In particolare $(0) = \{0\}$ e $(1) = A$ sono ideali di A.*

Definizione 21 (Omomorfismi, isomorfismi e nuclei). *Dati due anelli A, B, un omomorfismo tra A e B è una funzione $f : A \to B$ che sia contemporaneamente un omomorfismo di gruppi $(A, +) \to (B, +)$ e un omomorfismo di monoidi $(A, \cdot) \to (B, \cdot)$. L'omomorfismo f è detto isomorfismo se è sia iniettivo che suriettivo. Il nucleo dell'omomorfismo f è per definizione il suo nucleo in quanto omomorfismo di gruppi additivi, ovvero* $\ker(f) := \{x \in A \mid f(x) = 0\}$.

Esercizio 70. *Il nucleo di un omomorfismo è un ideale del dominio, e l'immagine di un omomorfismo è un sottoanello del codominio.*

Esercizio 71. *Un omomorfismo di anelli è iniettivo se e solo se il suo nucleo è $\{0\}$.*

Definizione 22 (Domini, campi). *Un anello commutativo A si dice dominio (di integrità) se l'ideale $\{0\}$ è primo. A si dice campo se l'ideale $\{0\}$ è massimale.*

Esercizio 72. *Mostrare che un anello commutativo A è un dominio di integrità se e solo se ogni volta che $a, b \in A$ sono non nulli, il prodotto ab è non nullo.*

Esercizio 73. *Mostrare che un anello commutativo A è un campo se e solo se ogni elemento non nullo di A è invertibile.*

Esercizio 74. *Un'intersezione arbitraria di ideali di un anello A è un ideale di A.*

Esempio: se S è un sottoinsieme di un anello A, l'ideale generato da S è per definizione l'intersezione di tutti gli ideali di A contenenti S. Si tratta del "più piccolo" ideale di A contenente S. Lo si indica con $\langle S \rangle$. È ovvio che $\langle S \rangle$ eguaglia

$$\{\sum_{k \in F} a_k s_k \mid a_k \in A,\ s_k \in S\ \forall k \in F,\ F\ finito\},$$

essendo tale insieme un ideale di A ed ogni ideale contenente S contenendo tale insieme, per definizione.

Definizione 23 (Quozienti). *Siano A un anello e I un suo ideale. La relazione su A definita da $x \sim y \Leftrightarrow x - y \in I$ è un'equivalenza; l'insieme quoziente, A/I, ha la struttura di anello con le operazioni $(x+I)+(y+I) = (x+y)+I$ e $(x+I)(y+I) = xy + I$. A/I si dice anello quoziente di A modulo I.*

Esercizio 75. *Se I è un ideale di A, A/I è un dominio di integrità se e solo se I è primo, e A/I è un campo se e solo se I è massimale.*

Ne segue che ogni ideale massimale è primo, dato che ogni campo è un dominio di integrità.

Esercizio 76. *Mostrare che dato un intero n le seguenti affermazioni sono equivalenti:*

- *n è un numero primo;*
- *$n\mathbb{Z}$ è un ideale primo di $\mathbb{Z}$;*
- *$n\mathbb{Z}$ è un ideale massimale di $\mathbb{Z}$.*

Segue in particolare che se p è un primo l'anello $\mathbb{Z}/p\mathbb{Z}$ è un campo finito con p elementi.

ESERCIZIO 77 (Primo Teorema di Isomorfismo). *: dato un omomorfismo $f : A \to B$ di anelli, la funzione*

$$\tilde{f} : A/\ker(f) \to f(A)$$
$$a + \ker(f) \mapsto f(a)$$

è ben definita ed è un isomorfismo di anelli.

ESERCIZIO 78 (Teorema di Corrispondenza di Ideali). *: dato un anello A ed un suo ideale I, l'insieme degli ideali di A/I è identificabile con l'insieme degli ideali di A contenenti I tramite l'ovvia corrispondenza.*

Osservazione: dato un anello A e una famiglia $(I_k)_{k\in K}$ di ideali di A, i seguenti sono egualmente ideali di A:

$$\bigcap_k I_k, \qquad \sum_k I_k := \langle \bigcup_k I_k \rangle = \{\sum_{k\in F} i_k \mid i_k \in I \ \forall k \in K,\ F \subseteq K \ finito\}.$$

PROPOSIZIONE 16. *Un dominio di integrità finito è un campo.*

DIMOSTRAZIONE. Sia allora A un dominio di integrità finito. Allora per ogni $0 \neq a \in A$ la moltiplicazione per a

$$A \xrightarrow{\cdot a} A$$

è iniettiva, e quindi è pure suriettiva perché A è finito (principio dei cassetti). Ne segue che qualcosa viene mandato in 1, ovvero esiste un $b \in A$ tale che $ab = 1$. Quindi ogni elemento non nullo di A è invertibile, ovvero A è un campo. □

DEFINIZIONE 24 (A-moduli). *Dato un anello commutativo A, un A-modulo è un gruppo abeliano $(M, +)$ dotato di una funzione $A \times M \to M$, $(a, m) \mapsto a \cdot m$ (moltiplicazione per scalare), tale che:*

- *$1 \cdot m = m$ per ogni $m \in M$;*
- *$(a + b) \cdot m = a \cdot m + b \cdot m$ per ogni $a, b \in A$, $m \in M$;*
- *$a \cdot (m + n) = a \cdot m + a \cdot n$ per ogni $a \in A$, $m, n \in M$.*

Un omomorfismo tra due A-moduli M, N è un omomorfismo di gruppi abeliani $f : M \to N$ che sia A-lineare, ovvero tale che $f(a \cdot m) = a \cdot f(m)$ per ogni $a \in A$, $m \in M$. Un sotto-A-modulo di un A-modulo M è un sottoinsieme N di M che eredita da M la struttura di A-modulo (cioè $(N, +) \leq (M, +)$ e $a \cdot n \in N$ per ogni $a \in A$, $n \in N$); indicheremo ciò con $N \leq M$.

ESEMPIO: dato un campo k, un k-modulo non è altro che un k-spazio vettoriale.

ESEMPIO: ogni gruppo abeliano $(G, +)$ ha un'unica struttura di $\mathbb{Z}$-modulo: la moltiplicazione di $n \in \mathbb{Z}$ con $g \in G$ è la somma di g con se stesso n volte se $n > 0$, l'opposto della somma di g con se stesso $-n$ volte se $n < 0$, e 0 se $n = 0$. Quindi un gruppo abeliano non è altro che uno $\mathbb{Z}$-modulo.

ESEMPIO: ogni anello A è un A-modulo con la struttura canonica: il prodotto per scalare è l'usuale prodotto in A. Un ideale di A non è altro che un sotto-A-modulo di A.

ESEMPIO: dato un anello A, l'insieme A^n per un $n \in \mathbb{N}$ è un A-modulo in cui la moltiplicazione per scalari è per componenti.

ESEMPIO: dato un omomorfismo di anelli $\varphi : A \to B$, B assume la struttura di A-modulo data da $a \cdot b := \varphi(a)b$ per ogni $a \in A$, $b \in B$.

DEFINIZIONE 25 (Algebre). *Un'A-algebra è un omomorfismo di anelli $A \to B$. A volte si dice che B è un'A-algebra, lasciando sottinteso il morfismo strutturale $A \to B$. Un'A-algebra $\varphi : A \to B$ è in particolare un A-modulo con l'operazione $a \cdot b := \varphi(a)b$ per $a \in A$, $b \in B$.*

ESEMPIO: l'anello dei polinomi $A[X]$ è un'A-algebra con $A \to A[X]$, $a \mapsto a$.

DEFINIZIONE 26 (Complessi, sequenze esatte). *Un complesso di gruppi abeliani è una catena di morfismi*

$$\cdots \longrightarrow M_{-2} \longrightarrow M_{-1} \longrightarrow M_0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \cdots$$

tale che la composizione di due qualsiasi frecce successive sia il morfismo nullo, ovvero l'immagine di ogni freccia sia contenuta nel nucleo della successiva. La catena si chiama sequenza esatta se l'immagine di ogni freccia coincide col nucleo della successiva. Complessi e sequenze esatte di moduli sono complessi e sequenze esatte dei sottostanti gruppi additivi.

ESERCIZIO 79. *Un omomorfismo $M \to N$ è iniettivo se e solo se la sequenza $0 \to M \to N$ è esatta, è suriettivo se e solo se la sequenza $M \to N \to 0$ è esatta.*

Ricordiamo che un diagramma di oggetti e frecce si dice commutativo se ogni composizione di frecce dipende solo dall'oggetto di partenza e da quello di arrivo. Ricordiamo inoltre che dato un omomorfismo $f : G \to H$ di gruppi abeliani, il conucleo di f, $\operatorname{coker}(f)$, è il quoziente $H/f(G)$.

LEMMA 20 (Caccia al diagramma: il lemma del serpente). *Sia dato un diagramma commutativo di gruppi abeliani con le righe esatte*

$$\begin{array}{ccccccccc} & & M' & \xrightarrow{a} & M & \xrightarrow{b} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & N' & \xrightarrow{c} & N & \xrightarrow{d} & N'' & & \end{array}$$

Allora esiste una sequenza esatta canonica di gruppi abeliani

$$\ker(f) \xrightarrow{r} \ker(g) \xrightarrow{s} \ker(h) \xrightarrow{t} \operatorname{coker}(f) \xrightarrow{u} \operatorname{coker}(g) \xrightarrow{v} \operatorname{coker}(h)$$

Inoltre:

- *se $a : M' \to M$ è iniettiva allora $r : \ker(f) \to \ker(g)$ è iniettiva;*
- *se $d : N \to N''$ è suriettiva allora $v : \operatorname{coker}(g) \to \operatorname{coker}(h)$ è suriettiva.*

DIMOSTRAZIONE. Si tratta appunto di un esercizio di "caccia al diagramma". Ovvero bisogna operare sempre percorrendo le frecce del diagramma e utilizzando le sue proprietà. Dapprima costruiamo il morfismo $t : \ker(h) \longrightarrow \operatorname{coker}(f)$.

- Sia $x \in ker(h)$. Allora $h(x) = 0$ e $x = b(m)$ per qualche $m \in M$ dacché b è suriettiva; per cui $0 = h(x) = h(b(m)) = d(g(m))$. Ne segue che $g(m) \in \ker(d) = c(N')$, e quindi esiste $n' \in N'$ tale che $g(m) = c(n')$. Definiamo allora $t(x) := n' + f(M')$. Per verificare che la definizione posta ha senso dobbiamo scegliere in modo arbitrario $\overline{m} \in M$, $\overline{n}' \in N'$ tali che $x = b(\overline{m})$ e $g(\overline{m}) = c(\overline{n}')$ e verificare che $n' + f(M') = \overline{n}' + f(M')$, ovvero

che $n'-\overline{n}' \in f(M')$. Abbiamo che $0 = x-x = b(m)-b(\overline{m}) = b(m-\overline{m})$, da cui $m-\overline{m} \in \ker(b) = a(M')$, quindi $m-\overline{m} = a(m')$ per qualche $m' \in M$. Poiché c è iniettiva, per mostrare che $f(m') = n'-\overline{n}'$ basta mostrare che $c(f(m')) = c(n-\overline{n}')$. Ora $c(f(m')) = g(a(m')) = g(m-\overline{m}) = g(m)-g(\overline{m}) = c(n')-c(\overline{n}') = c(n'-\overline{n}')$.

I morfismi r, s sono le restrizioni di a, b rispettivamente a $\ker(f)$, $\ker(g)$ (e sono ben definiti perché $a(\ker(f)) \subseteq \ker(g)$, $b(\ker(g)) \subseteq \ker(h)$), e u, v sono indotti da c, d (e sono ben definiti perché $c(f(M')) \subseteq g(M)$ e $d(g(M)) \subseteq h(M'')$). Continuazione posposta. □

Esercizio 80. *Sia G un gruppo abeliano, con notazione additiva. Mostrare che l'insieme* $\mathrm{End}(G)$ *degli endomorfismi di G è un anello rispetto a somma e composizione, e che $U(\mathrm{End}(G)) = \mathrm{Aut}(G)$. Mostrare che se G è ciclico finito di ordine n allora* $\mathrm{End}(G)$ *è isomorfo a G come gruppo e a $\mathbb{Z}/n\mathbb{Z}$ come anello. Dedurre che $|\mathrm{Aut}(G)| = \varphi(n)$.*

2. Categorie: definizioni ed esempi

Definizione 27 (Categoria). *Una categoria $\mathcal{C}$ consiste di:*

- *Una classe di oggetti $Ob(\mathcal{C})$.*
- *Per ogni $A, B \in Ob(\mathcal{C})$, un* ***insieme*** $\mathrm{Hom}_{\mathcal{C}}(A, B)$. *I suoi elementi si dicono morfismi tra A e B e un morfismo f tra A e B si indica con $f : A \to B$ oppure con $A \xrightarrow{f} B$.*
- *Per ogni $A, B, C \in Ob(\mathcal{C})$, una funzione*

$$\circ : \mathrm{Hom}_{\mathcal{C}}(B, C) \times \mathrm{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, C)$$

detta composizione.

ed è tale che:

- *La composizione tra morfismi sia associativa, ovvero: per ogni $A, B, C, D \in Ob(\mathcal{C})$, e per ogni $A \xrightarrow{f} B$, $B \xrightarrow{g} C$, $C \xrightarrow{h} D$, si ha $(h \circ g) \circ f = h \circ (g \circ f)$.*
- *Per ogni $A \in Ob(\mathcal{C})$ esista $1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ tale che per ogni $A \xrightarrow{f} B$ e per ogni $C \xrightarrow{g} A$ si abbia $f \circ 1_A = f$ e $1_A \circ g = g$.*

Definizione 28 (Sottocategorie). *Data una categoria $\mathcal{C}$, una categoria $\mathcal{D}$ si dice sottocategoria di $\mathcal{C}$ se $Ob(\mathcal{D}) \subseteq Ob(\mathcal{C})$ e per ogni $A, B \in Ob(\mathcal{D})$,* $\mathrm{Hom}_{\mathcal{D}}(A, B) \subseteq \mathrm{Hom}_{\mathcal{C}}(A, B)$, *e la composizione è ottenuta restringendo a $\mathcal{D}$ la composizione in $\mathcal{C}$. Una sottocategoria $\mathcal{D}$ di $\mathcal{C}$ si dice intera se per ogni $A, B \in Ob(\mathcal{D})$,* $\mathrm{Hom}_{\mathcal{D}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$.

Definizione 29 (Monomorfismi, epimorfismi, isomorfismi). *Un morfismo $f : A \to B$ in una categoria $\mathcal{C}$ si dice:*

- *monomorfismo se per ogni $g, h : B \to C$ in $\mathcal{C}$, se $f \circ g = f \circ h$ allora $g = h$.*
- *epimorfismo se per ogni $g, h : C \to A$ in $\mathcal{C}$, se $g \circ f = h \circ f$ allora $g = h$.*
- *isomorfismo se esiste $l : B \to A$ in $\mathcal{C}$ tale che $f \circ l = 1_A$ e $l \circ f = 1_B$.*

Quando due oggetti A e B di una categoria sono isomorfi, ovvero quando esiste un isomorfismo tra essi, si scrive $A \cong B$.

ESEMPIO: Sia $(X, \leq)$ un insieme parzialmente ordinato. Costruiamo la categoria $\mathcal{C}$ definendo $Ob(\mathcal{C}) := X$, e dati $x, y \in X$ definiamo:

$$\mathrm{Hom}_{\mathcal{C}}(x, y) = \{\emptyset\} \textit{ se } x \leq y$$

$$\mathrm{Hom}_{\mathcal{C}}(x, y) = \emptyset \textit{ se } x \not\leq y$$

Rimane da definire la composizione. Siano dunque $x, y, z \in X$. Dobbiamo definire una funzione

$$\circ : \mathrm{Hom}_{\mathcal{C}}(y, z) \times \mathrm{Hom}_{\mathcal{C}}(x, y) \to \mathrm{Hom}_{\mathcal{C}}(x, z)$$

Per transitività della relazione d'ordine, se il codominio di questa funzione è vuoto allora tale è anche il dominio (la verifica è immediata: ricordare che un prodotto cartesiano è vuoto se e solo se uno dei fattori è vuoto). In tal caso dichiariamo la nostra funzione $\circ$ essere uguale al vuoto (funzione vuota), ovvero l'unica possibile funzione $\emptyset \to \emptyset$ (da cui in un certo senso in algebra $0^0 = |\emptyset|^{|\emptyset|} = |\emptyset^{\emptyset}| = 1$). In caso contrario il codominio non è vuoto, il che significa che $x \leq z$. Se il dominio è vuoto poniamo $\circ = \emptyset$, altrimenti definiamo $\circ$ come l'unica funzione possibile tra i due insiemi (ricordare che esiste una sola funzione tra due insiemi con un solo elemento: essa manda l'elemento del primo insieme nell'elemento del secondo). È facile verificare che otteniamo una categoria, in particolare se $x \in X$ allora $\mathrm{Hom}_{\mathcal{C}}(x, x) = \{\emptyset\}$ per la proprietà riflessiva, quindi $1_x = \emptyset$.

Per esempio dato un qualsiasi insieme Y possiamo considerare la categoria associata all'insieme parzialmente ordinato dall'inclusione $P(Y)$.

ESEMPIO: Le seguenti, come l'intuizione suggerisce, sono categorie:

- Set. Gli oggetti sono gli insiemi, i morfismi sono le funzioni tra insiemi.
- Group. Gli oggetti sono i gruppi, i morfismi sono gli omomorfismi di gruppi.
- Ring. Gli oggetti sono gli anelli, i morfismi sono gli omomorfismi di anelli.
- Mod-A, dove A è un anello. Gli oggetti sono gli A-moduli destri, i morfismi sono gli omomorfismi di A-moduli destri.
- A-Mod, A-moduli sinistri. Similmente a sopra.
- Vect-k=Mod-k=k-Mod, dove k è un campo. k-spazi vettoriali.

ESEMPIO: Data una categoria $\mathcal{C}$, possiamo definire la categoria duale od opposta $\mathcal{C}^{op}$ ponendo $Ob(\mathcal{C}^{op}) := Ob(\mathcal{C})$ e $\mathrm{Hom}_{\mathcal{C}^{op}}(A, B) := \mathrm{Hom}_{\mathcal{C}}(B, A)$ per ogni $A, B \in Ob(\mathcal{C}^{op})$.

ESERCIZIO 81. *Mostrare che nella categoria degli insiemi un monomorfismo è una funzione iniettiva, un epimorfismo è una funzione suriettiva e un isomorfismo è una funzione biiettiva. Mostrare che ciò non è vero nella categoria degli anelli.*

Un suggerimento: domandarsi se è sempre vero che un isomorfismo è un morfismo che sia contemporaneamente monomorfismo ed epimorfismo.

DEFINIZIONE 30 (Oggetti iniziali, terminali, zero-oggetti). *Data una categoria $\mathcal{C}$, un oggetto $A \in Ob(\mathcal{C})$ si dice:*

- *iniziale se per ogni $X \in Ob(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}}(A, X)$ consiste di un solo elemento.*
- *terminale se per ogni $Y \in Ob(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}}(Y, A)$ consiste di un solo elemento.*
- *zero-oggetto se è sia iniziale che terminale. Salvo contrordine, denoteremo con 0 un zero-oggetto e sempre con 0 l'unico morfismo $0 \to X$ e l'unico morfismo $X \to 0$, per ogni oggetto X.*

ESEMPIO: Nella categoria Set, il vuoto è l'*unico* oggetto iniziale, e qualunque insieme con un solo elemento è un oggetto terminale. È facile convincersi che in Set non esistono zero-oggetti (il vuoto non è un oggetto terminale).

ESERCIZIO 82. *Nella categoria Ring, l'anello degli interi $\mathbb{Z}$ è un oggetto iniziale (la caratteristica di un anello è determinata da questo fatto).*

ESERCIZIO 83. *Due zero-oggetti in una categoria sono isomorfi tramite un unico isomorfismo.*

DEFINIZIONE 31 (Funtori). *Siano $\mathcal{C}, \mathcal{D}$ due categorie. Un funtore $F : \mathcal{C} \to \mathcal{D}$ è una legge che associa:*

- *ad ogni $A \in Ob(\mathcal{C})$ un oggetto $F(A) \in Ob(\mathcal{D})$.*
- *ad ogni $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ un morfismo $F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$. Ciò determina una funzione $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$.*

tale che:

- *Sia rispettata la composizione: per ogni $A \xrightarrow{f} B$, $B \xrightarrow{g} C$ in $\mathcal{C}$,*
$$F(g \circ f) = F(g) \circ F(f)$$
- *Per ogni $A \in \mathcal{C}$, $F(1_A) = 1_{F(A)}$.*

ESEMPIO: Il funtore dimentico ("forgetful functor") è quel funtore che "dimentica la struttura": un esempio è il funtore $Group \to Set$ che manda un gruppo nel sottostante insieme, un omomorfismo nella sottostante funzione tra insiemi.

DEFINIZIONE 32 (Funtori interamente fedeli, funtori essenzialmente suriettivi). *Un funtore $F : \mathcal{C} \to \mathcal{D}$ si dice:*

- *Intero se per ogni $A, B \in Ob(\mathcal{C})$, la funzione*
$$\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$$
$$g \mapsto F(g)$$
è suriettiva.
- *Fedele se per ogni $A, B \in Ob(\mathcal{C})$, la funzione*
$$\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$$
$$g \mapsto F(g)$$
è iniettiva.
- *Interamente fedele se è sia intero che fedele.*
- *Essenzialmente suriettivo se per ogni $C \in Ob(\mathcal{C})$ esiste $D \in Ob(\mathcal{D})$ tale che $F(C) \cong D$.*

DEFINIZIONE 33 (Morfismi tra funtori). *Date due categorie $\mathcal{C}$ e $\mathcal{D}$, possiamo costruire la categoria $Fct(\mathcal{C}, \mathcal{D})$ i cui oggetti sono i funtori tra $\mathcal{C}$ e $\mathcal{D}$, e i cui morfismi sono le cosiddette "trasformazioni naturali" tra funtori. Una trasformazione naturale tra i funtori $F, G \in Ob(Fct(\mathcal{C}, \mathcal{D}))$ è una legge, indicata con $h : F \to G$, che associa ad ogni $A \in Ob(\mathcal{C})$ un morfismo $h_A \in \mathrm{Hom}_{\mathcal{D}}(F(A), G(A))$, in modo tale che per ogni $A, B \in Ob(\mathcal{C})$ e per ogni $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ il seguente diagramma*

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ \downarrow{\scriptstyle h_A} & & \downarrow{\scriptstyle h_B} \\ G(A) & \xrightarrow{G(f)} & G(B) \end{array}$$

commuti, ovvero $h_B \circ F(f) = G(f) \circ h_A$ *(questa è una naturale richiesta di compatibilità).*

La composizione di trasformazioni naturali si definisce nel modo ovvio, ponendo $(h \circ k)_A = h_A \circ k_A$ *per ogni oggetto* A.

h *si dice isomorfismo naturale se* h_A *è un isomorfismo per ogni* $A \in Ob(\mathcal{C})$.

DEFINIZIONE 34 (Equivalenze). *Un funtore* $F : \mathcal{C} \to \mathcal{D}$ *si dice equivalenza di categorie se esiste un funtore* $G : \mathcal{D} \to \mathcal{C}$ *tale che* $G \circ F \cong \mathrm{Id}_{\mathcal{C}}$ *e* $F \circ G \cong \mathrm{Id}_{\mathcal{D}}$.

Si può dimostrare il seguente:

TEOREMA 11. *Un funtore* $F : \mathcal{C} \to \mathcal{D}$ *è un'equivalenza di categorie se e solo se esso è interamente fedele ed essenzialmente suriettivo.*

3. Il lemma di Yoneda

Cominciamo col seguente importantissimo risultato:

TEOREMA 12 (Lemma di Yoneda). *Sia* $\mathcal{C}$ *una categoria. Definiamo*

$$\hat{\mathcal{C}} := Fct(\mathcal{C}^{op}, Set)$$

Osserviamo che dato $X \in Ob(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}}(-, X)$ *è un funtore* $\mathcal{C}^{op} \to Set$ *che manda* $A \in Ob(\mathcal{C})$ *in* $\mathrm{Hom}_{\mathcal{C}}(A, X)$ *e* $f \in \mathrm{Hom}_{\mathcal{C}^{op}}(A, B)$ *nel morfismo di insiemi* $\mathrm{Hom}_{\mathcal{C}}(A, X) \to \mathrm{Hom}_{\mathcal{C}}(B, X)$ *che manda* $A \xrightarrow{a} X$ *in* $a \circ f$. *Similmente si può considerare il funtore* $\mathrm{Hom}_{\mathcal{C}}(X, -) : \mathcal{C} \to Set$.

Consideriamo il funtore

$$h_{\mathcal{C}} : \mathcal{C} \to \hat{\mathcal{C}}$$

che manda $X \in Ob(\mathcal{C})$ *in* $\mathrm{Hom}_{\mathcal{C}}(-, X) \in Ob(\hat{\mathcal{C}})$ *e* $A \xrightarrow{f} B$ *in* $h_{\mathcal{C}}(f) : \mathrm{Hom}_{\mathcal{C}}(-, X) \to \mathrm{Hom}_{\mathcal{C}}(-, Y)$, *la trasformazione naturale che, fissato* $A \in Ob(\mathcal{C})$, *associa al morfismo* $\alpha \in \mathrm{Hom}_{\mathcal{C}}(A, X)$ *il morfismo* $f \circ \alpha \in \mathrm{Hom}_{\mathcal{C}}(A, Y)$.

Allora per $X \in Ob(\mathcal{C})$, $A \in Ob(\hat{\mathcal{C}})$, $\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A) \cong A(X)$, ***funtorialmente*** *in* A *e in* X, *ovvero tale isomorfismo induce isomorfismi naturali*

$$\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), -) \to -(X)$$
$$\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(-), A) \to A(-)$$

fissato X *nel primo caso,* A *nel secondo.*

DIMOSTRAZIONE. Cominciamo col costruire i morfismi

$$\varphi : \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A) \to A(X), \qquad \psi : A(X) \to \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A)$$

che vogliamo essere uno l'inverso dell'altro:

- $\varphi : \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A) \to A(X)$. Sia $\gamma : h_{\mathcal{C}}(X) \to A$, trasformazione naturale. Vogliamo associargli un elemento dell'insieme $A(X)$. Decidiamo che tale elemento sia $\gamma_X(\mathrm{Id}_X)$ (ricordare che $\gamma_X : \mathrm{Hom}_{\mathcal{C}}(X, X) \to A(X)$).
- $\psi : A(X) \to \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A)$. Sia $x \in A(X)$. Vogliamo associargli una trasformazione naturale $\gamma : h_{\mathcal{C}}(X) \to A$. La naturalità ci richiede che per ogni $\beta \in \mathrm{Hom}_{\mathcal{C}^{op}}(T', T)$ noi otteniamo un diagramma commutativo

$$\begin{array}{ccc} h_{\mathcal{C}}(X)(T') & \xrightarrow{\gamma_{T'}} & A(T') \\ \downarrow{\scriptstyle h_{\mathcal{C}}(X)(\beta)} & & \downarrow{\scriptstyle A(\beta)} \\ h_{\mathcal{C}}(X)(T) & \xrightarrow{\gamma_T} & A(T) \end{array}$$

Fissato $T \in Ob(\mathcal{C}^{op}) = Ob(\mathcal{C})$ definiamo

$$\gamma_T(f) := A(f)(x)$$

per ogni $f \in \mathrm{Hom}_{\mathcal{C}^{op}}(X,T) = \mathrm{Hom}_{\mathcal{C}}(T,X) = h_{\mathcal{C}}(X)(T)$.

Naturalità: dato $\beta \in \mathrm{Hom}_{\mathcal{C}^{op}}(T',T) = \mathrm{Hom}_{\mathcal{C}}(T,T')$, e dato $g \in h_{\mathcal{C}}(X)(T') = \mathrm{Hom}_{\mathcal{C}}(T',X) = \mathrm{Hom}_{\mathcal{C}^{op}}(X,T')$,

$$A(\beta)(\gamma_{T'}(g)) = A(\beta)(A(g)(x)) = A(\beta \circ g)(x)$$

$$\gamma_T(h_{\mathcal{C}}(X)(\beta)(g)) = \gamma_T(\beta \circ g) = A(\beta \circ g)(x)$$

Mostriamo che $\psi \circ \varphi = 1_{\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X),A)}$ e che $\varphi \circ \psi = 1_{A(X)}$.

- $\psi \circ \varphi = 1_{\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X),A)}$. Sia $l \in \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X),A)$, e sia $x := l_X(\mathrm{Id}_X)$. Vogliamo mostrare che la trasformazione naturale $\gamma : h_{\mathcal{C}}(X) \to A$ associata a x tramite ψ è esattamente l. γ è definita dall'essere, fissato $T \in Ob(\mathcal{C})$,

  $$\gamma_T(f) = A(f)(x) = A(f)(l_X(\mathrm{Id}_X))$$

  per ogni $f \in h_{\mathcal{C}}(X)(T) = \mathrm{Hom}_{\mathcal{C}}(T,X) = \mathrm{Hom}_{\mathcal{C}^{op}}(X,T)$. Fissiamo una tale f. Poiché l è trasformazione naturale il seguente diagramma commuta:

  $$\begin{array}{ccc} h_{\mathcal{C}}(X)(X) & \xrightarrow{h_{\mathcal{C}}(X)(f)} & h_{\mathcal{C}}(X)(T) \\ \downarrow{\scriptstyle l_X} & & \downarrow{\scriptstyle l_T} \\ A(X) & \xrightarrow{A(f)} & A(T) \end{array}$$

  In particolare

  $$l_T(f) = l_T(h_{\mathcal{C}}(X)(f)(\mathrm{Id}_X)) = A(f)(l_X(\mathrm{Id}_X)) = \gamma_T(f)$$

- $\varphi \circ \psi = 1_{A(X)}$. Sia $x \in A(X)$, e sia $l : h_{\mathcal{C}}(X) \to A(X)$ la trasformazione naturale associata tramite ψ. Vogliamo mostrare che $l_X(\mathrm{Id}_X) = x$. l è definita dall'essere $l_T(f) = A(f)(x)$ per ogni $f \in h_{\mathcal{C}}(X)(T) = \mathrm{Hom}_{\mathcal{C}}(T,X) = \mathrm{Hom}_{\mathcal{C}^{op}}(X,T)$. Scegliendo $T = X$ e $f = \mathrm{Id}_X$ si ha $l_X(\mathrm{Id}_X) = A(\mathrm{Id}_X)(x) = \mathrm{Id}_X(x) = x$.

Funtorialità in $A \in \hat{\mathcal{C}}$. Definiamo, com'è ovvio, la trasformazione naturale

$$\Phi : \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), -) \to -(X)$$

ponendo

$$\Phi_A : \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A) \to A(X)$$
$$l \mapsto l_X(\mathrm{Id}_X)$$

Ogni tale morfismo è un isomorfismo, per quanto abbiamo appena visto.

Per verificare la naturalità dobbiamo accertarci che per ogni $j \in \mathrm{Hom}_{\hat{\mathcal{C}}}(A,B)$ il seguente diagramma commuti.

$$\begin{array}{ccc} \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A) & \xrightarrow{\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), j)} & \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), B) \\ \downarrow{\scriptstyle \Phi_A} & & \downarrow{\scriptstyle \Phi_B} \\ A(X) & \xrightarrow{j_X} & B(X) \end{array}$$

Fissiamo dunque $g : h_{\mathcal{C}}(X) \to A$ in $\hat{\mathcal{C}}$. Abbiamo:

$$\Phi_B(\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}, j)(g)) = \Phi_B(j \circ g) = (j \circ g)_X(\mathrm{Id}_X) = j_X(g_X(\mathrm{Id}_X)) = j_X(\Phi_A(g))$$

Funtorialità in $X \in Ob(\mathcal{C})$. Definiamo, com'è ovvio, la trasformazione naturale

$$\Psi : \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(-), A) \to A(-)$$

ponendo

$$\Psi_X : \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A) \to A(X)$$
$$l \mapsto l_X(\mathrm{Id}_X)$$

Per verificare la naturalità dobbiamo accertarci che per ogni $i \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ il seguente diagramma commuti.

$$\begin{array}{ccc} \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A) & \xrightarrow{\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(i), A)} & \mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(Y), A) \\ \downarrow{\scriptstyle \Psi_X} & & \downarrow{\scriptstyle \Psi_Y} \\ A(X) & \xrightarrow{A(i)} & A(Y) \end{array}$$

Fissiamo dunque $g : h_{\mathcal{C}}(X) \to A$ in $\hat{\mathcal{C}}$. Abbiamo:

$$\Psi_Y(\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(i), A)(g)) = \Psi_Y(g \circ h_{\mathcal{C}}(i)) = g_Y(h_{\mathcal{C}}(i)_Y(\mathrm{Id}_Y)) = g_Y(i)$$

$$A(i)(\Psi_X(g)) = A(i)(g_X(\mathrm{Id}_X)) = g_Y(h_{\mathcal{C}}(X)(i)(\mathrm{Id}_X)) = g_Y(i)$$

(l'ultima relazione valendo per naturalità di g). □

Corollario 1. *Il funtore $h_{\mathcal{C}}$ del lemma di Yoneda è interamente fedele. Esso si dice "immersione di Yoneda".*

Dimostrazione. Sappiamo che $\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), A) \cong A(X)$ funtorialmente in $A \in Ob(\hat{\mathcal{C}})$ e in $X \in Ob(\mathcal{C})$. Prendendo $A = h_{\mathcal{C}}(Y) = \mathrm{Hom}_{\mathcal{C}}(-, Y)$ in tale relazione, per $Y \in Ob(\mathcal{C})$, otteniamo

$$\mathrm{Hom}_{\hat{\mathcal{C}}}(h_{\mathcal{C}}(X), h_{\mathcal{C}}(Y)) \cong \mathrm{Hom}_{\mathcal{C}}(X, Y)$$

Ora basta osservare che in questo caso il morfismo ψ definito nella dimostrazione del lemma di Yoneda è quello canonico. □

In particolare, possiamo vedere una qualsiasi categoria $\mathcal{C}$ come una sottocategoria intera di $\hat{\mathcal{C}} = Fct(\mathcal{C}^{op}, Set)$. Ne segue:

Corollario 2. *Sia $\mathcal{C}$ una categoria, e siano $X, Y \in Ob(\mathcal{C})$, $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.*

1. *Se la composizione a sinistra con f $\mathrm{Hom}_{\mathcal{C}}(Z, X) \to \mathrm{Hom}_{\mathcal{C}}(Z, Y)$ è biiettiva per ogni $Z \in Ob(\mathcal{C})$ allora f è un isomorfismo.*
2. *Se la composizione a destra con f $\mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$ è biiettiva per ogni $Z \in Ob(\mathcal{C})$ allora f è un isomorfismo.*

Dimostrazione. Primo punto. Equivalentemente, se il morfismo corrispondente a f in $\hat{\mathcal{C}}$ è isomorfismo naturale, allora f è isomorfismo. Questo segue immediatamente dal lemma di Yoneda (avere gli stessi morfismi implica avere gli stessi isomorfismi).

Secondo punto. Si deduce dal primo considerando la categoria opposta $\mathcal{C}^{op}$. □

4. Funtori rappresentabili

Non è però detto che l'immersione di Yoneda sia un funtore essenzialmente suriettivo. Chiameremo "rappresentabili" i funtori che giacciono nell'immagine essenziale di tale immersione:

DEFINIZIONE 35 (Funtori rappresentabili). *Sia $\mathcal{C}$ una categoria. $F \in Ob(\hat{\mathcal{C}})$ si dice rappresentabile se esiste $X \in Ob(\mathcal{C})$ tale che $F \cong h_{\mathcal{C}}(X)$ in $\hat{\mathcal{C}}$, ovvero $F(Y) \cong h_{\mathcal{C}}(X)(Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$ funtorialmente in $Y \in Ob(\mathcal{C})$. X si dice rappresentante di F.*

Il rappresentante di un funtore rappresentabile è individuato a meno di isomorfismi: se $h_{\mathcal{C}}(X) \cong h_{\mathcal{C}}(X')$ allora per interezza $X \cong X'$ (in generale, se $F : \mathcal{C} \to \mathcal{D}$ è un funtore pienamente fedele e f è un isomorfismo in $\mathcal{C}$ con inverso g allora $F(f)$ è un isomorfismo in $\mathcal{D}$ con inverso $F(g)$; in particolare per ogni $A, B \in Ob(\mathcal{C})$, $A \cong B$ in $\mathcal{C}$ se e solo se $F(A) \cong F(B)$ in $\mathcal{D}$).

ESEMPIO: Sia k un campo, e sia A una k-algebra, ovvero un anello dotato di un omomorfismo di anelli $k \to A$ (necessariamente iniettivo - k è un campo - per cui si può pensare che $k \subseteq A$). Siano N_A, ${}_AM$, L_k (ovvero: sia N un A-modulo destro, sia M un A-modulo sinistro, sia L un k-modulo). Sia

$$B(N \times M, L) := \{mappe\ N \times M \to L\ (A, k) - bilineari\}$$

Ricordiamo che una mappa $h : N \times M \to L$ si dice (A, k)-bilineare se $h(na, m) = h(n, am)$ e $h(nl, m) = lh(n, m)$ per ogni $n \in N$, $m \in M$, $a \in A$, $l \in k$.

Ricordiamo cosa sia il prodotto tensoriale di N e M: $k^{(N\times M)}$, prodotto diretto di $|N \times M|$ copie di k (cioè il sottoinsieme di $\prod_{j\in N\times M} k$ che consiste degli elementi le cui componenti sono tutte 0 eccetto per un numero finito), ha la struttura di k-modulo (l'azione di k è componente per componente); possiamo considerare $N \times M$ come un sottoinsieme di $k^{(N\times M)}$ associando ad (n, m) l'elemento $t(n, m) \in k^{(N\times M)}$ che ha 1 nella posizione (n, m) e 0 altrove. Consideriamo il sottomodulo W di $k^{(N\times M)}$ generato dai seguenti elementi:

$$(n + n', m) - (n, m) - (n', m)$$
$$(n, m + m') - (n, m) - (n, m')$$
$$(na, m) - (n, am)$$
$$l(n, m) - (nl, m)$$

al variare di $n, n' \in N$, $m, m' \in M$, $a \in A$, $l \in k$. Definiamo

$$N \otimes_A M := k^{(N\times M)}/W$$

Esso è un k-modulo detto prodotto tensoriale degli A-moduli N e M, e soddisfa la seguente proprietà universale: per ogni mappa (A, k)-bilineare $h : N \times M \to L$ esiste un'unica mappa k-lineare $\varphi : N \otimes_A M \to L$ tale che $\varphi|_{N\times M} = h$. Ovvero indicando con β la mappa naturale

$$N \times M \to N \otimes_A M,\ (n, m) \mapsto t(n, m) + W =: n \otimes m,$$

ogni mappa (A, k)-bilineare $N \times M \to L$ si fattorizza unicamente attraverso β.

Ovvero, ad ogni elemento di $B(N \times M, L)$ è associato un unico morfismo di k-moduli $N \otimes_A M \to L$ (che lo estende). Ciò è la parafrasi del seguente isomorfismo di k-moduli:

$$B(N \times M, L) \cong \mathrm{Hom}_{Mod-k}(N \otimes_A M, L)$$

Consideriamo $\mathcal{C} := (Mod - k)^{op}$, e il funtore $F \in \hat{\mathcal{C}}$ che manda il k-modulo L in $B(N \times M, L)$, e il morfismo $L \xrightarrow{f} L'$ nella composizione a sinistra con f $B(N \times M, L) \to B(N \times M, L')$. L'isomorfismo sopra si può riscrivere come

$$F(L) \cong \mathrm{Hom}_{\mathcal{C}}(L, N \otimes_A M)$$

ed esso è funtoriale in L. Questo dice che F è rappresentato dal prodotto tensoriale $N \otimes_A M$.

Nota Bene: Quanto fin qui esposto dice che c'è un legame molto stretto tra proprietà universali e funtori rappresentabili. In realtà sono due modi di vedere la stessa cosa. Per capire meglio cosa questo significhi si vedano i paragrafi successivi.

5. Funtori aggiunti

Date due categorie $\mathcal{C}$, $\mathcal{C}'$, la categoria prodotto è quella categoria, indicata con $\mathcal{C} \times \mathcal{C}'$, che ha come classe di oggetti

$$Ob(\mathcal{C}) \times Ob(\mathcal{C}'),$$

e dati $(A, B), (A', B') \in Ob(\mathcal{C} \times \mathcal{C}')$, come insieme di morfismi

$$\mathrm{Hom}_{\mathcal{C}\times\mathcal{C}'}((A, B), (A', B')) := \mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}'}(A', B')$$

Un funtore $F : \mathcal{C} \times \mathcal{C}' \to \mathcal{D}$ si dice anche bifuntore, rispetto alle due categorie $\mathcal{C}$ e $\mathcal{C}'$.

Definizione 36 (Funtori aggiunti). *Siano $F : \mathcal{C} \to \mathcal{C}'$, $G : \mathcal{C}' \to \mathcal{C}$ due funtori. Si dice che (F, G) è una coppia di funtori aggiunti, o che F è aggiunto a sinistra a G, o che G è aggiunto a destra a F, se esiste un isomorfismo di bifuntori*

$$\mathrm{Hom}_{\mathcal{C}'}(F(-), -) \cong \mathrm{Hom}_{\mathcal{C}}(-, G(-))$$

Notiamo che se (F, G) è una coppia di funtori aggiunti allora $G(Y)$ è un rappresentante del funtore $\mathrm{Hom}_{\mathcal{C}}(F(-), Y) : \mathcal{C}^{op} \to Set$. Di conseguenza due funtori aggiunti a destra ad un fissato funtore F sono tra loro isomorfi. In particolare per ogni $Y', Z' \in Ob(\mathcal{C}')$ abbiamo $\mathrm{Hom}_{\mathcal{C}'}(F(G(Y')), Z') \cong \mathrm{Hom}_{\mathcal{C}}(G(Y'), G(Z'))$, funtorialmente in $G(Y')$ e in $G(Z')$, *quindi anche* in Y' e in Z' (questo andrebbe giustificato). In altre parole (ragionando analogamente per F) otteniamo isomorfismi

$$\mathrm{Hom}_{\mathcal{C}'}((F \circ G)(-), -) \cong \mathrm{Hom}_{\mathcal{C}}(G(-), G(-))$$

$$\mathrm{Hom}_{\mathcal{C}'}(F(-), F(-)) \cong \mathrm{Hom}_{\mathcal{C}}(-, (G \circ F)(-))$$

Guardando ai morfismi corrispondenti a $1_{G(Y)}$ e a $1_{F(X)}$ otteniamo morfismi di funtori

$$F \circ G \to \mathrm{Id}_{\mathcal{C}'},\ \mathrm{Id}_{\mathcal{C}} \to G \circ F$$

Esempio: Osserviamo che dati tre insiemi X, Y, Z,

$$\mathrm{Hom}_{Set}(X \times Y, Z) \cong \mathrm{Hom}_{Set}(X, \mathrm{Hom}_{Set}(Y, Z)) \cong \mathrm{Hom}_{Set}(Y, Z)^X,$$

ove tutto è canonico: per esempio il primo isomorfismo è ottenuto mandando una funzione $f : X \times Y \to Z$ nella funzione $X \to \mathrm{Hom}_{Set}(Y, Z)$ che manda x nella funzione $Y \to Z$ che manda y in $f(x, y)$. Sempre il primo isomorfismo dice che il funtore $\mathrm{Hom}_{Set}(Y, -) : Set \to Set$ è aggiunto a destra al funtore $- \times Y : Set \to Set$.

ESEMPIO: Sia k un campo, A una k-algebra e $L \in Mod - k$. Il funtore $\mathrm{Hom}_k(L, -) : Mod - A \to Mod - A$ è aggiunto a destra al funtore $- \otimes_k L$. Questo segue dal fatto che per ogni $M, N \in Mod - A$ e $L \in Mod - k$,

$$\mathrm{Hom}_A(L \otimes_k N, M) \cong \mathrm{Hom}_A(N, \mathrm{Hom}_k(L, M)) \cong \mathrm{Hom}_k(L, \mathrm{Hom}_A(N, M))$$

6. Prodotti, coprodotti, nuclei, conuclei

DEFINIZIONE 37 (Prodotti e coprodotti). *Sia $\mathcal{C}$ una categoria, I un insieme, e sia $\{X_i\}_{i \in I}$ una famiglia di oggetti di $\mathcal{C}$.*

- *Se il funtore $\mathcal{C}^{op} \to Set$, $Y \mapsto \prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(Y, X_i)$ è rappresentabile, denotiamo un rappresentante $\prod_{i \in I} X_i$ e lo chiamiamo prodotto degli X_i.*
- *Se il funtore $\mathcal{C} \to Set$, $Y \mapsto \prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(X_i, Y)$ è rappresentabile, denotiamo un rappresentante $\coprod_{i \in I} X_i$ e lo chiamiamo coprodotto degli X_i.*
- *Se per ogni famiglia di oggetti indiciati da I il loro prodotto (risp. coprodotto) esiste, diciamo che la categoria $\mathcal{C}$ ammette prodotti (risp. coprodotti) indiciati da I.*
- *Se $X_i = X$ per ogni $i \in I$ indichiamo con X^I il loro prodotto, con $X^{(I)}$ il loro coprodotto.*

Osserviamo che per definizione il funtore $\mathcal{C}^{op} \to Set$, $Y \mapsto \prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(Y, X_i)$ è rappresentabile se e solo se

$$\prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(-, X_i) \cong \mathrm{Hom}_{\mathcal{C}}(-, \prod_{i \in I} X_i)$$

Similmente, il funtore $\mathcal{C} \to Set$, $Y \mapsto \prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(X_i, Y)$ è rappresentabile se e solo se

$$\prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(X_i, -) \cong \mathrm{Hom}_{\mathcal{C}}(\coprod_{i \in I} X_i, -)$$

Supponiamo ora che il prodotto degli X_i esista, sia esso X. Allora abbiamo, in particolare, che

$$\prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(X, X_i) \cong \mathrm{Hom}_{\mathcal{C}}(X, X)$$

In corrispondenza dell'identità di X, Id_X, otteniamo quindi una famiglia di morfismi, detti proiezioni,

$$\pi_i : \prod_{i \in I} X_i \to X_i.$$

Similmente per il coprodotto, se esso esiste otteniamo i morfismi canonici

$$\varepsilon_i : X_i \to \coprod_{i \in I} X_i$$

Sappiamo che se il prodotto esiste deve soddisfare, per ogni $Y \in Ob(\mathcal{C})$, l'isomorfismo

$$\prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(Y, X_i) \cong \mathrm{Hom}_{\mathcal{C}}(Y, \prod_{i \in I} X_i)$$

Ciò significa che dare un morfismo $Y \to \prod_{i \in I} X_i$ è lo stesso che dare una famiglia di morfismi $(f_i : Y \to X_i)_{i \in I}$. Sia $f : Y \to \prod_{i \in I} X_i$ il morfismo associato agli f_i.

La funtorialità ci fa commutare il seguente diagramma:

$$\begin{array}{ccc} \prod_{i\in I}\mathrm{Hom}_{\mathcal{C}}(\prod_{j\in I}X_j, X_i) & \longrightarrow & \prod_{i\in I}\mathrm{Hom}_{\mathcal{C}}(Y, X_i) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(\prod_{i\in I}X_i, \prod_{i\in I}X_i) & \longrightarrow & \mathrm{Hom}_{\mathcal{C}}(Y, \prod_{i\in I}X_i) \end{array}$$

Percorrendo il diagramma da in alto a sinistra verso in basso a destra vediamo che la famiglia delle proiezioni viene mandata da un lato in f, dall'altro nel morfismo $Y \to \prod_{i\in I} X_i$ associato ai morfismi $\pi_i \circ f : Y \to X_i$. Per commutatività, f coincide proprio col morfismo corrispondente ai $\pi_i \circ f$. Per biunivocità, $f_i = \pi_i \circ f$ per ogni $i \in I$ (ricordare che f è il morfismo corrispondente agli f_i). Quindi data la famiglia $(f_i)_i$, esiste un unico morfismo $f : Y \to \prod_{i\in I} X_i$ tale che $\pi_i \circ f = f_i$ per ogni $i \in I$.

Analogamente per il coprodotto: data una qualsiasi famiglia di morfismi $f_i : X_i \to Y$, esiste un unico morfismo $f : \coprod_{i\in I} X_i \to Y$ tale che $f \circ \varepsilon_i = f_i$ per ogni $i \in I$.

Esempio: Ricordiamo che un insieme parzialmente ordinato $(P, \leq)$ induce una categoria i cui oggetti sono gli elementi di X, ed esiste un solo morfismo tra x e y se $x \leq y$, altrimenti non ne esistono. Prendiamo un insieme X, e la categoria corrispondente all'insieme parzialmente ordinato dall'inclusione $P(X)$. Detta $(U_i)_{i\in I}$ una famiglia di elementi di $P(X)$, ovvero di sottoinsiemi di X, il loro prodotto esiste ed è la loro intersezione, il loro coprodotto esiste ed è la loro unione.

Nella categoria Set, dati due morfismi $f, g : X \to Y$, definiamo

$$\ker(f, g) := \{x \in X \mid f(x) = g(x)\}$$

Scriviamo anche $\ker(X \rightrightarrows Y)$ se f e g sono sottointesi.

Definizione 38. *Sia $\mathcal{C}$ una categoria, e siano $f, g : X_0 \to X_1$ morfismi in $\mathcal{C}$.*

- *Se il funtore*
$$\mathcal{C}^{op} \to Set$$
$$Y \mapsto \ker(\mathrm{Hom}(Y, X_0) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(Y, X_1))$$
è rappresentabile, denotiamo un rappresentante con $\ker(f, g)$ e lo chiamiamo nucleo (o equalizzatore) di (f, g).
- *Se il funtore*
$$\mathcal{C} \to Set$$
$$Y \mapsto \ker(\mathrm{Hom}_{\mathcal{C}}(X_1, Y) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(X_0, Y))$$
è rappresentabile, denotiamo un rappresentante con $\mathrm{coker}(f, g)$ e lo chiamiamo conucleo (o coequalizzatore) di (f, g).
- *Una sequenza $Z \to X_0 \rightrightarrows X_1$ si dice esatta se $Z \cong \ker(X_0 \rightrightarrows X_1)$*
- *Una sequenza $X_0 \rightrightarrows X_1 \to Z$ si dice esatta se $Z \cong \mathrm{coker}(X_0 \rightrightarrows X_1)$*
- *Supponiamo che in $\mathcal{C}$ esista uno zero-oggetto 0. Sia $f : X \to Y$ un morfismo in $\mathcal{C}$. Un nucleo di f è un nucleo di $(f, 0)$ (lo denoteremo $\ker(f)$). Un conucleo di f è un conucleo di $(f, 0)$ (lo denoteremo $\mathrm{coker}(f)$).*

Per definizione, l'esistenza di nuclei e conuclei implica rispettivamente l'esistenza dei seguenti isomorfismi, funtorialmente in $Y \in Ob(\mathcal{C})$:

$$\mathrm{Hom}_{\mathcal{C}}(Y, \ker(f, g)) \cong \ker(\mathrm{Hom}_{\mathcal{C}}(Y, X_0) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(Y, X_1))$$
$$\mathrm{Hom}_{\mathcal{C}}(\mathrm{coker}(f, g), Y) \cong \ker(\mathrm{Hom}_{\mathcal{C}}(X_1, Y) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(X_0, Y))$$

Usando il primo di questi isomorfismi, possiamo considerare il morfismo $h : \ker(X_0 \rightrightarrows X_1) \to X_0$ associato al morfismo $\mathrm{Id}_{\ker(f,g)}$. Osserviamo che per definizione di nucleo, $f \circ h = g \circ h$. La funtorialità ci fa commutare il seguente diagramma, per ogni fissato morfismo $t : Y \to \ker(f, g)$ in $\mathcal{C}$:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(\ker(f,g), \ker(f,g)) & \longrightarrow & \ker(\mathrm{Hom}_{\mathcal{C}}(\ker(f,g), X_0) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(\ker(f,g), X_1)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(Y, \ker(f,g)) & \longrightarrow & \ker(\mathrm{Hom}_{\mathcal{C}}(Y, X_0) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(Y, X_1)) \end{array}$$

Prendendo l'identità in alto a sinistra, otteniamo che il morfismo corrispondente a t è $h \circ t$. Per biunivocità, ogni volta che $h \circ t = h \circ s$ abbiamo $t = s$. Ovvero, h è un monomorfismo.

Ora sia $p : Y \to X_0$ un morfismo tale che $f \circ p = g \circ p$. In altre parole $p \in \ker(\mathrm{Hom}_{\mathcal{C}}(Y, X_0) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(Y, X_1))$. Ad esso corrisponde un unico morfismo $\overline{p} \in \mathrm{Hom}_{\mathcal{C}}(Y, \ker(f, g))$. Come abbiamo visto, a $\overline{p}$ corrisponde $h \circ \overline{p}$. Per biunivocità, $p = h \circ \overline{p}$. Quindi per ogni $p : Y \to X_0$ tale che $f \circ p = g \circ p$, esiste un unico $\overline{p} : Y \to \ker(f, g)$ tale che $p = h \circ \overline{p}$.

Un ragionamento analogo vale per il conucleo: usando il secondo isomorfismo, consideriamo il morfismo $l : X_1 \to \mathrm{coker}(f, g)$ associato all'identità del conucleo. l risulta essere un epimorfismo, ed ogni volta che un morfismo $p : X_1 \to Z$ è tale che $p \circ f = p \circ g$, otteniamo un unico morfismo $\tilde{p} : \mathrm{coker}(f, g) \to Z$ tale che $p = \tilde{p} \circ l$.

7. Limiti

Sia I una categoria.

Per ogni categoria $\mathcal{C}$, un funtore $\alpha : I \to \mathcal{C}$ sarà detto un sistema induttivo in $\mathcal{C}$ indiciato da I; un funtore $\beta : I^{op} \to \mathcal{C}$ sarà detto un sistema proiettivo in $\mathcal{C}$ indiciato da I.

Esempio: Se I corrisponde ad un insieme parzialmente ordinato $(I, \leq)$, un sistema induttivo in $\mathcal{C}$ indiciato da I è il dato di una famiglia di oggetti $\{X_i\}_{i \in I}$ di $\mathcal{C}$ con, per ogni $i \leq j$ in I (cioè per ogni *morfismo* in I), un morfismo $X_i \to X_j$ in $\mathcal{C}$, tali che per ogni (*composizione*) $i \leq j \leq k$, la composizione $X_i \to X_j \to X_k$ coincida col morfismo $X_i \to X_k$.

Sia ora $\beta : I^{op} \to Set$ un sistema proiettivo. Definiamo:

$$\varprojlim \beta := \{\{x_i\}_{i \in I} \in \prod_{i \in I} \beta(i) \mid \beta(s)(x_j) = x_i \ \forall s \in \mathrm{Hom}_I(i, j)\}$$

Lemma 21. *Sia $\beta : I^{op} \to \mathcal{C}$ un sistema proiettivo, e sia $X \in Ob(Set)$. Esiste un isomorfismo naturale*

$$\mathrm{Hom}_{Set}(X, \varprojlim \beta) \cong \varprojlim \mathrm{Hom}_{Set}(X, \beta),$$

dove $\mathrm{Hom}_{Set}(X, \beta)$ denota il funtore $I^{op} \to Set$, $i \mapsto \mathrm{Hom}_{Set}(X, \beta(i))$.

Dimostrazione. Scriviamo:

$$\varprojlim \mathrm{Hom}_{Set}(X, \beta) =$$

$$= \{\{x_i\}_{i \in I} \in \prod_{i \in I} \mathrm{Hom}_{Set}(X, \beta(i)) \mid \mathrm{Hom}_{Set}(X, \beta(s))(x_j) = x_i \ \forall s \in \mathrm{Hom}_I(i, j)\}$$

Per avere la mappa dell'enunciato, associamo ad un morfismo $f : X \to \varprojlim \beta$ l'elemento $(f_i : X \to \beta(i))_{i\in I} \in \varprojlim \mathrm{Hom}_{Set}(X, \beta)$ definito da $f_i(x) := (f(x))_i$ per ogni $x \in X$, $i \in I$. Esso è ben definito, ed è un isomorfismo. □

DEFINIZIONE 39. *Sia $\mathcal{C}$ una categoria, e siano $\beta : I^{op} \to \mathcal{C}$, $\alpha : I \to \mathcal{C}$ due funtori.*

- *Se il funtore $\mathcal{C}^{op} \to Set$, $X \mapsto \varprojlim \mathrm{Hom}_{\mathcal{C}}(X, \beta)$ è rappresentabile, indichiamo con $\varprojlim \beta$ un suo rappresentante e diciamo che β ammette un limite proiettivo in $\mathcal{C}$. Per definizione abbiamo un isomorfismo*

$$\mathrm{Hom}_{\mathcal{C}}(X, \varprojlim \beta) \cong \varprojlim \mathrm{Hom}_{\mathcal{C}}(X, \beta)$$

  funtoriale in $X \in Ob(\mathcal{C})$.
- *Se il funtore $\mathcal{C} \to Set$, $X \mapsto \varprojlim \mathrm{Hom}_{\mathcal{C}}(\alpha, X)$ è rappresentabile, indichiamo con $\varinjlim \alpha$ un rappresentante e diciamo che α ammette un limite induttivo in $\mathcal{C}$. Per definizione abbiamo un isomorfismo*

$$\mathrm{Hom}_{\mathcal{C}}(\varinjlim \alpha, X) \cong \varprojlim \mathrm{Hom}_{\mathcal{C}}(\alpha, X)$$

  funtoriale in $X \in Ob(\mathcal{C})$.

In particolare se β ammette un limite proiettivo, otteniamo un isomorfismo

$$\mathrm{Hom}_{\mathcal{C}}(\varprojlim \beta, \varprojlim \beta) \cong \varprojlim \mathrm{Hom}_{\mathcal{C}}(\varprojlim \beta, \beta),$$

quindi in corrispondenza dell'identità di $\varprojlim \beta$ otteniamo una famiglia di morfismi $\rho_i : \varprojlim \beta \to \beta(i)$.

Osserviamo che il funtore $\mathrm{Hom}_{\mathcal{C}}(-, \varprojlim \beta)$ è $\mathcal{C}^{op} \to Set$.

La funtorialità ci fa commutare il seguente diagramma, per ogni fissato morfismo $f : X \to \varprojlim \beta$:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(\varprojlim \beta, \varprojlim \beta) & \longrightarrow & \varprojlim \mathrm{Hom}_{\mathcal{C}}(\varprojlim \beta, \beta) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(X, \varprojlim \beta) & \longrightarrow & \varprojlim \mathrm{Hom}_{\mathcal{C}}(X, \beta) \end{array}$$

Ne segue subito, studiando il comportamento di $\mathrm{Id}_{\varprojlim \beta}$, che l'elemento associato a f in $\varprojlim \mathrm{Hom}_{\mathcal{C}}(X, \beta)$ è $(\rho_i \circ f)_{i\in I}$. Ne segue che per ogni $(f_i)_{i\in I} \in \varprojlim \mathrm{Hom}_{\mathcal{C}}(\varprojlim \beta, \beta)$ esiste un unico morfismo $f : X \to \varprojlim \beta$ tale che $\rho_i \circ f = f_i$ per ogni $i \in I$.

N.B.: Dire che $(f_i)_{i\in I} \in \varprojlim \mathrm{Hom}_{\mathcal{C}}(\varprojlim \beta, \beta)$ significa dotare la famiglia di morfismi $f_i : \varprojlim \beta \to \beta(i)$ della seguente proprietà di compatibilità: per ogni morfismo $a : i \to j$ in I, la composizione $\beta(a) \circ f_j$ coincide con f_i.

Analogamente, se α ammette limite induttivo in $\mathcal{C}$ allora

$$\mathrm{Hom}_{\mathcal{C}}(\varinjlim \alpha, X) \cong \varprojlim \mathrm{Hom}_{\mathcal{C}}(\alpha, X),$$

funtorialmente in X. In particolare

$$\mathrm{Hom}_{\mathcal{C}}(\varinjlim \alpha, \varinjlim \alpha) \cong \varprojlim \mathrm{Hom}_{\mathcal{C}}(\alpha, \varinjlim \alpha)$$

Osserviamo che il funtore $\mathrm{Hom}_{\mathcal{C}}(\varinjlim \alpha, -)$ è $\mathcal{C} \to Set$.

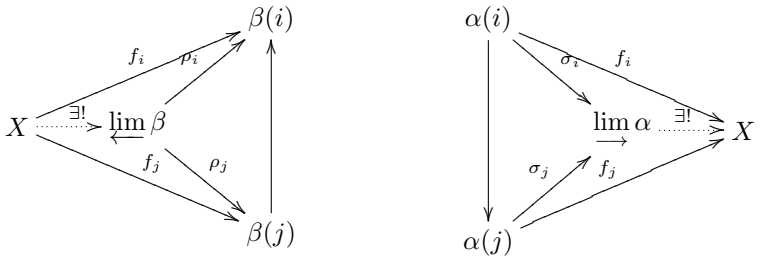
Fissato un morfismo $f : \varinjlim \alpha \to X$, andando a vedere dove va l'identità del limite induttivo nel diagramma commutativo

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(\varinjlim \alpha, \varinjlim \alpha) & \longrightarrow & \varprojlim \mathrm{Hom}_{\mathcal{C}}(\alpha, \varinjlim \alpha) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(\varinjlim \alpha, X) & \longrightarrow & \varprojlim \mathrm{Hom}_{\mathcal{C}}(\alpha, X) \end{array}$$

otteniamo che, detti $\sigma_i : \alpha(i) \to \varinjlim \alpha$ gli elementi della famiglia associata all'identità del limite induttivo, l'elemento associato ad f è $(f \circ \sigma_i)_{i \in I}$.

Similmente a prima, tutto ciò si può tradurre come segue: per ogni famiglia $(f_i : \alpha(i) \to X)_{i \in I}$ "compatibile", ovvero appartenente al "limite degli Hom" (i.e. verificante la condizione "$f_j \circ \alpha(i \to j) = f_i$ per ogni $i \to j$ in I"), esiste un'unico morfismo $f : \varinjlim \alpha \to X$ tale che $f \circ \sigma_i = f_i$ per ogni $i \in I$".

Sintetizziamo tutto ciò con due diagrammi:



Esempio: Dato un insieme X, nella categoria $P(X)$ il limite proiettivo esiste e coincide con l'intersezione, il limite induttivo esiste e coincide con l'unione.

Esempio: Una categoria si dice discreta se gli unici morfismi sono le identità. Supponiamo che I sia una categoria discreta. Allora il limite proiettivo indiciato da I coincide col prodotto indiciato da I, il limite induttivo indiciato da I coincide col coprodotto indiciato da I (ciò è immediato: arrangiare opportunamente i diagrammi qui sopra).

Esempio: Sia I una categoria con due soli oggetti, dotata oltre che delle identità, di due soli morfismi dal primo oggetto al secondo. Tale categoria si può sintetizzare con la scrittura $\bullet \rightrightarrows \bullet$.

Un funtore $I \to \mathcal{C}$ si può sintetizzare con la scrittura $f, g : X_0 \rightrightarrows X_1$, dove X_0, X_1 sono le immagini dei due oggetti e f, g sono le immagini dei due morfismi.

Ebbene, fissati f, g morfismi in $\mathcal{C}$ e una tale categoria α, il nucleo di f, g coincide col limite proiettivo di α (: $(I^{op})^{op} \to \mathcal{C}$), il conucleo di f, g coincide col limite induttivo di α. Abbiamo infatti, nel caso $\mathcal{C} = Set$,

$$\begin{aligned} \varprojlim \alpha &= \{(x_0, x_1) \in X_0 \times X_1 \mid \alpha(s)(x_j) = x_i \ \forall s \in \mathrm{Hom}_{I^{op}}(i, j)\} \\ &= \{(x_0, x_1) \in X_0 \times X_1 \mid f(x_0) = x_1,\ g(x_0) = x_1\} \\ &\cong \{x_0 \in X_0 |\ f(x_0) = g(x_0)\} = \ker(f, g), \end{aligned}$$

l'isomorfismo di insiemi essendo ben definito da $(x_0, x_1) \mapsto x_0$ (l'inverso è definito da $x \mapsto (x, f(x)) = (x, g(x))$). Generalizziamo a una qualunque categoria $\mathcal{C}$ usando

la rappresentatività: il seguente diagramma di isomorfismi commuta.

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(Y, \ker(f,g)) & \longrightarrow & \ker(\mathrm{Hom}_{\mathcal{C}}(Y, X_0) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(Y, X_1)) \\ \downarrow \exists & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(Y, \varprojlim \alpha) & \longleftarrow & \varprojlim \mathrm{Hom}_{\mathcal{C}}(Y, \alpha) \end{array}$$

ESEMPIO: Sia I la categoria vuota, e sia $\alpha : I \to \mathcal{C}$ un funtore. Se $\varprojlim \alpha$ esiste allora

$$\mathrm{Hom}_{\mathcal{C}}(Y, \varprojlim \alpha) \cong \varprojlim \mathrm{Hom}_{\mathcal{C}}(Y, \alpha) = \{\emptyset\}.$$

Per convincersene osservare che vale, per ogni famiglia di insiemi X_i indiciati sul vuoto,

$$\emptyset \in \prod_{i \in \emptyset} X_i, \qquad\qquad |\prod_{i \in \emptyset} X_i| = 1.$$

(ricordare che $\bigcup_{i \in \emptyset} X_i = \emptyset$ e la definizione di prodotto cartesiano). Quindi $\varprojlim \alpha$ è un oggetto terminale. Viceversa, ogni oggetto terminale è un limite proiettivo indiciato sul vuoto. Analogamente un oggetto iniziale è caratterizzato dall'essere un limite induttivo indiciato sul vuoto.

NOTAZIONE: Una categoria I si dice finita se la classe dei suoi morfismi è un insieme finito (quindi in particolare anche la classe degli oggetti è un insieme finito). Se ogni funtore $I^{op} \to \mathcal{C}$ (risp. $I \to \mathcal{C}$) ammette un limite proiettivo (risp. induttivo) in $\mathcal{C}$, diciamo che $\mathcal{C}$ ammette limiti proiettivi (risp. induttivi) indiciati da I. Se questa proprietà vale per ogni categoria (finita) I, allora diciamo che $\mathcal{C}$ ammette limiti proiettivi (risp. induttivi) (finiti).

Ora vogliamo descrivere i limiti usando prodotti, coprodotti, nuclei, conuclei.

Data una categoria I, indichiamo con $Mor(I)$ l'insieme dei morfismi di I. Consideriamo le due mappe naturali

$$\sigma : Mor(I) \to Ob(I), \ (i \to j) \mapsto i$$

$$\tau : Mor(I) \to Ob(I), \ (i \to j) \mapsto j$$

Sia $\mathcal{C}$ una categoria che ammette limiti proiettivi, e sia $\beta : I^{op} \to \mathcal{C}$ un funtore. Dato $s : i \to j$ morfismo in I, otteniamo i due morfismi

$$\pi_{\beta(i)}, \beta(s) \circ \pi_{\beta(j)} : \beta(i) \times \beta(j) \to \beta(i).$$

Più in generale,

$$\pi_{\sigma(s)}, \beta(s) \circ \pi_{\tau(s)} : \prod_{i \in I} \beta(i) \to \beta(\sigma(s)).$$

A tali morfismi sono associati morfismi nel prodotto, rispettivamente

$$a, b : \prod_{i \in I} \beta(i) \longrightarrow \prod_{s \in Mor(I)} \beta(\sigma(s)).$$

Similmente, se $\mathcal{C}$ ammette limiti induttivi e $\alpha : I \to \mathcal{C}$ è un funtore, otteniamo morfismi

$$c, d : \coprod_{s \in Mor(I)} \alpha(\sigma(s)) \longrightarrow \coprod_{i \in I} \alpha(i),$$

c associato a $\varepsilon_{\alpha(\sigma(s))}$, d associato a $\varepsilon_{\alpha(\tau(s))} \circ \alpha(s)$.

PROPOSIZIONE 17. *Dati α, β, a, b, c, d come sopra, assumendo che $\mathcal{C}$ ammetta limiti proiettivi e induttivi, si ha:*

$$\varprojlim \beta \cong \ker(a, b), \qquad \varinjlim \alpha \cong \operatorname{coker}(c, d).$$

DIMOSTRAZIONE. Mostriamo solo la prima affermazione (la seconda è analoga, è il duale della prima). Possiamo ridurci al caso $\mathcal{C} = Set$, in quanto se abbiamo risolto questo caso allora concludiamo notando, come abbiamo già fatto, che, fissato $Y \in Ob(\mathcal{C})$, otteniamo un quadrato di isomorfismi

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(Y, \ker(a,b)) & \longrightarrow & \ker(\mathrm{Hom}_{\mathcal{C}}(Y, X_0) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(Y, X_1)) \\ \downarrow \exists & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(Y, \varprojlim \beta) & \longleftarrow & \varprojlim \mathrm{Hom}_{\mathcal{C}}(Y, \beta) \end{array}$$

dove $X_0 = \prod_{i \in I} \beta(i)$, $X_1 = \prod_{s \in Mor(I)} \beta(\sigma(s))$. Il punto chiave sta nella freccia a destra: possiamo applicare il caso Set operando la sostituzione

$$\beta \rightsquigarrow \mathrm{Hom}_{\mathcal{C}}(Y, \beta)$$

in quanto il funtore $\mathrm{Hom}_{\mathcal{C}}(Y, \beta) : I^{op} \to Set$ induce gli stessi oggetti: per *definizione* di prodotto,

$$\prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(Y, \beta(i)) \cong \mathrm{Hom}_{\mathcal{C}}(Y, \prod_{i \in I} \beta(i)) = \mathrm{Hom}_{\mathcal{C}}(Y, X_0),$$

$$\prod_{s \in Mor(I)} \mathrm{Hom}_{\mathcal{C}}(Y, \beta(\sigma(s))) \cong \mathrm{Hom}_{\mathcal{C}}(Y, \prod_{s \in Mor(I)} \beta(\sigma(s))) = \mathrm{Hom}_{\mathcal{C}}(Y, X_1).$$

È immediato che i morfismi corrispondenti ad a e b in questo caso sono esattamente i morfismi canonici (composizione con a e con b rispettivamente).

Siamo quindi ridotti al caso Set. Sia $\mathcal{C} = Set$.

$$\begin{aligned} \ker(a,b) &= \{(x_i)_{i \in I} \in \prod_{i \in I} \beta(i) \mid \pi_{\sigma(s)}((x_i)_i) = \beta(s)(\pi_{\tau(s)}((x_i)_i)) \ \forall s \in Mor(I)\} = \\ &= \{(x_i)_{i \in I} \in \prod_{i \in I} \beta(i) \mid x_{\sigma(s)} = \beta(s)(x_{\tau(s)}) \ \forall s \in Mor(I)\} = \varprojlim \beta, \end{aligned}$$

come volevamo. □

In particolare, nella precedente dimostrazione abbiamo utilizzato solo l'esistenza di prodotti e di nuclei. Ne segue che:

- Una categoria $\mathcal{C}$ ammette limiti proiettivi finiti se e solo se ammette un oggetto terminale, un prodotto di qualsivoglia due oggetti di $\mathcal{C}$, e un nucleo di qualsivoglia due morfismi in $\mathcal{C}$ per cui il nucleo abbia senso.
- Una categoria $\mathcal{C}$ ammette limiti induttivi finiti se e solo se ammette un oggetto iniziale, un coprodotto di qualsivoglia due oggetti di $\mathcal{C}$, e un conucleo di qualsivoglia due morfismi in $\mathcal{C}$ per cui il conucleo abbia senso.

Osserviamo, senza dimostrarlo, che date tre categorie I, J, $\mathcal{C}$, esistono equivalenze

$$Fct(I \times J, \mathcal{C}) \sim Fct(J, Fct(I, \mathcal{C})) \sim Fct(I, Fct(J, \mathcal{C}))$$

Consideriamo un funtore $\beta : I^{op} \times J^{op} \to \mathcal{C}$. Usando tali equivalenze, possiamo associargli due funtori

$$\beta_J : I^{op} \to Fct(J^{op}, \mathcal{C})$$

$$\beta_I : J^{op} \to Fct(I^{op}, \mathcal{C})$$

Non dimostriamo il seguente lemma.

LEMMA 22. *Siano $I, \mathcal{C}$ categorie, e sia $X \in Ob(\mathcal{C})$. Denotiamo con ΔX il funtore $\mathcal{C} \to Fct(I, \mathcal{C})$ che manda ogni oggetto in X e ogni morfismo nell'identità di X. Sia $G : I^{op} \to \mathcal{C}$ un funtore. Allora abbiamo che*

$$\mathrm{Hom}_{\mathcal{C}}(X, \varprojlim G) \cong \mathrm{Hom}_{Fct(I^{op}, \mathcal{C})}(\Delta X, G)$$

Questo lemma ci porta in pochi passaggi al fatto che $\varprojlim \varprojlim \beta_J \cong \varprojlim \beta$. Infatti:

$$\begin{aligned}
\mathrm{Hom}_{\mathcal{C}}(X, \varprojlim \varprojlim \beta_J) &\cong \mathrm{Hom}_{Fct(J^{op}, \mathcal{C})}(\Delta X, \varprojlim \beta_J) \\
&\cong \mathrm{Hom}_{Fct(I^{op}, Fct(J^{op}, \mathcal{C}))}(\Delta\Delta X, \beta_J) \\
&\cong \mathrm{Hom}_{Fct(I^{op} \times J^{op}, \mathcal{C})}(\Delta X, \beta) \\
&\cong \mathrm{Hom}_{\mathcal{C}}(X, \varprojlim \beta)
\end{aligned}$$

Il penultimo isomorfismo si giustifica osservando che $\Delta\Delta X : I^{op} \to Fct(J^{op}, \mathcal{C})$ corrisponde a ΔX in $Fct(I^{op} \times J^{op}, \mathcal{C})$ rispetto all'equivalenza succitata.

CAPITOLO 3

Campi e teoria di Galois

1. Anello dei polinomi su un campo e campo delle frazioni di un dominio

PROPOSIZIONE 18. *Sia K un campo. $K[X]$ si dice anello dei polinomi nella indeterminata X a coefficienti in K. È un dominio di integrità e non è mai un campo. Se $f(x), g(x) \in K[X]$ e $g(x) \neq 0$ allora esistono unici $q(x), r(x) \in K[X]$ con $\deg(r(x)) < \deg(g(x))$ tali che $f(x) = q(x)g(x) + r(x)$, assunto $\deg(0) = -\infty$. Ne segue che $K[X]$ è a ideali principali (cioè un P.I.D.). $(p(x))$ è massimale in $K[X]$ se e solo se $p(x)$ è irriducibile in $K[X]$.*

DIMOSTRAZIONE. La dimostrazione dell'esistenza e l'unicità di quoziente e resto è posposta.

Proviamo che $K[X]$ è un P.I.D.. Sia quindi I un ideale di $K[X]$. L'insieme dei gradi dei polinomi di I è un sottoinsieme di $\mathbb{N}$, quindi ammette un minimo, chiamiamolo m. Sia $f(x) \in I$ monico (cioè tale che il coefficiente del termine di grado massimo è 1) tale che $\deg(f(x)) = m$. Sia ora $g(x) \in I$. Dividiamo $g(x)$ per $f(x)$ ottenendo $g(x) = q(x)f(x) + r(x)$ con $\deg(r(x)) < n$ oppure $r(x) = 0$. Ne segue che $r(x) = g(x) - q(x)f(x) \in I$, quindi $r(x) = 0$ oppure $\deg(r(x)) \geq m$ per minimalità di m. Per l'assunzione precedente, $r(x) = 0$, quindi $g(x)$ è un multiplo di $f(x)$.

Proviamo che $(p(x)) \trianglelefteq K[X]$ è massimale se e solo se $p(x)$ è irriducibile.

Sia $(p(x))$ massimale, scriviamo $p(x) = a(x)b(x)$ con $a(x), b(x) \in K[X]$ e supponiamo che $b(x) \notin K$. Allora $(p(x)) \subseteq (a(x))$, quindi $(a(x)) = K[X]$ perché se $(a(x)) = (p(x))$ allora $b(x) = b \in K$, contro l'ipotesi. Di conseguenza $a(x) \in K$, dovendo dividere 1.

Sia $p(x)$ irriducibile, e supponiamo $(p(x)) \subseteq (q(x)) \subseteq K[X]$. Allora $p(x) = q(x)h(x)$ per qualche $h(x) \in K[X]$, e poiché $p(x)$ è irriducibile, $q(x) \in K$ oppure $h(x) \in K$. Se $q(x) \in K$ allora $(q(x)) = K[X]$. Se $h(x) \in K$ allora $(q(x)) = (p(x))$. □

Con ragionamenti analoghi si mostra che se $p \in \mathbb{Z}$ è primo allora l'ideale $p\mathbb{Z} := (p)$ è massimale. Di conseguenza $\mathbb{Z}/p\mathbb{Z}$ è un campo. Lo indicheremo con $\mathbb{F}_p$.

DEFINIZIONE 40 (Campo delle frazioni per un dominio di integrità). *Sia A un dominio di integrità. Consideriamo la relazione di equivalenza su $A \times (A \setminus \{0\})$ definita da*

$$(a, b) \sim (a', b') \Leftrightarrow ab' = ba'$$

Indichiamo $[(a, b)]_\sim$ con $\frac{a}{b}$, e indichiamo l'insieme quoziente con $K(A)$. $K(A)$ è un campo con le operazioni

$$\frac{a}{b}\frac{a'}{b'} = \frac{aa'}{bb'}, \quad \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + ba'}{bb'}$$

Tali operazioni sono ben definite. L'inverso di $\frac{a}{b}$ *è* $\frac{b}{a}$. $K(A)$ *si dice campo delle frazioni del dominio* A.
Abbiamo l'immersione canonica $\varepsilon : A \to K(A),\ a \mapsto \frac{a}{1}$.
Proprietà universale: per ogni campo K *e per ogni omomorfismo iniettivo* $f : A \to K$ *esiste un unico omomorfismo* $\tilde{f} : K(A) \to K$ *tale che* $\tilde{f} \circ \varepsilon = f$ *(ovvero tale che* $\tilde{f}(\frac{a}{1}) = f(a)$ *per ogni* $a \in A$*). Esso manda* $\frac{a}{b}$ *in* $f(a)f(b)^{-1}$. *Avendo per dominio un campo,* $\tilde{f}$ *è iniettiva.*

Si osservi che nella proprietà universale, la richiesta che f sia iniettiva è necessaria per il seguente motivo: affinché $\tilde{f}$ sia omomorfismo è necessario che se $\frac{a}{b} \in K(A)$ allora $\tilde{f}(\frac{a}{b}) = \tilde{f}(\frac{a}{1}\frac{1}{b}) = \tilde{f}(\frac{a}{1})\tilde{f}(\frac{1}{b}) = f(a)\tilde{f}((\frac{b}{1})^{-1})$. Quindi bisogna che se $b \neq 0$ anche $f(b) \neq 0$.

Nel linguaggio delle categorie il campo $K(A)$ rappresenta il funtore che manda un campo K nell'insieme degli omomorfismi iniettivi $A \to K$.

DEFINIZIONE 41. $K[X_1, ..., X_n]$ *si dice anello dei polinomi a coefficienti in* K *con le indeterminate simultanee* $X_1, ..., X_n$. $K(X_1, ..., X_n)$ *è il campo dei quozienti di* $K[X_1, ..., X_n]$.

DEFINIZIONE 42. *Sia* K *campo con* $S \subseteq K$ *non vuoto. Indichiamo con* $[S]$ *il sottoanello di* K *generato da* S*, che è per definizione l'intersezione dei sottoanelli di* K *contenenti* S*, e con* (S) *il sottocampo di* K *generato da* S*, che è per definizione l'intersezione dei sottocampi di* K *contenenti* S.

DEFINIZIONE 43 (Caratteristica). *Sia* R *un anello. Allora esiste un unico omomorfismo di anelli* $g : \mathbb{Z} \to R$. g *manda* $n \in \mathbb{Z}$ *in* $n \cdot 1_R$ *se* $n > 0$*, in* 0_R *se* $n = 0$*, in* $(-n) \cdot 1_R$ *se* $n < 0$*, dove se* $0 < n \in \mathbb{Z}$ *e* $r \in R$*,*

$$n \cdot r := r + ... + r \ (n \text{ volte})$$

Il nucleo di g *è un ideale di* $\mathbb{Z}$*, quindi è principale, generato da* $0 \leq c \in \mathbb{Z}$. c *è univocamente individuato, si indica con* $\chi(R)$ *e si dice caratteristica di* R.

Si osservi che se R è un dominio di integrità, la sua caratteristica è 0 oppure un numero primo. Infatti indicato con $g : \mathbb{Z} \to R$ l'unico omomorfismo di anelli siffatto, se $ker(g) = (c)$ allora $c \cdot 1_R = 0_R$. Se $0 < c = ab$ con $a, b \in \mathbb{Z}$ positivi, allora $0_R = c \cdot 1_R = ab \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R)$, quindi $a \cdot 1_R = 0_R$ oppure $b \cdot 1_R = 0_R$ perché R è un dominio. Supponiamo senza perdita in generalità che $a \cdot 1_R = 0_R$. Allora $a \in ker(g) = (c)$ quindi $a = cd$ per qualche $d \in \mathbb{Z}$. Allora $c = ab = cdb$ quindi $db = 1$ perché $\mathbb{Z}$ è un dominio. Quindi $b = 1$ essendo b positivo e un'unità in $\mathbb{Z}$.

In particolare se K **è un campo,** $\chi(K)$ **è** 0 **oppure un numero primo**. D'altra parte come visto nella proposizione 16 un dominio di integrità finito è un campo.

PROPOSIZIONE 19 (Anelli primi, campi primi). *L'anello primo di un anello* R *è l'intersezione di tutti i suoi sottoanelli, ed è isomorfo a* $\mathbb{Z}$ *se* $\chi(R) = 0$*, a* $\mathbb{Z}/n\mathbb{Z}$ *se* $\chi(R) = n$*. Il campo primo di un campo* K *è l'intersezione di tutti i suoi sottocampi. È isomorfo a* $\mathbb{Q}$ *se* $\chi(K) = 0$*, a* $\mathbb{F}_p$ *se* $\chi(K) = p$.

DIMOSTRAZIONE. Osserviamo che dato l'omomorfismo $g : \mathbb{Z} \to R$, la sua immagine, chiamiamola R_0, è l'anello primo di R. Per il primo teorema di isomorfismo, detto $n = \chi(R)$, $\mathbb{Z}/n\mathbb{Z} \cong R_0$. Se $n = 0$, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}$.

Ora sia K un campo e sia $g : \mathbb{Z} \to K$ l'unico omomorfismo siffatto. Sia K_0 il campo primo di K. Certamente $g(\mathbb{Z}) \subseteq K_0$ quindi possiamo restringere il codominio e considerare $g : \mathbb{Z} \to K_0$.

Se la caratteristica di K è il numero primo p, allora $g(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ è un campo, quindi $g(\mathbb{Z}) = K_0$, essendo K_0 il sottocampo minimale di K. Ma allora $K_0 \cong \mathbb{Z}/p\mathbb{Z}$.

Se invece la caratteristica di K è 0, l'omomorfismo $g : \mathbb{Z} \to K_0$ è iniettivo. $\mathbb{Q}$ è per definizione il campo delle frazioni del dominio $\mathbb{Z}$, quindi per la proprietà universale esiste un unico omomorfismo $\tilde{g} : \mathbb{Q} \to K_0$ che manda $\frac{a}{1}$ in $g(a)$, ed è iniettivo. Per mostrare che $K_0 \cong \mathbb{Q}$ basta mostrare che $\tilde{g}$ è suriettivo, ovvero per minimalità di K_0, basta mostrare che $g(\mathbb{Q})$ è un campo. Sia $g(\frac{a}{b}) \neq 0$. Allora $a \neq 0$, e $g(\frac{a}{b})g(\frac{b}{a}) = g(\frac{a}{b}\frac{b}{a}) = g(1) = 1$. Quindi $g(\frac{a}{b})$ è invertibile. □

Ecco un semplice risultato utile in seguito:

LEMMA 23. *Sia K un campo e sia K_0 il suo campo primo. Allora ogni automorfismo di K ristretto a K_0 è l'identità.*

DIMOSTRAZIONE. Basta osservare che K_0 è il più piccolo sottocampo di K contenente 0 e 1, quindi è ottenuto da 0 e 1 sommando, sottraendo, moltiplicando o dividendo elementi ottenuti in questo modo a partire da 0 e 1. Poiché ogni automorfismo di K fissa 0 e 1 e rispetta tutte queste operazioni, esso fissa ogni elemento di K_0. □

2. L'endomorfismo di Frobenius

Se il campo K ha caratteristica p, ovvero se il suo campo primo è $\mathbb{F}_p$, consideriamo la mappa

$$\phi : K \to K$$

$$a \mapsto a^p.$$

Esso è un omomorfismo, detto "endomorfismo di Frobenius". Nella fattispecie, per mostrare che $(a + b)^p = a^p + b^p$ si osserva che sviluppando il binomio secondo Newton si ottiene:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i.$$

Se $1 \leq i \leq p-1$ si ha

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-i+1)}{i \cdot (i-1) \cdot \ldots \cdot 2 \cdot 1} \equiv 0 \ mod(p).$$

Infatti il denominatore non può avere fattori comuni con p, essendo quest'ultimo primo ed essendo $i < p$. Quindi nella sommatoria sopravvivono solo $i = 0$ e $i = p$, porgendo il risultato che volevamo dimostrare.

3. Struttura di un'estensione semplice

DEFINIZIONE 44. *Siano $K \leq L$ campi. L si dice sovracampo, estensione o ampliamento di K. Si usa la notazione L/K. Se esiste $u \in L$ tale che $L = K(u)$ (ovvero L è generato dagli elementi di K e da u) allora L si dice estensione semplice di K.*

DEFINIZIONE 45 (Grado di un'estensione). *Se $K \leq L$, L si atteggia in modo naturale a spazio vettoriale su K. La dimensione di L rispetto a K si dice grado o dimensione dell'estensione L/K e si indica con $[L : K]$. Se $[L : K]$ è finito L si dice estensione finita (i.e. di grado finito) di K.*

Ora definiamo i nostri strumenti.

TEOREMA 13. *Sia L/K un'estensione di campi, e sia $u \in L$. Esiste un unico omomorfismo $v_u : K[X] \to L$ che è l'identità su K e manda x in u. Esso è l'omomorfismo di valutazione (o "omomorfismo di sostituzione") in u: manda il polinomio $f(x)$ in $f(u) \in L$.*

- *u si dice algebrico su K se v_u non è iniettiva, ovvero se esiste $0 \neq f(x) \in K[X]$ tale che $f(u) = 0$.*
- *u si dice trascendente su K se v_u è iniettiva, ovvero se $0 \in K[X]$ è l'unico polinomio che ammette u come zero.*

Indicheremo $v_u(K[X])$ con $K[u]$.

Se u è algebrico su K abbiamo che $v_u : K[X] \to L$ non è iniettiva, quindi ammette un nucleo non nullo che è un'ideale di $K[X]$, quindi principale, generato da un polinomio monico irriducibile univocamente individuato, $f(x)$, detto il polinomio minimo di u su K. $f(x)$ è il polinomio monico di grado minimo tra quelli che ammettono u come zero. $K[u] \cong K[X]/(f(x))$ è un campo, essendo $f(x)$ irriducibile in $K[X]$, o equivalentemente essendo $(f(x))$ ideale massimale di $K[X]$. Quindi $K[u] = K(u)$. Il grado dell'estensione $[K(u) : K]$ coincide con il grado del polinomio f, e detto esso n, una base di $K(u)$ su K è $\{1, u, u^2, ..., u^{n-1}\}$.

Se u è trascendente su K allora $K[u] \cong K[X]$.

DIMOSTRAZIONE. Per l'unicità di v_u si osservi che se $g : K[X] \to L$ fissa K e manda x in u allora detto $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, $v_u(f(x)) = v_u(a_n x^n + ... + a_1 x + a_0) = a_n v_u(x)^n + ... + a_1 v_u(x) + a_0 = a_n u^n + ... + a_1 u + a_0 = f(u)$. Ora sia u algebrico su K, e sia I il nucleo di v_u. Allora I è principale, e possiamo scegliere il generatore monico (eventualmente dividendo per il coefficiente direttore): $I = (f(x))$ con $f(x)$ monico. Dobbiamo mostrare che $f(x)$ è irriducibile e univocamente individuato.

Proviamo che $f(x)$ è irriducibile. Supponiamo che $f(x) = g(x)h(x)$ per qualche $g(x), h(x) \in K[X]$. Dobbiamo mostrare che uno dei due fattori è invertibile in $K[X]$ (ovvero appartiene a K). Abbiamo $f(u) = g(u)h(u) = 0$, e quindi $g(u) = 0$ oppure $h(u) = 0$ essendo L un campo (e quindi un dominio). Supponiamo senza perdita in generalità che $g(u) = 0$. Allora $g(x) \in ker(v_u) = (f(x))$, quindi $g(x) = f(x)l(x)$ per qualche $l(x) \in K[X]$. Ne segue che $f(x) = g(x)h(x) = f(x)l(x)h(x)$, ed essendo $f(x) \neq 0$ abbiamo $l(x)h(x) = 1$. Ciò significa che $l(x)$ e $h(x)$ hanno grado 0 quindi sono costanti (elementi di K). Infatti il grado di $l(x)h(x)$ è la somma del grado di $l(x)$ col grado di $h(x)$, e tale somma deve fare 0 (il grado di 1).

Proviamo che $f(x)$ è unico. Supponiamo $(f(x)) = (g(x))$ con $g(x)$ monico. Allora $f(x) = g(x)h(x)$ e $g(x) = f(x)l(x)$, da cui $f(x) = f(x)l(x)h(x)$, quindi $l(x)$ e $h(x)$ sono elementi di K: $l(x) = l \in K$, $h(x) = h \in K$. Ma $g(x) = lf(x)$ quindi $l = 1$ essendo $g(x)$ monico.

Sia n il grado di $f(x) = a_n x^n + ... + a_1 x + a_0$. Un elemento di $K[u]$ è del tipo $g(u)$ per qualche $g(x) \in K[X]$. Effettuiamo la divisione con resto di $g(x)$ per $f(x)$: $g(x) = q(x)f(x) + r(x)$ ove il grado di $r(x)$ è minore di n oppure $r(x) = 0$. Allora si ha $g(u) = q(u)f(u) + r(u) = r(u)$ essendo $f(u) = 0$. Ne segue che un qualunque

elemento di $K[u]$ è del tipo $g(u)$ con $g(x) \in K[X]$ di grado minore di n. Viceversa ogni tale elemento sta in $K[u]$. Ne segue che $\{1, u, u^2, ..., u^{n-1}\}$ è un insieme di generatori per $K[u]$. Ci rimane da mostrare che è anche linearmente indipendente. Se $b_0+b_1u+b_2u^2+...+b_{n-1}u^{n-1} = 0$ allora $h(x) := b_0+b_1x+...+b_{n-1}x^{n-1} \in K[X]$, se non è il polinomio nullo, ha grado minore di n e ammette u come zero. Il che è assurdo perché contraddice la minimalità del grado di f. Quindi $h(x) = 0$, ovvero $b_0 = b_1 = ... = b_{n-1} = 0$. □

4. Formula dei gradi

DEFINIZIONE 46. *Un'estensione L/K si dice algebrica se ogni $u \in L$ è algebrico su K.*

TEOREMA 14 (Formula dei gradi). *Siano $K \leq L \leq M$ campi. Allora $[M : K]$ è finito se e solo se $[M : L]$ e $[L : K]$ sono finiti. In tal caso*

$$[M : K] = [M : L][L : K]$$

DIMOSTRAZIONE. Supponiamo che $[M : K] = m$ sia finito, e sia $\{u_1, ..., u_m\}$ una K-base di M. Allora $\{u_1, ..., u_m\}$ è un insieme di generatori per M come L-spazio vettoriale, quindi $[M : L]$ è finito. Inoltre ogni elemento di L è combinazione lineare degli u_i con coefficienti in K, quindi anche $[L : K]$ è finito. Ora supponiamo che $[M : L] = n$ e $[L : K] = r$ siano finiti, e siano $\{v_1, ..., v_n\}$ e $\{w_1, ..., w_r\}$ rispettivamente una L-base di M e una K-base di L. Dato $v \in M$, $v = a_1v_1 + ... + a_nv_n$ con $a_i \in L$ per ogni $i = 1, ..., n$. Inoltre per ogni $i = 1, ..., n$, $a_i = b_{i1}w_1 + ... + b_{ir}w_r$ con $b_{ij} \in K$ per ogni $j = 1, ..., r$. Di conseguenza $\{v_iw_j \mid i = 1, ..., n,\ j = 1, ..., r\}$ è un insieme di generatori per M su K. Rimane da mostrare che esso è linearmente indipendente. Supponiamo quindi che per qualche $a_{ij} \in K$,

$$\sum_{i=1}^{n}\sum_{j=1}^{r} a_{ij}v_iw_j = \sum_{i=1}^{n}(\sum_{j=1}^{r} a_{ij}w_j)v_i = 0$$

Per l'indipendenza lineare dei v_i su L, per ogni $i = 1, ..., n$ si ha

$$\sum_{j=1}^{r} a_{ij}w_j = 0$$

Per l'indipendenza lineare dei w_j su K, per ogni $j = 1, ..., r$ si ha $a_{ij} = 0$. □

Di conseguenza:

- Ogni estensione finita è algebrica: se $[L : K]$ è finito e $u \in L$ allora $[L : K(u)]$ e $[K(u) : K]$ sono finiti. In particolare $[K(u) : K]$ è finito, quindi u è algebrico su K.
- Gli elementi di L algebrici su K formano un campo, chiamato chiusura algebrica relativa di K in L. Infatti se u e v sono elementi di L algebrici su K, $K \leq K(u) \leq K(u, v)$, e v è algebrico su $K(u)$ (essendolo su K). Quindi $[K(u)(v) : K(u)]$ e $[K(u) : K]$ sono finiti. Per il teorema precedente $[K(u, v) : K]$ è finito. Quindi poiché $K \leq K(uv) \leq K(u, v)$ e $K \leq K(u + v) \leq K(u, v)$, anche $[K(uv) : K]$ e $[K(u + v) : K]$ sono finiti. Di conseguenza anche uv e $u + v$ sono algebrici su K.
- Per induzione dal caso precedente, se $u_1, ..., u_r$ sono elementi di L algebrici su K allora l'estensione $K(u_1, ..., u_r)/K$ è finita.
- Se M/L e L/K sono algebriche, M/K è algebrica.

5. Campi di riducibilità completa

PROPOSIZIONE 20 (esistenza di zeri). *Siano K campo e sia $f(x) \in K[X]$ di grado positivo. Allora esiste $L \geq K$ in cui $f(x)$ ha uno zero.*

DIMOSTRAZIONE. Poiché $K[X]$ è U.F.D., possiamo scrivere $f(x) = p(x)l(x)$ con $p(x) \in_{irr} K[X]$. Poniamo $L := K[X]/(p(x))$. Sia

$$\phi : K \to L$$

$$a \mapsto a + (p(x))$$

Sia $\overline{K} := \phi(K) \leq L$. Poiché $\deg(p(x)) \geq 1$, ϕ è iniettiva: se $a + (p(x)) = b + (p(x))$ allora $a - b$ è un multiplo di $p(x)$, quindi dev'essere uguale a 0 (se non lo fosse sarebbe un polinomio di grado 0). Quindi $K \cong \overline{K} \leq L$. Ne segue che L è un'estensione di K. Consideriamo

$$u := x + (p(x)) \in L$$

Se $p(x) = a_0 + a_1 x + ... + a_t x^t$, in L

$$\begin{aligned} p(u) &= p(x + (p(x))) = \overline{a_0} + \overline{a_1}(x + (p(x))) + ... + \overline{a_t}(x + (p(x)))^t \\ &= a_0 + (p(x)) + (a_1 + (p(x)))(x + (p(x))) + ... + (a_t + (p(x)))(x^t + (p(x))) \\ &= (a_0 + a_1 x + ... + a_t x^t) + (p(x)) = p(x) + (p(x)) = (p(x)) = 0_L. \end{aligned}$$

Dunque in L $f(u) = p(u)l(u) = 0l(u) = 0$. Quindi L può essere ottenuto da K tramite aggiunzione di u. □

DEFINIZIONE 47 (Campo di riducibilità completa). *Sia K campo e sia $f(x) \in K[X]$, di grado maggiore di 0. $M \geq K$ è detto campo di riducibilità completa (c.r.c.), o split, o campo di spezzamento, di $f(x)$ su K se valgono i seguenti fatti:*

1. *$M = K(u_1, ..., u_r)$ dove $f(u_i) = 0$ $\forall i = 1, ..., r$.*
2. *$f(x)$ si fattorizza in $M[X]$ in fattori lineari, cioè di grado 1.*

Equivalentemente, M è un campo minimale rispetto a

1. *$M \geq K$.*
2. *Se $p(x) \in_{irr} M[X]$ e $p(x)|f(x)$, allora $\deg(p(x)) = 1$.*

TEOREMA 15. *Sia K campo, e $f(x) \in K[X]$ con $n := \deg(f(x)) \geq 1$. Allora esiste un c.r.c. M su K. È $[M : K] \leq n!$, e anzi $[M : K]$ divide $n!$.*

DIMOSTRAZIONE. Per induzione su n. Se $n = 1$, scelgiamo $M = K$. Sia ora $n > 1$. Scriviamo

$$f(x) = f_1(x) f_2(x)$$

con $f_1(x) \in_{irr} K[X]$. Per l'esistenza di zeri, esiste $K(u_1)$ con $f_1(u_1) = 0$, e quindi $f(u_1) = 0$.

$$[K(u_1) : K] = \deg(f_1(x)) \leq n$$

e in $K(u_1)[X]$

$$f(x) = h(x)(x - u_1).$$

Per ipotesi induttiva esiste un c.r.c. M di $h(x)$ su $K(u_1)$, e

$$[M : K(u_1)] \leq (n-1)!$$

Quindi

$$[M : K] = [M : K(u_1)][K(u_1) : K] \leq (n-1)!n = n!$$

Inoltre in $M[X]$

$$f(x) = (x - u_1)(x - u_2)...(x - u_n)$$

dove $u_2, ..., u_n$ sono zeri di $h(x)$ e $u_1 \in M$. Quindi M è c.r.c. di $f(x)$ su K. □

PROPOSIZIONE 21. *Se M è c.r.c. su un campo K di $f(x) \in K[X]$ con $\deg(f(x)) = n$ e $[M : K] = n!$, allora $f(x)$ è irriducibile in $K[X]$.*

DIMOSTRAZIONE. Poiché $[M : K] \leq n!$, basta provare che se $f(x)$ è riducibile allora $[M : K] < n!$. Sia quindi $f(x) = h(x)g(x)$ con $h(x) \in_{irr} K[X]$ e $\deg(h(x)) < \deg(f(x)) = n$. Se $u \in M$ è zero di $h(x)$, M è c.r.c. su $K(u)$ di $f(x)$, essendolo su K, quindi è c.r.c. di $l(x)g(x)$ dove $f(x) = (x-u)l(x)g(x)$, e $\deg(l(x)g(x)) = n-1$, da cui $[M : K(u)] \leq (n-1)! \Rightarrow [M : K] = [M : K(u)][K(u) : K] \leq (n-1)![K(u) : K] < (n-1)!n = n!$. □

Osserviamo che se A e T sono anelli commutativi, $\sigma : A \to T$ è omomorfismo, e $c \in T$, allora esiste un unico omomorfismo $\overline{\sigma} : A[X] \to T$ tale che $\overline{\sigma}|A = \sigma$ e $\overline{\sigma}(x) = c$.

TEOREMA 16. *Siano K e $\overline{K}$ campi, $\sigma : K \to \overline{K}$ isomorfismo. Allora σ si estende in modo unico ad un isomorfismo di $K[X]$ su $\overline{K}[\overline{X}]$ in cui x va in $\overline{x}$. Sia $f(x) \in_{irr} K[X]$ e sia $\overline{f}(\overline{x})$ il corrispondente in $\overline{K}[\overline{X}]$. Siano $L := K(u) = K[u]$, $\overline{L} := \overline{K}(\overline{u}) = \overline{K}[\overline{u}]$, ove u è zero di $f(x)$ e $\overline{u}$ è zero di $\overline{f}(\overline{x})$. Allora esiste un isomorfismo di L su $\overline{L}$ che estende σ e manda u in $\overline{u}$, esso è unico.*

DIMOSTRAZIONE. σ si estende a

$$\widehat{\sigma} : K[X] \to \overline{K}[\overline{X}]$$

$$g(x) = g_0 + g_1 x + ... + g_t x^t \mapsto \overline{g}(\overline{x}) = \overline{g_0} + \overline{g_1}\ \overline{x} + ... + \overline{g_t}\ \overline{x}^t$$

dove $\overline{g_i} := \sigma(g_i)\ \forall i = 1, ..., t$. È isomorfismo perché è suriettivo e se $\overline{g}(\overline{x}) = 0$, $\overline{g_i} = 0\ \forall i = 1, ..., t$ quindi $g_i = 0\ \forall i = 1, ..., t$, quindi $g(x) = 0$. Sia ora

$$\widehat{\sigma}^* : K[X]/(f(x)) \to \overline{K}[\overline{X}]/(\overline{f}(\overline{x}))$$

$$g(x) + (f(x)) \mapsto \overline{g}(\overline{x}) + (\overline{f}(\overline{x}))$$

$\widehat{\sigma}^*$ è isomorfismo (verifica diretta). Siano

$$\alpha : K[X]/(f(x)) \to K[u] = K(u)$$

$$\beta : \overline{K}[\overline{X}]/(\overline{f}(\overline{x})) \to \overline{K}[\overline{u}] = \overline{K}(\overline{u})$$

gli isomorfismi indotti dall'omomorfismo di sostituzione. Allora

$$\beta \circ \widehat{\sigma}^* \circ \alpha^{-1} : K(u) \to \overline{K}(\overline{u})$$

è l'isomorfismo cercato. Abbiamo quindi il seguente diagramma commutativo:

$$\begin{array}{ccc} K[X]/(f(x)) & \xrightarrow{\alpha} & K[u] \\ \downarrow{\scriptstyle \widehat{\sigma}^*} & & \downarrow{\scriptstyle \beta \circ \widehat{\sigma}^* \circ \alpha^{-1}} \\ \overline{K}[\overline{X}]/\overline{f}(\overline{x}) & \xrightarrow{\beta} & \overline{K}[\overline{u}] \end{array}$$

□

TEOREMA 17. *Sia $\sigma : K \to \overline{K}$ isomorfismo di campi, e $\widehat{\sigma} : K[X] \to \overline{K}[\overline{X}]$ la sua estensione ai rispettivi anelli di polinomi; sia $f(x) \in K[X]$ e $\overline{f}(\overline{x}) := \widehat{\sigma}(f(x))$; siano M e $\overline{M}$ c.r.c. di $f(x)$ e $\overline{f}(\overline{x})$ rispettivamente, su K e $\overline{K}$ rispettivamente, dove $\deg(f(x)) > 0$. Allora σ si estende a un isomorfismo di M su $\overline{M}$. Il numero dei modi in cui σ si può estendere è minore o uguale di $[M : K]$, ed è proprio $[M : K]$*

se e solo se i fattori irriducibili di $f(x)$ si fattorizzano in $M[X]$ in fattori lineari a due a due non associati (i.e. in M ciascuno ha zeri distinti).

DIMOSTRAZIONE. Ricordiamo che se $h(x) \in_{irr} K[X]$ e $h(u) = 0$, $\overline{h}(\overline{u}) = 0$, allora esiste un unico isomorfismo $\overline{\sigma} : K(u) \to \overline{K}(\overline{u})$ tale che $\overline{\sigma}|K = \sigma$ e $\overline{\sigma}(u) = \overline{u}$, come visto nel teorema 16.

Dimostriamo l'asserto per induzione sul grado $n := [M : K]$.

Se $n = 1$, $M = K$ quindi $f(x)$ si fattorizza completamente in $K[X]$. Quindi $\overline{f}(\overline{x})$ si fattorizza completamente in $\overline{K}[\overline{X}]$, quindi $\overline{M} = \overline{K}$ e si deve prendere proprio σ. Di conseguenza c'è un solo modo di estendere σ se $n = 1$.

Sia ora $n \geq 2$.

Sia $h(x) \in_{irr} K[X]$ di grado maggiore di 1 e valga $f(x) = h(x)t(x)$ in $K[X]$. Questo è possibile perché $K[X]$ è U.F.D. e se tutti i polinomi irriducibili di $K[X]$ che dividono $f(x)$ avessero grado 1 allora K sarebbe uguale a M. Abbiamo $\overline{h}(\overline{x}) \in_{irr} \overline{K}[\overline{X}]$, $\overline{h}(\overline{x})|\overline{f}(\overline{x})$ e M, $\overline{M}$ sono c.r.c. di $f(x)$ e $\overline{f}(\overline{x})$ su $K(u)$ e $\overline{K}(\overline{u})$ rispettivamente (essendolo su K e $\overline{K}$ rispettivamente). Inoltre dalla formula dei gradi $[M : K(u)] < [M : K]$, quindi per ipotesi induttiva $\overline{\sigma}$ si estende ad un isomorfismo di M su $\overline{M}$. Il numero delle possibili estensioni siffatte è, sempre per ipotesi induttiva, minore o uguale di $[M : K(u)]$.

Ora sia u zero di $h(x)$, e siano $\overline{u_1}, \overline{u_2}, ..., \overline{u_r}$ gli zeri distinti di $\overline{h}(\overline{x})$ in $\overline{M}$. Sia

$$\sigma_i : K(u) \to \overline{K}(\overline{u_i})$$

l'isomorfismo che estende σ e manda u in $\overline{u_i}$ (esso è unico). Evidentemente

$$r \leq \deg(h(x)) = [K(u) : K].$$

Poiché $[M : K(u)] < [M : K]$, per l'ipotesi induttiva σ_i si può estendere a M in al più $[M : K(u)]$ modi, e il numero di isomorfismi costruiti in questo modo è al più

$$[K(u) : K][M : K(u)] = [M : K]$$

Per concludere basta mostrare che ogni isomorfismo $\phi : M \to \overline{M}$ che estende σ si ottiene estendendo qualche σ_i: se u è zero di $h(x)$, $\phi(u)$ è zero di $\overline{\phi}(h(x))$, dove $\overline{\phi}$ è l'unico isomorfismo $M[X] \to \overline{M}[\overline{X}]$ che estende ϕ. Infatti se $h(x) = a_n x^n + ...a_1 x + a_0$ allora $\overline{\phi}(h(x)) = \phi(a_n)\overline{x}^n + ... + \phi(a_1)\overline{x} + \phi(a_0)$ e quindi

$$\begin{aligned} \overline{\phi}(h(\phi(u))) &= \phi(a_n)\phi(u)^n + ... + \phi(a_1)\phi(u) + \phi(a_0) \\ &= \phi(a_n u^n + ... + a_1 u + a_0) = \phi(h(u)) = \phi(0) = 0. \end{aligned}$$

Quindi $\phi(u) = \overline{u}_i$ per qualche $i \in \{1, ..., r\}$, ovvero $\phi|_{K(u)} = \sigma_i$.
Per studiare l'uguaglianza, si ripercorra la dimostrazione ricordando che se $f(x) \in K[X]$ è tale che ogni suo fattore irriducibile ha zeri distinti, allora conserva tale proprietà in ogni estensione di K. Si ricordi che nelle notazioni usate in tale dimostrazione, $h(x)$ si fattorizza in fattori lineari distinti se e solo se il suo grado è proprio r. □

DEFINIZIONE 48. *Siano K campo, $L, \overline{L} \geq K$. Un isomorfismo $\sigma : L \to \overline{L}$ si dice K-isomorfismo se $\sigma|_K$ è l'identità. Se $\overline{L} = L$ si parla di K-automorfismi di L.*

Dal teorema 17 segue:

- Sia K campo, sia $f(x) \in K[X]$ di grado positivo. Siano M e $\overline{M}$ c.r.c. per $f(x)$ su K. Allora M e $\overline{M}$ sono K-isomorfi. Basta applicare il teorema 17 con $\overline{K} = K$ e $\sigma = id_K$.

- Siano K campo, $f(x) \in K[X]$ di grado positivo, M c.r.c. su K di $f(x)$. Allora i K-automorfismi di M sono al più $[M : K]$, e sono esattamente $[M : K]$ se e solo se i fattori irriducibili di $f(x)$ hanno zeri distinti.
- Siano $T \geq K$ campi, $f(x) \in K[X]$ di grado positivo. Allora esiste al più un c.r.c. di $f(x)$ su K contenuto in T.

Esempi.

1. $\mathbb{Q}(i)$ è c.r.c. su $\mathbb{Q}$ di $x^2 + 1$, e i $\mathbb{Q}$-automorfismi di $\mathbb{Q}(i)$ sono $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ perché i fattori irriducibili di $x^2 + 1$ hanno zeri distinti.

2. $\mathbb{F}_p(y)$, ove y è trascendente su $\mathbb{F}_p$, è c.r.c. per $x^p - y^p$ su $\mathbb{F}_p(y^p)$. Poiché $x^p - y^p = (x - y)^p$, esiste un solo $\mathbb{F}_p(y^p)$-automorfismo di $\mathbb{F}_p(y)$.

Teorema 18. *Siano K campo, e $L \geq K$. Le seguenti affermazioni sono equivalenti:*

(1) *L è c.r.c. per qualche $f(x) \in K[X]$*
(2) *$[L : K] < \infty$ e ogni $g(x) \in K[X]$ avente uno zero in L si fattorizza completamente in $L[X]$ (i.e. L contiene un c.r.c. di $g(x)$).*

Dimostrazione.
(1) $\Rightarrow$ (2). Da (1) segue immediatamente che $[L : K] < \infty$. Infatti L è ottenuto da K mediante aggiunzione di elementi algebrici su K. Sia $g(x) \in K[X]$ tale che esista $u \in L$ con $g(u) = 0$, e scriviamo $g(x) = h(x)t(x)$ con $h(x) \in_{irr} L[X]$. Sia v zero di $h(x)$ in una opportuna estensione S di L. Si ha $L(v) \leq S$. L'identità di K si estende ad un isomorfismo σ di $K(u)$ su $K(v)$, essendo u e v zeri di $g(x)$. L è c.r.c. di $f(x)$ su $K(u)$, e $L(v)$ è c.r.c. di $\sigma(f(x)) = f(x)$ su $K(v)$, quindi σ si estende ad un K-automorfismo di L su $L(v)$ (teorema 17), quindi L e $L(v)$ sono entrambi c.r.c. per $f(x)$ su K ed entrambi sono contenuti in $L(v)$. Quindi $L = L(v)$, ovvero $v \in L$.

(2) $\Rightarrow$ (1). Valga (2). $L = K(a_1, ..., a_n)$ dove $\{a_1, ..., a_n\}$ è una base per L su K. Siano $f_1(x), ..., f_n(x)$ i polinomi minimi di $a_1, ..., a_n$ rispettivamente, su K. Allora L è c.r.c. su K di $f(x) := f_1(x)...f_n(x)$. □

6. Separabilità dei polinomi irriducibili

Definizione 49 (derivata formale). *Sia K campo, e sia*

$$f(x) := \sum_{i=0}^{n} a_i x^i \in K[X]$$

La derivata formale di $f(x)$ è

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$$

Proposizione 22. *L'operatore di derivata formale è endomorfismo di $K[X]$ come spazio vettoriale. Inoltre se $f(x),\ g(x) \in K[X]$,*

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$$

Dimostrazione. Per non cercare di costruire una noiosa dimostrazione dettagliata, ricorrere all'analisi. □

Proposizione 23. *Siano K campo, $f(x) \in K[X],\ a \in K$. Le seguenti affermazioni sono equivalenti:*

(1) $(x-a)^2|f(x)$, *cioè* a *è zero multiplo di* $f(x)$.
(2) $(x-a)|f(x)$ *e* $(x-a)|f'(x)$, *cioè* a *è zero di* $f(x)$ *e di* $f'(x)$.

DIMOSTRAZIONE. Valga (1). Allora $f(x) = (x-a)^2 g(x)$ per qualche $g(x) \in K[X]$. Di conseguenza $(x-a)$ divide $f(x)$. Inoltre $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x) = (x-a)(2g(x) + (x-a)g'(x))$. Quindi $(x-a)$ divide $f'(x)$.

Valga (2). Allora $f(x) = (x-a)h(x)$ per qualche $h(x) \in K[X]$. Inoltre $f'(x) = h(x) + (x-a)h'(x) = (x-a)l(x)$ per qualche $l(x) \in K[X]$. Di conseguenza $x-a$ divide $h(x)$, ovvero $h(x) = (x-a)s(x)$ per qualche $s(x) \in K[X]$ (nella fattispecie $s(x) = l(x) - h'(x)$). Quindi $f(x) = (x-a)h(x) = (x-a)^2 s(x)$. Quindi $(x-a)^2$ divide $f(x)$. □

PROPOSIZIONE 24. *Siano* K *campo,* $f(x) \in_{irr} K[X]$. *Le seguenti affermazioni sono equivalenti:*

(1) *In ogni estensione di* K *gli eventuali zeri di* $f(x)$ *sono tutti semplici.*
(2) *Esiste una estensione di* K *in cui* $f(x)$ *ha uno zero semplice.*
(3) $f'(x) \neq 0$.

DIMOSTRAZIONE.
(1) $\Rightarrow$ (2). Basta prendere un c.r.c. per $f(x)$ su K.

(2) $\Rightarrow$ (3). Sia L una estensione di K in cui $f(x)$ ha uno zero, sia esso a. Se $f'(x) = 0$ allora $(x-a)$ divide sia $f(x)$ che $f'(x)$. Quindi $(x-a)^2|f(x)$, ovvero a non è zero semplice di f.

(3) $\Rightarrow$ (1). Se $f'(x) \neq 0$ allora $\deg(f'(x)) < \deg(f(x))$ e $MCD(f(x), f'(x)) = 1$ essendo $f(x)$ irriducibile su K. Quindi non vi sono zeri comuni per $f(x)$ e $f'(x)$. Quindi $f(x)$ non ha zeri multipli in nessuna estensione. □

DEFINIZIONE 50. $f(x) \in_{irr} K[X]$ *che verifichi una delle tre proprietà della proposizione precedente si dice separabile .*

PROPOSIZIONE 25. *Sia* K *campo e sia* $f(x) \in K[X]$. *Allora:*

(1) *Se* K *ha caratteristica* 0 *allora* $f'(x) = 0$ *se e solo se* $f(x) = c \in K$.
(2) *Se la caratteristica di* K *è un primo* p *allora* $f'(x) = 0$ *se e solo se* $f(x) = g(x^p)$ *per qualche* $g(x) \in K[X]$.

DIMOSTRAZIONE.

(1) Sia $f(x) \in K[X]$. Se il grado di $f(x)$ è maggiore di 0 allora scriviamo $f(x) = a_n x^n + ... + a_1 x + a_0$ con $a_n \neq 0$. Supponiamo che la derivata formale di $f(x)$ sia il polinomio nullo, ovvero
$$na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} ... + 2a_2 x + a_1 = 0$$
Allora $na_n = (n-1)a_{n-1} = ... = 2a_2 = a_1 = 0$. In particolare $na_n = 0$, che implica $n = 0$ oppure $a_n = 0$ in K. Ma a_n si era supposto essere diverso da 0, quindi $n = 0$ in K. D'altra parte n non è 0 in $\mathbb{N}$ perché $f(x)$ ha grado maggiore di 0. Quindi K non può avere caratteristica 0. Di conseguenza se $\chi(K) = 0$ e $f'(x) = 0$ è necessario che $f(x)$ abbia grado 0. Ciò è anche sufficiente perché la derivata formale di un elemento di K (ovvero di un polinomio di grado zero in $K[X]$) è 0.
(2) Sia p la caratteristica del campo K, e supponiamo $f'(x) = 0$. Allora, come sopra, se $f(x) = a_n x^n + ... + a_1 x + a_0$ con $a_n \neq 0$ si ha
$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + 2a_2 x + a_1 = 0$$

Di conseguenza $na_n = (n-1)a_{n-1} = ... = 2a_2 = a_1 = 0$. Ne segue che se per qualche $i \in \{1, ..., n\}$ si ha $a_i \neq 0$ allora $i = 0$ in K, ovvero i, come numero naturale, è un multiplo di p. Siano $i_1, ..., i_r$ gli indici multipli di p, con $i_j = pt_j$ per ogni $j = 1, ..., r$. Allora

$$f(x) = \sum_{j=1}^{r} a_{i_j} x^{pt_j} = g(x^p)$$

dove $g(x) := a_{i_1} x^{t_1} + ... + a_{i_r} x^{t_r}$.

Viceversa se $g(x) \in K[X]$, sempre ricorrendo all'analisi per la derivazione di funzioni composte, la derivata formale di $g(x^p)$ è $px^{p-1}g'(x^p) = 0$ in K.

□

In particolare se K ha caratteristica 0 allora ogni polinomio di $K[X]$ irriducibile è separabile. Se invece K ha come caratteristica il primo p, $f(x) \in K[X]$ irriducibile è separabile se e solo se non è della forma $g(x^p)$ con $g(x) \in K[X]$.

TEOREMA 19. *Sia K campo e sia $f(x) \in_{irr} K[X]$.*

1. *Se K ha caratteristica zero allora $f(x)$ ha zeri tutti semplici in ogni estensione.*
2. *Se la caratteristica di K è il primo p allora $f(x)$ ha zeri multipli se e solo se $f(x) = g(x^p)$ per qualche $g(x) \in K[X]$.*
3. *Se la caratteristica di K è il primo p e p^l è la massima potenza di p tale che $f(x) = h(x^{p^l})$ per qualche $h(x) \in K[X]$, allora $h(x)$ è irriducibile, la sua derivata formale non è il polinomio nullo, e in una opportuna estensione di K si ha*
$$f(x) = a(x - \alpha_1)^{p^l} ... (x - \alpha_t)^{p^l}$$
dove $\alpha_1, ..., \alpha_t$ sono a due a due distinti, e $a \in K$. Quindi tutti gli zeri di f hanno la stessa molteplicità.

DIMOSTRAZIONE. (1) e (2) sono già stati dimostrati. Mostriamo (3). Sia $f(x) = h(x^{p^l})$ dove p^l è la massima potenza di p tale che $f(x)$ si possa esprimere come polinomio in x^{p^l} a coefficienti in K. Se scriviamo $h(x)$ come prodotto di polinomi in $K[X]$, diciamo $h(x) = b(x)c(x)$, allora $f(x) = b(x^{p^l})c(x^{p^l})$ con $b(x), c(x) \in K[X]$. Ma $f(x)$ è irriducibile, quindi uno tra $b(x)$ e $c(x)$ ha grado 0. Quindi $h(x)$ è irriducibile. Inoltre non è della forma $u(x^p)$ per qualche $u(x) \in K[X]$, perché se fosse così allora $f(x) = h(x^{p^l}) = u((x^{p^l})^p) = u(x^{p^{l+1}})$, e questo contraddice la massimalità di p^l. Quindi $h(x)$ è separabile: in un c.r.c. si ha

$$h(x) = a(x - \beta_1)(x - \beta_2)...(x - \beta_t)$$

per qualche $a \in K$, detto t il grado di $h(x)$. I β_i sono a due a due distinti. Di conseguenza

$$f(x) = a(x^{p^l} - \beta_1)...(x^{p^l} - \beta_t).$$

Detto α_i uno zero di $x^{p^l} - \beta_i$ per ogni $i = 1, ..., t$, si ha che $\beta_i = \alpha_i^{p^l}$ e dunque ricordando l'endomorfismo di Frobenius,

$$f(x) = a(x^{p^l} - \alpha_1^{p^l})...(x^{p^l} - \alpha_t^{p^l}) = a(x - \alpha_1)^{p^l} ... (x - \alpha_t)^{p^l}.$$

□

Ne segue che un polinomio irriducibile $f(x) \in K[X]$ è separabile se K ha caratteristica 0, e se K ha come caratteristica un primo p allora $f(x)$ ha zeri tutti multipli con la stessa molteplicità, uguale a qualche potenza di p.

DEFINIZIONE 51. *Sia L/K estensione di campi. $u \in L$ algebrico su K si dice separabile su K se il suo polinomio minimo su K è separabile. L'estensione L/K si dice separabile se ogni $u \in L$ è separabile su K.*

Si osservi che se K ha caratteristica 0 allora ogni estensione algebrica di K è separabile. Se invece la caratteristica di K è il primo p, per ogni $\alpha \in L$ algebrico su K esiste $l \in \mathbb{N}$ tale che α^{p^l} è separabile su K.

7. La pura inseparabilità

DEFINIZIONE 52. *Sia L/K estensione di campi. $\alpha \in L$ si dice puramente inseparabile su K se valgono le seguenti condizioni:*

(1) *Se $\chi(K) = 0$ allora $\alpha \in K$.*
(2) *Se $\chi(K) = p > 0$ allora esiste $l \in \mathbb{N}$ tale che $\alpha^{p^l} \in K$.*

L'estensione L/K si dice puramente inseparabile se ogni $u \in L$ è puramente inseparabile su K.

TEOREMA 20. *Sia L/K estensione di campi e sia $\alpha \in L$ algebrico su K. Le seguenti affermazioni sono equivalenti:*

(1) *α è puramente inseparabile su K.*
(2) *Il polinomio minimo di α su K è una potenza di $x - \alpha$.*

DIMOSTRAZIONE. Se K ha caratteristica 0 l'equivalenza tra le due affermazioni è immediata: se α è puramente inseparabile su K allora $\alpha \in K$ e quindi $x - \alpha$ è il suo polinomio minimo. Viceversa se $(x - \alpha)^m$ è il polinomio minimo di α su K allora $m = 1$ perché ogni polinomio irriducibile è separabile.

Ora la caratteristica di K sia il primo p.

(1) $\Rightarrow$ (2). Sia $l \in \mathbb{N}$ tale che $\alpha^{p^l} \in K$. Allora il polinomio minimo di α su K divide $x^{p^l} - \alpha^{p^l} = (x - \alpha)^{p^l}$, e quindi è una potenza di $x - \alpha$.

(2) $\Rightarrow$ (1). Sia $(x - \alpha)^m$ il polinomio minimo di α su K. Se $m = 1$ allora $\alpha \in K$ quindi α è puramente inseparabile su K. Se $m > 1$ allora α è zero multiplo del polinomio irriducibile $(x - \alpha)^m$, di conseguenza $(x - \alpha)^m = g(x^{p^l})$ per qualche $g(x) \in K[X]$, in modo che $l \in \mathbb{N}$ sia il massimo possibile. Allora $g(x)$ è irriducibile e separabile, e $m = sp^l$ per qualche $s \in \mathbb{N}$. Quindi $(x-\alpha)^m = (x-\alpha)^{sp^l} = (x^{p^l} - \alpha^{p^l})^s$, e $g(x) = (x - \alpha^{p^l})^s$ è separabile. Quindi $s = 1$, e $\alpha^{p^l} \in K$. □

Ne segue immediatamente che se L/K è estensione di campi, $\alpha \in L$ è puramente inseparabile e separabile su K se e solo se $\alpha \in K$.

TEOREMA 21. *Sia K campo di caratteristica $p > 0$, e sia $x^{p^n} - c \in K[X]$ ove $n \geq 1$. Allora $x^{p^n} - c$ è riducibile in $K[X]$ se e solo se $c \in K^p$, ovvero c è potenza p-esima di un elemento di K.*

DIMOSTRAZIONE. La sufficienza è ovvia, basta usare l'endomorfismo di Frobenius. Proviamo la necessità. Se $x^{p^n} - c$ è riducibile allora $x^{p^n} - c = f(x)g(x)$ con $f(x),\ g(x) \in K[X]$ di grado positivo, e possiamo scegliere $f(x)$ irriducibile. Se α è uno zero di $f(x)$ in una opportuna estensione, allora è uno zero di $x^{p^n} - c$, quindi è puramente inseparabile su K e il suo polinomio minimo è $f(x)$. Ne segue che

$f(x) = (x-\alpha)^{p^s}$ con $s < n$. Quindi $f(x) = x^{p^s} - \alpha^{p^s}$. Ciò implica che $\alpha^{p^s} \in K$. Ora $c = \alpha^{p^n} = ((\alpha^{p^s})^{p^{n-s-1}})^p$ quindi c è potenza p-esima di un elemento di K. □

Ne segue che se K è un campo di caratteristica $p > 0$, il polinomio $x^p - c \in K[X]$ è irriducibile in $K[X]$ oppure si fattorizza in fattori lineari in $K[X]$.

Esempio: consideriamo l'estensione L/K dove $K := \mathbb{F}_p(y^p)$ e $L := \mathbb{F}_p(y)$, essendo p un primo ed essendo y trascendente su $\mathbb{F}_p$. Certamente y è puramente inseparabile su K essendo $y^p \in K$. Se fosse anche separabile dovrebbe appartenere a K. Ma in tal caso esisterebbero $f(x),\ g(x) \in \mathbb{F}_p[X]$ tali che $y = \frac{f(y^p)}{g(y^p)}$, ovvero $yg(y^p) = f(y^p)$. Un facile conto mostra che questo è impossibile. Quindi y è puramente inseparabile ma non separabile su K. Di conseguenza il polinomio minimo di y è $(x-y)^p$ dovendo essere del tipo $(x-y)^{p^l}$ con $l \neq 0$, ed essendo $y^p \in K$. In particolare $x^p - y^p$ è irriducibile su $\mathbb{F}_p(y^p)$.

8. Campi perfetti

Definizione 53 (Campi perfetti). *Il campo K si dice perfetto se ogni elemento algebrico su K è separabile su K. Equivalentemente ogni polinomio irriducibile su K è separabile su K. Equivalentemente ogni estensione finita di K è separabile.*

In particolare ogni campo di caratteristica 0 è perfetto.

Proposizione 26. *Sia K un campo di caratteristica $p > 0$. K è perfetto se e solo se $K = K^p := \{a^p \mid a \in K\}$. Equivalentemente l'endomorfismo di Frobenius è suriettivo.*

Dimostrazione. Sia K un campo perfetto, e sia $c \in K$. Se $x^p - c \in K[X]$ è irriducibile, preso α in una opportuna estensione che sia zero di $x^p - c$, si ha $c = \alpha^p$ quindi $x^p - c = (x-\alpha)^p$ e quindi $x^p - c$ non è separabile. Quindi poiché K è perfetto, $x^p - c$ è riducibile, ovvero $c \in K^p$ (teorema 21).

Viceversa valga $K = K^p$, e sia $f(x) \in K[X]$. Supponiamo che $f(x)$ non sia separabile. Allora esiste $h(x) \in K[X]$ tale che $f(x) = h(x^p)$. Se $h(x) = a_k x^k + a_{k-1}x^{k-1} + ... + a_1 x + a_0$ possiamo scegliere $b_i \in K$ per ogni $i = 1, ..., k$ in modo che $b_i^k = a_i$. Quindi

$$f(x) = b_k^p x^{kp} + b_{k-1}^p x^{(k-1)p} + ... + b_1^p x^p + b_0^p = (b_k x^k + b_{k-1}x^{k-1} + ... + b_1 x + b_0)^p$$

Ne segue che $f(x)$ non è irriducibile. □

Abbiamo come conseguenza immediata che ogni campo finito è perfetto: se K è un campo finito la sua caratteristica è un primo p. L'endomorfismo di Frobenius

$$\phi : K \to K$$
$$a \mapsto a^p$$

è iniettivo, quindi è anche suriettivo essendo K finito (principio dei cassetti).

9. Il gruppo di Galois e le corrispondenze

Sia M/K un'estensione di campi.

Definizione 54 (Il gruppo di Galois). *Il gruppo di Galois dell'estensione M/K è per definizione $\mathcal{G}(M/K) := \{\sigma \in \mathrm{Aut}(M) \mid \sigma|_K = id_K\}$, ovvero il gruppo degli automorfismi di M che ristretti a K sono l'identità, ovvero il gruppo dei K-automorfismi di M, dove l'operazione è la composizione.*

Detto G il gruppo di Galois dell'estensione M/K, indicheremo con $[M/K]$ il reticolo degli intercampi di M/K (ovvero l'insieme parzialmente ordinato dei campi L tali che $K \leq L \leq M$, che è un reticolo), e indicheremo con $\mathcal{L}(G)$ il reticolo dei sottogruppi di G (ovvero l'insieme parzialmente ordinato dei sottogruppi di G, che è un reticolo).

DEFINIZIONE 55 (Le corrispondenze). *Consideriamo le seguenti applicazioni (dette corrispondenze di Galois):*

$$i : [M/K] \to \mathcal{L}(G),\ L \mapsto L'$$

$$j : \mathcal{L}(G) \to [M/K],\ H \mapsto H'$$

dove se $L \in [M/K]$ *definiamo* $i(L) = L' := \{m \in M \mid \sigma(m) = m\ \forall \sigma \in G\}$*, e se* $H \in \mathcal{L}(G)$ *definiamo* $j(H) = H' := \{\sigma \in G \mid \sigma(h) = h\ \forall h \in H\}$*. Queste sono tutte buone definizioni. Dati* $L \in [M/K]$*,* $H \in \mathcal{L}(G)$*,* $j(i(L))$ *e* $i(j(H))$ *si dicono le chiusure rispettivamente di* L *e di* H*. Se* L *e* H *coincidono con le proprie chiusure si dicono chiusi.*

Osserviamo alcune cose di facile verifica:

- Le corrispondenze di Galois invertono le inclusioni: se $L_1 \leq L_2$ allora $i(L_1) \geq i(L_2)$; se $H_1 \leq H_2$ allora $j(H_1) \geq j(H_2)$.
- Per ogni $L \in [M/K],\ L'' \geq L$. Per ogni $H \in \mathcal{L}(G),\ H'' \geq H$.
- $K' = G$.
- M è chiuso.
- $L \in [M/K]$ è chiuso se e solo se esiste $H \in \mathcal{L}(G)$ tale che $L = H'$. $H \in \mathcal{L}(G)$ è chiuso se e solo se esiste $L \in [M/K]$ tale che $H = L'$.
- $i \circ j$ ristretta all'insieme dei sottogruppi chiusi di G è l'identità; $j \circ i$ ristretta all'insieme degli intercampi chiusi di M/K è l'identità. Di conseguenza $i \circ j$ e $j \circ i$ inducono biiezioni, una l'inversa dell'altra, tra l'insieme dei sottogruppi chiusi e l'insieme degli intercampi chiusi.

10. Relazioni tra gradi e indici

TEOREMA 22. *Sia* M/K *estensione di campi. Siano* $L_1,\ L_2 \in [M/K]$ *con* $L_1 \leq L_2$ *e* $[L_2 : L_1] = n < \infty$*. Allora* $[L_1' : L_2'] \leq n$*.*

DIMOSTRAZIONE. Procediamo per induzione su n. Se $n = 1$ allora $L_1 = L_2$, quindi $L_1' = L_2'$, quindi $[L_2' : L_1'] = 1 \leq 1$.

Sia ora $n \geq 2$. Ci sono due casi possibili:

(1) Esiste $L_0 \in [M : K]$ tale che $L_1 < L_0 < L_2$. In tal caso siano $[L_0 : L_1] = n_1 < n$, $[L_2 : L_0] = n_2 < n$. Per la formula dei gradi $n = n_1 n_2$. Per ipotesi induttiva $[L_1' : L_0'] \leq n_1$, $[L_0' : L_2'] \leq n_2$. Per la formula degli indici (proposizione 2) si ha $[L_1' : L_2'] = [L_1' : L_0'][L_0' : L_2'] \leq n_1 n_2 = n$.

(2) Non esistono intercampi propri tra L_1 e L_2. In tal caso preso $u \in L_2 - L_1$ si ha $L_2 = L_1(u)$, quindi u è algebrico su L_1 perché L_2/L_1 è estensione finita (ha grado n). Il polinomio minimo di u su L_1, $f(x)$, ha grado n. Si ha, detto G il gruppo di Galois dell'estensione L_2/L_1,

$$L_2' = L_1(u)' = \{\sigma \in G \mid \sigma(u) = u,\ \sigma(l) = l\ \forall l \in L_1\}$$

Sia $r := [L_1' : L_2']$. Se $\sigma,\ \tau \in L_1'$ sono tali che $\sigma(u) = \tau(u)$ allora $u = \sigma^{-1}(\tau(u))$ quindi $\sigma^{-1}\tau \in L_2'$, ovvero σ e τ sono congrui modulo L_2': $\sigma L_2' = \tau L_2'$. Ne segue che se σ e τ sono incongrui modulo L_2' allora $\sigma(u) \neq \tau(u)$.

Quindi esistono r immagini distinte di u tramite elementi di L_1', siano essi $\tau_1(u),\ ...,\ \tau_r(u)$, coi $\tau_i \in L_1'$ a due a due incongrui modulo L_2'. Ma i τ_i sono l'identità su L_1, quindi $f(\tau_i(u)) = \tau_i(f(u)) = \tau_i(0) = 0$ per ogni $i = 1, ..., r$ (vedi dimostrazione del teorema 17). Abbiamo trovato r zeri distinti di $f(x)$, quindi $r \leq n$.

□

LEMMA 24. *Siano $K \leq H \leq G$ gruppi, e sia $\{\tau_1, ..., \tau_n\}$ un trasversale sinistro di K in H. Per ogni $\sigma \in H$, $\{\sigma\tau_1, ..., \sigma\tau_n\}$ è anch'esso un trasversale di K in H.*

DIMOSTRAZIONE. Dato $g \in H$ si ha $\sigma^{-1}g \in H$, quindi $\sigma^{-1}g = \tau_i h$ per qualche $i \in \{1, ..., n\}$ e per qualche $h \in H$. Quindi $g = \sigma\tau_i h$. Ora supponiamo che $\sigma\tau_i K = \sigma\tau_j K$. Allora $(\sigma\tau_i)^{-1}\sigma\tau_j \in K$, quindi $\tau_i^{-1}\sigma^{-1}\sigma\tau_j = \tau_i^{-1}\tau_j \in K$. Quindi $\tau_i = \tau_j$ perché $\{\tau_1, ..., \tau_n\}$ è trasversale di K in H. □

TEOREMA 23. *Sia M/K un'estensione di campi, con gruppo di Galois G, e siano $H_1,\ H_2 \in \mathcal{L}(G)$ con $H_1 \leq H_2$. Detto $n := [H_2 : H_1] < \infty$ si ha $[H_1' : H_2'] \leq n$.*

DIMOSTRAZIONE. Sia $\{\tau_1, ..., \tau_n\}$ trasversale sinistro di H_1 in H_2. Se $\sigma \in H_2$ allora per il lemma 24 $\{\sigma\tau_1, ..., \sigma\tau_n\}$ è un trasversale sinistro di H_1 in H_2. Evidentemente gli elementi di una stessa classe laterale sinistra di H_1 operano allo stesso modo sugli elementi di H_1'. Quindi se $\sigma \in H_2$ e $i \in \{1, ..., n\}$ esiste $j \in \{1, ..., n\}$ tale che $\tau_i(u) = \sigma(\tau_j(u))$ per ogni $u \in H_1'$.

Per assurdo, valga $[H_1' : H_2'] > n$. Siano $u_i \in H_1'$ per $i = 1, ..., n+1$, linearmente indipendenti su H_2'. Consideriamo il sistema

$$\begin{cases} \sum_{i=1}^{n+1} \tau_1(u_i)x_i = 0 \\ ... \\ \sum_{i=1}^{n+1} \tau_n(u_i)x_i = 0 \end{cases}$$

Si tratta di un sistema di n equazioni lineari e $n+1$ incognite, quindi ammette almeno una soluzione non nulla in M. Sia $(a_1, ..., a_r, 0, ..., 0)$ una soluzione non nulla (ottenuta a meno di riordinamento) col numero massimo possibile di zeri, e con $a_i \neq 0$ per ogni $i = 1, ..., r$. A meno di moltiplicare tale soluzione per a_1^{-1} (ottenendo ancora una soluzione) possiamo supporre $a_1 = 1$. La nostra soluzione diviene $(1, a_2, ..., a_r, 0, ..., 0)$. Esiste un unico $i \in \{1, ..., n\}$ tale che $\tau_i \in H_1$. Senza perdita in generalità possiamo supporre $i = 1$. Allora per ogni $i = 1, ..., n+1$ si ha $\tau_1(u_i) = u_i$. Esiste almeno un $j \in \{2, ..., r\}$ tale che $a_j \notin H_2'$, perché se $a_2, ..., a_r \in H_2'$ allora dalla prima equazione $u_1 + a_2u_2 + ... + a_ru_r = 0$, contro l'indipendenza lineare degli u_i su H_2'. Senza perdita in generalità sia $j = 2$. Sia dunque $\sigma \in H_2$ tale che $\sigma(a_2) \neq a_2$. Applicando σ al sistema otteniamo

$$\begin{cases} \sum_{i=1}^{n+1} (\sigma\tau_1)(u_i)\sigma(a_i) = 0 \\ ... \\ \sum_{i=1}^{n+1} (\sigma\tau_n)(u_i)\sigma(a_i) = 0 \end{cases}$$

Ma per quanto detto all'inizio della dimostrazione, i τ_i agiscono esattamente come i $\sigma\tau_i$ sugli u_i, cambia solo l'ordine. Di conseguenza

$$(\sigma(1), \sigma(a_2), ..., \sigma(a_r), \sigma(0), ..., \sigma(0)) = (1, \sigma(a_2), ..., \sigma(a_r), 0, ..., 0)$$

è un'altra soluzione del sistema di partenza. Effettuando la differenza con la soluzione $(1, a_2, ..., a_r, 0, ..., 0)$ otteniamo una terza soluzione. Essa è

$$(0, \sigma(a_2) - a_2, ..., \sigma(a_r) - a_r, 0, ..., 0)$$

Questa soluzione non è nulla perché $\sigma(a_2) - a_2 \neq 0$, e ha uno zero in più della soluzione $(1, a_2, ..., a_r, 0, ..., 0)$. Questo contraddice l'ipotesi che il numero di zeri in quest'ultima soluzione fosse massimo. □

Ne segue che se M/K è un'estensione di campi con gruppo di Galois G, e $L_1, L_2 \in [M/K]$, $H_1, H_2 \in \mathcal{L}(G)$, allora:

(1) Se $L_1 \leq L_2$, $[L_2 : L_1] = n \in \mathbb{N}$ e L_1 è chiuso, allora L_2 è chiuso e $[L_1' : L_2'] = n$.
Infatti $n = [L_2 : L_1] \geq [L_1' : L_2'] \geq [L_2'' : L_1''] = [L_2'' : L_1] = [L_2'' : L_2][L_2 : L_1] = [L_2'' : L_2]n$ da cui $[L_2'' : L_2] \leq 1$ da cui $[L_2'' : L_2] = 1$ ovvero $L_2'' = L_2$. Quindi le precedenti sono tutte uguaglianze e $n = [L_1' : L_2']$.

(2) Se $H_1 \leq H_2$, $[H_2 : H_1] = n \in \mathbb{N}$ e H_1 è chiuso, allora H_2 è chiuso e $[H_1' : H_2'] = n$.
Infatti $n = [H_2 : H_1] \geq [H_1' : H_2'] \geq [H_2'' : H_1''] = [H_2'' : H_1] = [H_2'' : H_2][H_2 : H_1] = [H_2'' : H_2]n$ da cui, come sopra $H_2'' = H_2$ e $[H_1' : H_2'] = n$.
In particolare ogni sottogruppo di G il cui indice su $\{1_G\}$ è finito, ovvero il cui ordine è finito, è chiuso.

11. Estensioni di Galois

Definizione 56 (Estensioni di Galois). *Sia M/K un'estensione di campi con gruppo di Galois G. M/K si dice estensione di Galois se una delle seguenti condizioni equivalenti è soddisfatta:*

- *K è chiuso, ovvero $G' = K$.*
- *Ogni $u \in M - K$ viene mosso da qualche $\sigma \in G$.*

In particolare se M/K è di Galois ogni intercampo L di M/K il cui grado su K è finito è chiuso, ovvero M/L è di Galois.
Un'estensione finita M/K è di Galois se e solo se $[M : K] = |\mathcal{G}(M/K)|$.

Osservazione 2. *Se M/K è estensione di Galois finita, gli intercampi e i sottogruppi sono chiusi.*

Dimostrazione. Sia $L \in [M/K]$. Allora $[L : K] \leq [M : K]$ è finito, quindi L è chiuso essendo K chiuso. Sia $H \in \mathcal{L}(G)$. Allora $\{1_G\} \leq H$ e $\{1_G\}$ è chiuso, quindi H è chiuso essendo $[H : \{1_G\}] \leq [M : H'] < \infty$. □

Osservazione 3. *Se M/K è estensione di Galois finita e $L \in [M/K]$ allora M/L è di Galois.*

Dimostrazione. Sappiamo che L è chiuso, ovvero che l'insieme degli elementi di M fissati da L' è L. Inoltre il gruppo di Galois di M/L è L'. Di conseguenza L è chiuso anche in M/L, e M/L è di Galois. □

Ne segue il nostro teorema fondamentale:

Teorema 24 (Teorema fondamentale della teoria di Galois). *Sia M/K estensione di Galois finita con gruppo di Galois G. Allora tutti gli intercampi sono chiusi e tutti i sottogruppi sono chiusi. Di conseguenza le corrispondenze di Galois inducono una corrispondenza biunivoca tra gli intercampi di M/K e i sottogruppi di G che inverte le inclusioni. L'indice relativo a due sottogruppi eguaglia il grado relativo ai corrispondenti intercampi. In particolare $|G| = [M : K]$.*

12. Normalità e stabilità

Ora osserviamo alcune cose interessanti. Sia M/K estensione di campi con gruppo di Galois G.

DEFINIZIONE 57. *$L \in [M/K]$ si dice stabile se per ogni $\sigma \in G$, $u \in L$ si ha $\sigma(u) \in L$.*

Si vede facilmente che L è stabile se e solo se $\sigma(L) = L$ per ogni $\sigma \in G$.

- Sia $L \in [M/K]$ intercampo stabile. Allora per ogni $\sigma \in G$, $\gamma \in L'$, $u \in L$ si ha $\sigma^{-1}(\gamma(\sigma(u))) = \sigma^{-1}(\sigma(u)) = u$ perché $\sigma(u) \in L$ essendo L stabile ed essendo $\gamma \in L'$. Quindi $\sigma^{-1} \circ \gamma \circ \sigma \in L'$. Questo prova che $L' \trianglelefteq G$.
- Sia $H \trianglelefteq G$. Allora per ogni $\gamma \in H$, $\sigma \in G$ e per ogni $u \in H'$ si ha $\sigma^{-1}(\gamma(\sigma(u))) = u$, ovvero $\gamma(\sigma(u)) = \sigma(u)$. Poiché questo vale per ogni $\gamma \in H$, si ha $\sigma(u) \in H'$, e questo vale per ogni $\sigma \in G$. Di conseguenza H' è stabile.

Ne segue che se M/K è un'estensione di campi con gruppo di Galois G, le corrispondenze inducono una biiezione tra l'insieme degli intercampi chiusi stabili di M/K e l'insieme dei sottogruppi chiusi normali di G. Inoltre se $H \trianglelefteq G$ allora $H'' \trianglelefteq G$, e se $L \in [M/K]$ è stabile allora L'' è stabile.

OSSERVAZIONE 4. *Sia M/K estensione di Galois. Se $L \in [M/K]$ è stabile allora L/K è di Galois.*

DIMOSTRAZIONE. Dato $u \in L - K$ basta mostrare l'esistenza di un $\gamma \in \mathcal{G}(L/K)$ tale che $\gamma(u) \neq u$. Poiché M/K è di Galois, esiste $\sigma \in \mathcal{G}(M/K)$ tale che $\sigma(u) \neq u$. Inoltre $\sigma(u) \in L$ essendo L stabile. In realtà la restrizione di σ a L è un automorfismo di L. Basta quindi prendere $\gamma := \sigma|_L$. □

TEOREMA 25. *Sia M/K estensione di Galois con gruppo di Galois G. Se $f(x) \in_{irr} K[X]$ ha uno zero in M allora $f(x)$ è separabile e si decompone in fattori lineari in $M[X]$. In particolare ogni $u \in M$ algebrico su K è separabile.*

DIMOSTRAZIONE. Supponiamo senza perdita in generalità che $f(x)$ sia monico. Siano $u_1, ..., u_r$ gli zeri distinti di $f(x)$ in M. Allora detto n il grado di $f(x)$ si ha $r \leq n$. Sia $g(x) := (x - u_1)...(x - u_r)$. Dato $\sigma \in G$, se u è zero di $f(x)$ in M anche $\sigma(u)$ è zero di $f(x)$. Di conseguenza

$$\{u_1, ..., u_r\} = \{\sigma(u_1), ..., \sigma(u_r)\}$$

Ovvero σ permuta gli zeri di $f(x)$ in M. In particolare detto $\overline{\sigma}$ l'unico automorfismo di $M[X]$ che estende σ e manda x in x, abbiamo che $\overline{\sigma}(g(x)) = g(x)$. I coefficienti di $g(x)$ sono quindi fissati da ogni $\sigma \in G$, quindi $g(x) \in K[X]$ perché K è chiuso. Inoltre $g(x)$ divide $f(x)$ avendo zeri in comune con $f(x)$, tutti di molteplicità 1. Poiché $f(x)$ è irriducibile in $K[X]$ questo implica che $g(x) = f(x)$. Quindi $f(x)$ è separabile e si decompone in fattori lineari in $M[X]$. □

Sappiamo che se M/K è di Galois e $L \in [M/K]$ è stabile, L/K è di Galois. Ci chiediamo quando vale il viceversa.

TEOREMA 26. *Siano $K \leq L \leq M$ campi. Se l'estensione L/K è algebrica e di Galois, L è stabile in M/K.*

DIMOSTRAZIONE. Supponiamo quindi che L/K sia un'estensione di Galois algebrica. Sia $\sigma \in \mathcal{G}(M/K)$ e sia $u \in L$. Dobbiamo mostrare che $\sigma(u) \in L$. Poiché L/K è algebrica, u è algebrico su K. Consideriamo $f(x) \in K[X]$, il polinomio minimo di u su K. Allora per il teorema precedente $f(x)$ si decompone in fattori lineari in $L[X]$. Sappiamo che anche $\sigma(u)$ è zero di $f(x)$ in $M \geq L$. Quindi $\sigma(u) \in L$. □

Ne segue che se M/K è estensione di Galois algebrica, $L \in [M/K]$ è stabile se e solo se L/K è di Galois.

Scopriamo ora la relazione che c'è tra $\mathcal{G}(L/K)$ e $\mathcal{G}(M/K)$ se L è stabile.

TEOREMA 27. *Sia M/K estensione di campi con gruppo di Galois G, e sia $L \in [M/K]$ stabile. Allora $L' \trianglelefteq G$ e G/L' è isomorfo al gruppo dei K-automorfismi di L che si estendono a M. Ogni K-automorfismo di L si estende a M se e solo se*

$$G/L' \cong \mathcal{G}(L/K)$$

canonicamente.

DIMOSTRAZIONE. Consideriamo $\alpha : G \to \mathcal{G}(L/K)$ definito da $\alpha(\sigma) := \sigma|_L$. Ovviamente $\alpha(G)$ è il gruppo dei K-automorfismi di L che si estendono a M. Il nucleo di α consiste dei K-automorfismi di M che sono l'identità su L, ovvero $ker(\alpha) = L'$. L'asserto segue dal primo teorema di isomorfismo per i gruppi. □

Ora se M/K è estensione di Galois finita con gruppo di Galois G, essa è algebrica e se $L \in [M/K]$ è stabile allora ogni K-automorfismo di L si estende a M. Infatti L/K è di Galois quindi $|\mathcal{G}(L/K)| = [L : K] = [K' : L'] = [G : L'] = |G/L'|$. Quindi l'omomorfismo iniettivo $G/L' \to \mathcal{G}(L/K)$ indotto dalla restrizione a L è un isomorfismo.

TEOREMA 28 (Supplemento al teorema fondamentale). *Sia M/K estensione di Galois finita. Allora esiste una biiezione tra intercampi e sottogruppi, e $L \in [M/K]$ è stabile se e solo se L' è normale in G, se e solo se L/K è di Galois. Se L è stabile allora $\mathcal{G}(L/K) \cong G/L'$.*

13. Caratterizzazione delle estensioni di Galois finite. Esempi.

Attenzione al prossimo importante risultato:

TEOREMA 29. *Sia M/K estensione di campi. Le seguenti affermazioni sono equivalenti:*

1. *M/K è di Galois finita.*
2. *M/K è separabile e M è c.r.c. su K.*
3. *M è c.r.c. su K per un polinomio di $K[X]$ a fattori irriducibili separabili.*

DIMOSTRAZIONE. (1) $\Rightarrow$ (2). Se M/K è di Galois finita allora è algebrica, quindi ogni $u \in M$ è separabile su K (teorema 25). Quindi M è c.r.c. su K per il teorema 18.

(2) $\Rightarrow$ (3). Se vale (2) allora M è c.r.c. su K per un polinomio i cui fattori irriducibili sono separabili essendo M/K separabile.

(3) $\Rightarrow$ (1). Se vale (3) allora M/K è finita perché ottenuta per aggiunzione di elementi algebrici su K, e dal teorema 17 si ha $[M : K] = |\mathcal{G}(M/K)|$, quindi M/K è di Galois. □

Facciamo alcuni esempi.

- $\mathbb{R}$ ha caratteristica 0 quindi è perfetto. L'estensione $\mathbb{C}/\mathbb{R}$ è di Galois perché $\mathbb{C} = \mathbb{R}(i)$ è c.r.c. su $\mathbb{R}$ per il polinomio irriducibile (quindi separabile) $x^2 + 1$. Ne segue che il gruppo di Galois, chiamiamolo G, ha ordine 2 quindi è ciclico. Se $\sigma \in G$ si ha $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, quindi $\sigma(i) = i$ oppure $\sigma(i) = -i$. Se $\sigma(i) = i$ allora σ è l'identità. Se $\sigma(i) = -i$ allora σ è il coniugio, perché manda $a + ib$ in $a - ib$. Ne segue che i due elementi di G sono identità e coniugio.
- $K := \mathbb{Q}$ ha caratteristica 0, quindi è perfetto. Sia $L := \mathbb{Q}(\sqrt[3]{2})$. L'estensione L/K non è di Galois. Infatti il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$ è $x^3 - 2$ (dal criterio di Eisenstein). Se L/K fosse di Galois tale polinomio dovrebbe fattorizzarsi completamente in $L[X]$, ma una facile verifica mostra che i suoi zeri sono, detto $\alpha = \sqrt[3]{2}$ e detta ε una radice primitiva terza dell'unità, α, $\varepsilon\alpha$, $\varepsilon^2\alpha$. Ne segue che detto $M := K(\alpha, \varepsilon)$, M/K è di Galois, essendo M c.r.c. per $x^3 - 2$ su K, irriducibile quindi separabile. Esplicitamente, $M = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. Quindi $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}$ è di Galois.

ESERCIZIO 84. *Sia $f(x) := x^4 + 4 \in \mathbb{Q}[X]$. Si decomponga $f(x)$ in fattori irriducibili in $\mathbb{Q}[X]$. Si studi il campo di riducibilità completa M per $f(x)$ su $\mathbb{Q}$ e si descriva il gruppo $\mathcal{G}(M/\mathbb{Q})$. Sia K un campo di caratteristica 5. Si risponda alle stesse domande dopo aver sostituito dovunque $\mathbb{Q}$ con K.*

ESERCIZIO 85. *Sia n un intero positivo, e sia K un campo che contiene tutte le radici n-esime di 1. Siano a un elemento di K ed M un campo di riducibilità completa su K per il polinomio $x^n - a$. Si provi che $\mathcal{G}(M/K)$ è ciclico.*

ESERCIZIO 86. *Sia F/K una estensione algebrica. Si provi che se ogni elemento di F appartiene ad un intercampo che è estensione di Galois di K, allora F/K è di Galois.*

ESERCIZIO 87. *Sia M un campo di riducibilità completa per il polinomio $(x^2 - 5)(x^3 - 5)$ su $\mathbb{Q}$. Si provi che $M/\mathbb{Q}$ contiene intercampi stabili L e N tali che $[L : \mathbb{Q}] > 1$, $[N : \mathbb{Q}] > 1$, $L \cap N = \mathbb{Q}$ e $(L \cup N) = M$. Si determini $\mathcal{G}(M/\mathbb{Q})$. Quante sono le possibili scelte per L e N?*

ESERCIZIO 88. *Si provi che $L := \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ e che $\mathcal{G}(L/\mathbb{Q}) \cong C_2 \times C_2$.*

ESERCIZIO 89. *Sia M/K un'estensione di campi, e sia $G := \mathcal{G}(M/K)$. Denotiamo come è solito con $[M/K]$ il reticolo degli intercampi di M/K. Si mostri che:*

1. *Se $L, S \in [M/K]$ allora $(L \cup S)' = L' \cap S'$, e se $H, J \leq G$ allora $\langle H, J\rangle' = H' \cap J'$.*
2. *Se $L, S \in [M/K]$ sono chiusi allora $L \cap S$ è chiuso, e se $H, J \leq G$ sono chiusi allora $H \cap J$ è chiuso.*
3. *Se $L \in [M/K]$, E/L e L/K sono di Galois e ogni K-automorfismo di L si estende a E allora E/K è di Galois.*

14. Applicazione: le funzioni simmetriche elementari

Sia R anello commutativo unitario, e siano $x_1, ..., x_n$ indeterminate distinte su R. È facile vedere che se S è un anello e $u_1, ..., u_n \in S$ allora esiste un unico omomorfismo $\eta_{u_1,...,u_n} : R[x_1, ..., x_n] \to S$ che manda x_i in u_i per ogni $i = 1, ..., n$.

Per la stessa ragione dato $\sigma \in S_n$ esiste un unico omomorfismo $\sigma^* : R[x_1, ..., x_n] \to R[x_1, ..., x_n]$ che manda x_i in $x_{\sigma(i)}$. Dati $\sigma_1, \sigma_2 \in S_n$ è facile vedere che $(\sigma_1 \circ \sigma_2)^* = {\sigma_1}^* \circ {\sigma_2}^*$ e $1^* = 1$, quindi la mappa

$$S_n \to \mathrm{End}(R[x_1, ..., x_n]), \qquad \sigma \mapsto \sigma^*$$

è un omomorfismo di gruppi. In particolare ogni σ^* è invertibile con inverso $(\sigma^{-1})^*$, quindi ogni σ^* è un automorfismo di $R[x_1, ..., x_n]$.

Se R è un dominio di integrità possiamo considerare $R(x_1, ..., x_n)$, il campo delle frazioni del dominio $R[x_1, ..., x_n]$. In particolare ciò è vero se $R = K$ è un campo, e in tal caso detto $E := K(x_1, ..., x_n)$ ogni σ^* si estende in modo unico ad un automorfismo $\overline{\sigma}$ di E, e si ha $\overline{\sigma_1 \circ \sigma_2} = \overline{\sigma_1} \circ \overline{\sigma_2}$. Segue che l'insieme degli automorfismi di E del tipo $\overline{\sigma}$ è un sottogruppo di $\mathcal{G}(E/K)$ isomorfo a S_n: chiamiamo tale gruppo G. Sia $S := G'$, la chiusura di G nell'estensione E/K. S si dice **campo delle funzioni razionali simmetriche** in $x_1, ..., x_n$. G è un gruppo finito (ha ordine $n!$) quindi è chiuso in E/K, i.e. $S' = G$, quindi S è chiuso e E/S è un'estensione di Galois con gruppo di Galois G. Se $H \leq G$ allora H è finito quindi chiuso, e E/H' è estensione di Galois. In particolare per il teorema di Cayley abbiamo ottenuto il seguente risultato:

PROPOSIZIONE 27. *Ogni gruppo finito è gruppo di Galois di una qualche estensione di Galois.*

Per $m = 1, ..., n$ definiamo

$$s_m := \sum_{1 \leq i_1 < ... < i_m \leq n} x_{i_1} ... x_{i_m}.$$

I s_m si dicono **funzioni simmetriche elementari**, ed appartengono a S. Per esempio si ha:

- $s_1 = x_1 + ... + x_n$.
- $s_2 = x_1x_2 + x_1x_3 + ... + x_1x_n + x_2x_3 + ... + x_2x_n + ... + x_{n-1}x_n$.

Abbiamo la seguente relazione

$$\begin{aligned} g(y) &:= (y - x_1)(y - x_2)...(y - x_n) = \\ &= y^n - s_1y^{n-1} + s_2y^{n-2} - ... + (-1)^{n-1}s_{n-1}y + (-1)^n s_n. \end{aligned}$$

In particolare $g(y)$ ha coefficienti in $K(s_1, ..., s_n)$, quindi $E = K(x_1, ..., x_n)$ è c.r.c. su $K(s_1, ..., s_n)$ di $g(y)$, che ha grado n, quindi $[K(x_1, ..., x_n) : K(s_1, ..., s_n)] \leq n!$ (teorema 15). Ma poiché $[E : S] = n!$, da

$$[E : K(s_1, ..., s_n)] = [E : S][S : K(s_1, ..., s_n)] \leq n!$$

discende che $S = K(s_1, ..., s_n)$.

In sintesi:

TEOREMA 30. *Sia K un campo. Ogni funzione razionale simmetrica di $K[x_1, ..., x_n]$ è funzione razionale delle funzioni simmetriche elementari $s_1, ..., s_n$, e l'estensione $K(x_1, ..., x_n)/K(s_1, ..., s_n)$ è di Galois con gruppo di Galois S_n.*

15. Sui campi finiti

TEOREMA 31. *Sia L campo finito.*

(1) *Esiste un primo p tale che $|L| = p^n$ per qualche $n \in \mathbb{N}$. L è c.r.c. su $\mathbb{F}_p$ di $x^{p^n} - x$.*

(2) *Per ogni primo p e per ogni $0 \neq n \in \mathbb{N}$ esiste un campo con p^n elementi. Due tali campi sono isomorfi.*
(3) *Se $K \leq L$, L/K è estensione di Galois con gruppo di Galois ciclico, ed esiste $m|n$ tale che $|K| = p^m$.*

DIMOSTRAZIONE.

(1) Sappiamo che se L ha caratteristica 0 allora esiste una funzione iniettiva $\mathbb{Q} \to L$, quindi L è infinito. Di conseguenza se L è finito la sua caratteristica è un numero primo. Chiamiamolo p. Ne segue che il suo campo primo è $\mathbb{F}_p$, e L è spazio vettoriale su $\mathbb{F}_p$ di dimensione finita. Chiamiamola n. Allora possiamo rappresentare gli elementi di L come vettori n-dimensionali ad entrate in $\mathbb{F}_p$, e di conseguenza $|L| = p^n$. Ora $L^* := L - \{0\}$ ha ordine $p^n - 1$ ed è un gruppo moltiplicativo. Quindi per ogni $a \in L$ si ha $a^{p^n-1} = 1$, quindi $a^{p^n} = a$, quindi ogni elemento di L è uno zero di $x^{p^n} - x$. D'altra parte L ha p^n elementi, quindi è c.r.c. su $\mathbb{F}_p$ di $x^{p^n} - x$.
(2) Sia L un c.r.c. di $x^{p^n} - x$ su $\mathbb{F}_p$. Sia $S := \{a \in L \mid a^{p^n} - a = 0\}$. Usando il fatto che l'applicazione $L \to L$, $l \mapsto l^{p^n}$ è endomorfismo di L si vede subito che S è un campo. Per minimalità di L rispetto a contenere gli zeri di $x^{p^n} - x$ si ha $L = S$. Ora la derivata formale di $x^{p^n} - x$ è -1, che non ammette zeri comuni con $x^{p^n} - x$. Per la proposizione 23 quindi $x^{p^n} - x$ non ha zeri multipli. Quindi $|L| = \deg(x^{p^n} - x) = p^n$.

    Se L_0 è un altro campo con p^n elementi abbiamo visto dal punto 1 che è un c.r.c. su $\mathbb{F}_p$ di $x^{p^n} - x$, di conseguenza è isomorfo ad ogni altro c.r.c., in particolare a L.
(3) Dal teorema 29, L/K è di Galois perché L è c.r.c. su K per $x^{p^n} - x$ che ha zeri tutti semplici (di conseguenza ogni fattore irriducibile è separabile). Sappiamo che l'ordine di K è una potenza di p, diciamo $|K| = p^m$. Allora $n = [L : \mathbb{F}_p] = [L : K][K : \mathbb{F}_p] = [L : K]m$, di conseguenza $m|n$.

    Ci rimane da mostrare che $\mathcal{G}(L/K)$ è ciclico. Per fare questo basta (e bisogna) mostrare che $G := \mathcal{G}(L/\mathbb{F}_p)$ è ciclico. Abbiamo che $L/\mathbb{F}_p$ è di Galois, di conseguenza $|G| = |\operatorname{Aut}(L)| = n$. Ricordiamo infatti che ogni automorfismo di L ristretto a $\mathbb{F}_p$ è l'identità (lemma 23). Sia $\phi : L \to L$ l'endomorfismo di Frobenius, che sappiamo essere un automorfismo perché L è finito. Abbiamo che $\phi^n(l) = l^{p^n} = l$ per ogni $l \in L$, quindi $\phi^n = id_L$. Per concludere basta mostrare che ϕ^r non è l'identità per ogni $r < n$. Se non fosse così detto $r < n$ tale che $\phi^r = id_L$, ogni $l \in L$ soddisferebbe $l^{p^r} = l$, quindi gli elementi di L sarebbero al più p^r. Questo è assurdo perché $p^r < p^n$ e L ha ordine p^n. Quindi $\operatorname{Aut}(L)$ è ciclico generato da ϕ.

    Ora $|\mathcal{G}(L/K)| = [L : K] = [L : \mathbb{F}_p]/[K : \mathbb{F}_p] = n/m$, quindi $\mathcal{G}(L/K)$ è ciclico generato da ϕ^m.

□

Mostriamo ora che ogni sottogruppo finito del gruppo moltiplicativo di un campo è ciclico. In particolare il gruppo moltiplicativo di un campo finito è ciclico. Per questo basta mostrare il seguente lemma.

LEMMA 25. *Sia G un gruppo finito di ordine n tale che per ogni divisore d di n si abbia*

$$|\{x \in G \mid x^d = 1\}| \leq d.$$

Allora G è ciclico.

Infatti in un campo l'equazione $x^d - 1 = 0$ ammette al più d soluzioni.

DIMOSTRAZIONE. Per ogni divisore d di n sia d^* il numero di elementi di G di ordine d, e sia d^{**} il numero degli elementi di C_n di ordine d. Sia $d|n$. Se esiste $g \in G$ di ordine d, siccome ogni elemento x di $\langle g\rangle$ verifica $x^d = 1$, dall'ipotesi segue che $\langle g\rangle = \{x \in G \mid x^d = 1\}$ e $d^* = d^{**}$. Se G non ha elementi di ordine d allora $d^* = 0$, quindi in particolare deduciamo che $d^* \leq d^{**}$ per ogni divisore d di n. Ma allora

$$n = \sum_{d|n} d^* \leq \sum_{d|n} d^{**} = n,$$

e questo implica $\sum_{d|n}(d^* - d^{**}) = 0$. Siccome gli addendi di questa somma sono tutti non negativi si deve avere $d^* = d^{**}$ per ogni $d|n$, in particolare $n^* = n^{**} \geq 1$. □

In particolare data l'estensione $L/\mathbb{F}_p$ con L campo finito, e detto a un generatore del gruppo moltiplicativo ciclico $L - \{0\}$, si ha $L = \mathbb{F}_p(a)$, quindi ogni campo finito di caratteristica p è un'estensione semplice di $\mathbb{F}_p$.

OSSERVAZIONE 5. *Sia L campo finito di ordine p^n con p primo. Dato $m|n$ esiste un unico sottocampo di L di ordine p^m.*

DIMOSTRAZIONE. Sia $\phi : L \to L$ l'endomorfismo di Frobenius. Sappiamo che $\mathcal{G}(L/\mathbb{F}_p) = \langle\phi\rangle$. Sia $K := \langle\phi^m\rangle'$. Allora $[K : \mathbb{F}_p] = [\langle\phi\rangle : \langle\phi^m\rangle] = n/(n/m) = m$. Quindi $|K| = p^m$. D'altra parte se $K \leq L$ ha ordine p^m allora $m = [K : \mathbb{F}_p] = [\langle\phi\rangle : K']$ dunque K' ha indice m, quindi ha ordine n/m. L'unico sottogruppo di $\langle\phi\rangle$ di ordine n/m è $\langle\phi^m\rangle$, dunque $K' = \langle\phi^m\rangle$. □

OSSERVAZIONE 6. *Sia p un primo. Il polinomio $x^{p^n} - x$ si fattorizza in $\mathbb{F}_p[X]$ nel prodotto di tutti e soli i polinomi monici irriducibili di $\mathbb{F}_p[X]$ di grado un divisore di n.*

DIMOSTRAZIONE. Sia L c.r.c. per $x^{p^n} - x$ su $\mathbb{F}_p$. Sia $f(x) \in \mathbb{F}_p[X]$ monico e irriducibile di grado $m|n$. Sia u uno zero di $f(x)$ in una opportuna estensione. Allora $\mathbb{F}_p(u)/\mathbb{F}_p$ è di Galois, quindi contiene un c.r.c. per $f(x)$. Inoltre $[\mathbb{F}_p(u) : \mathbb{F}_p] = m$. Ne segue che $\mathbb{F}_p(u)$ è c.r.c. su $\mathbb{F}_p$ per $x^{p^m} - x$, che divide $x^{p^n} - x$, quindi ogni zero di $f(x)$ è anche zero di $x^{p^n} - x$, e $\mathbb{F}_p(u)$ ha ordine m. Quindi $\mathbb{F}_p(u)$ è isomorfo all'unico sottogruppo di $\mathcal{G}(L/\mathbb{F}_p)$ di ordine p^m, sia esso K. Possiamo assumere $K = \mathbb{F}_p(u)$. Ne consegue che, essendo $f(x)$ irriducibile e quindi separabile in $\mathbb{F}_p[X]$ (essendo $\mathbb{F}_p$ finito, quindi perfetto), $f(x)$ divide $x^{p^n} - x$.

D'altra parte se u è uno zero di $x^{p^n} - x$ in L (ovvero $u \in L$) allora detto $f(x)$ il polinomio minimo di u su $\mathbb{F}_p$, $f(x)$ si fattorizza completamente in L essendo $L/\mathbb{F}_p$ estensione di Galois, quindi $f(x)$ divide $x^{p^n} - x$ essendo separabile. Sia ora m il grado di $f(x)$. Allora $[\mathbb{F}_p(u) : \mathbb{F}_p] = m$ e quindi $|\mathbb{F}_p(u)| = p^m$. Quindi $m|n$ dalla formula dei gradi (o dal teorema 31 di struttura). □

Per esempio consideriamo $E = \mathbb{F}_{16} := \mathbb{F}_2(a)$ con a di grado 4 su $\mathbb{F}_2$. Sappiamo che gli intercampi di E sono 3, uno per ogni divisore di 4. Essi sono $\mathbb{F}_2$, $\mathbb{F}_4$ e $\mathbb{F}_{16}$. L'ordine indotto dall'inclusione sul reticolo degli intercampi è totale, nel senso che $\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16}$. Gli $u \in E$ tali che $\mathbb{F}_2(u) = E$ sono gli elementi di $\mathbb{F}_{16} - \mathbb{F}_4$, quindi sono 12. Invece i generatori di $\mathbb{F}_{16}^*$ sono $\phi(16-1) = \phi(15) = \phi(5\cdot 3) = \phi(5)\cdot\phi(3) = 4 \cdot 2 = 8$, dove φ è la funzione di Euler.

LEMMA 26. *Sia $f(x) \in \mathbb{F}_p[X]$. Se α è zero di $f(x)$ in qualche estensione E di $\mathbb{F}_p$ allora anche α^p è zero di $f(x)$.*

DIMOSTRAZIONE. L'endomorfismo di Frobenius è automorfismo di E e ristretto a $\mathbb{F}_p$ è l'identità. □

PROPOSIZIONE 28. *Sia $f(x) \in \mathbb{F}_p[X]$ irriducibile di grado n e monico. Se $\alpha \in E \geq \mathbb{F}_p$ è uno zero di $f(x)$ allora in $E[X]$*

$$f(x) = (x-\alpha)(x-\alpha^p)...(x-\alpha^{p^{n-1}})$$

DIMOSTRAZIONE. Sappiamo che α^{p^i} è zero di $f(x)$ per ogni $i = 0, ..., n-1$. Basta quindi provare che gli α^{p^i} sono distinti. Supponiamo $\alpha^{p^i} = \alpha^{p^j}$ con $i < j$. Allora α^{p^i} è zero di $x^{p^{j-i}} - x$. $f(x)$ è il polinomio minimo di α^{p^i} su $\mathbb{F}_p$ perciò divide $x^{p^{j-i}} - x$, quindi per l'osservazione 6, n divide $j-i$, che è minore di n. Quindi $j - i = 0$. □

Ora sia E campo finito di ordine p^n con p primo. Definiamo una relazione di equivalenza su E dicendo che $\alpha \sim \beta$ se e solo se α e β hanno lo stesso polinomio minimo su $\mathbb{F}_p$. Sia $\alpha \in E$ un generatore di E^*, cioè tale che

$$E^* = \{1, \alpha, ..., \alpha^{p^n-2}\}$$

Definiamo una nuova relazione di equivalenza, chiamiamola ancora $\sim$, sull'insieme $\{0, 1, ..., p^{n-2}\}$, equipotente a E, dicendo che $a \sim b$ se e solo se $\alpha^a \sim \alpha^b$. Le classi di tale partizione si dicono classi ciclotomiche modulo $p^n - 1$. Osserviamo subito che se $C \subseteq \{0, 1, ..., p^n - 2\}$ è classe ciclotomica allora $|C|$ divide n, essendo il grado di un polinomio irriducibile su $\mathbb{F}_p$ che ha come zeri elementi di E (quindi se u è un suo zero allora $\mathbb{F}_p(u)$ ha ordine p^m per qualche $m|n$).

Sia ora $0 \leq s \leq p^n - 2$ e sia C_s la classe ciclotomica di s. Se $|C_s| = m_s$ abbiamo che gli zeri del polinomio minimo di α^s (ovvero gli elementi di E equivalenti a α^s) sono $\alpha^s, \alpha^{sp}, ..., \alpha^{sp^{m_s-1}}$. m_s è quindi il più piccolo intero positivo tale che $sp^{m_s} - s$ è divisibile per $p^n - 1$. m_s è dunque la più piccola soluzione positiva della congruenza

$$sp^{m_s} \equiv s \ mod(p^n - 1)$$

Riassumendo:

PROPOSIZIONE 29 (Criterio di costruzione di polinomi irriducibili). *Sia $F := \mathbb{F}_p$ e sia $E \geq F$ di ordine p^n, ovvero di grado n su F. Sia inoltre $\alpha \in E$ un generatore del gruppo ciclico E^*. Sia $s \in \{0, 1, ..., p^n - 2\}$ e sia $f(x) \in F[X]$ il polinomio minimo di α^s su F. Allora detta m_s la minima soluzione positiva della congruenza*

$$sp^{m_s} \equiv s \ mod(p^n - 1)$$

si ha che m_s è il grado di $f(x)$ e

$$f(x) = (x-\alpha^s)(x-\alpha^{sp})...(x-\alpha^{sp^{m_s-1}})$$

Inoltre la classe ciclotomica di s consiste delle classi di sp^i modulo $p^n - 1$ comprese tra 0 e $p^n - 2$, ove $i = 0, ..., m_s - 1$.

Ad esempio se $E = \mathbb{F}_{16}$ si ha: $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$, $C_7 = \{7, 14, 13, 11\}$. Consideriamo ora $f(x) := x^4 + x + 1 \in \mathbb{F}_2[X]$. Mostriamo che è irriducibile. Se fosse riducibile e avesse un fattore di grado 1

allora ammetterebbe uno zero in $\mathbb{F}_2$, ma questo non è vero perché $f(0) = 1 = f(1)$. L'unica scomposizione possibile è quella in due fattori di grado 2:

$$\begin{aligned} f(x) &= x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1) \\ &= x^4 + bx^3 + x^2 + ax^3 + abx^2 + ax + x^2 + bx + 1 \\ &= x^4 + (a+b)x^3 + abx^2 + (a+b)x + 1 \end{aligned}$$

Questo è assurdo perché implicherebbe $a + b = 0$ e $a + b = 1$. Ne segue che $f(x)$ è irriducibile in $\mathbb{F}_2[X]$. Se a è uno zero di $f(x)$ in un opportuna estensione (il che implica $a^4 = a + 1$) allora $\mathbb{F}_{16} \cong \mathbb{F}_2(a)$. Abbiamo che a è un generatore di E^*, infatti: $a^0 = 1$, $a^1 = a$, $a^2 = a^2$, $a^3 = a^3$, $a^4 = a + 1$, $a^5 = a^2 + a$, $a^6 = a^3 + a^2$, $a^7 = a^3 + a + 1$, $a^8 = a^2 + 1$, $a^9 = a^3 + a$, $a^{10} = a^2 + a + 1$, $a^{11} = a^3 + a^2 + a$, $a^{12} = a^3 + a^2 + a + 1$, $a^{13} = a^3 + a^2 + 1$, $a^{14} = a^3 + 1$.

Ora applicando quello che conosciamo abbiamo che il polinomio minimo di a dev'essere il polinomio monico i cui zeri sono $a,\ a^2,\ a^4,\ a^8$. Calcoliamo

$$\begin{aligned} &(x-a)(x-a^2)(x-a^4)(x-a^8) \\ &= (x^2 - (a+a^2)x + a^3)(x^2 - (a^4+a^8)x + a^{12}) \\ &= (x^2 + a^5x + a^3)(x^2 + a^5x + a^{12}) \\ &= x^4 + a^5x^3 + a^{12}x^2 + a^5x^3 + a^{10}x^2 + a^2x + a^3x^2 + a^8x + 1 \\ &= x^4 + (a^{12} + a^{10} + a^3)x^2 + (a^8 + a^2)x + 1 \\ &= x^4 + x + 1 \end{aligned}$$

come dev'essere. Analogamente, detto $f_i(x)$ il polinomio minimo di a^i si ha

$$f_1(x) = x^4 + x + 1,\ f_3(x) = x^4 + x^3 + x^2 + x + 1$$

$$f_5(x) = x^2 + x + 1,\ f_7(x) = x^4 + x^3 + 1$$

In particolare ci sono 3 polinomi monici irriducibili di grado 4 in $\mathbb{F}_2[X]$.

16. La funzione di Moebius

Il nostro obiettivo ora è studiare $N_p(n)$, per definizione il numero dei polinomi monici irriducibili di grado n in $\mathbb{F}_p[X]$. Per fare questo introduciamo la funzione di Moebius.

Definizione 58 (La funzione di Moebius). *La funzione di Moebius classica è la funzione*

$$\mu : \mathbb{N} - \{0\} \to \{0, -1, 1\}$$

che manda $0 \neq n \in \mathbb{N}$ *in* 1 *se* $n = 1$, *in* $(-1)^r$ *se* n *è prodotto di* r *primi distinti, e in* 0 *se* n *è divisibile per un quadrato maggiore di* 1.

Così ad esempio $\mu(14) = \mu(2 \cdot 7) = (-1)^2 = 1$, $\mu(12) = \mu(2^2 \cdot 3) = 0$, $\mu(30) = \mu(3 \cdot 5 \cdot 2) = (-1)^3 = -1$.

Lemma 27. *Sia* μ *la funzione di Moebius.*

1. *Se* $n, m \in \mathbb{N}$ *sono coprimi allora* $\mu(nm) = \mu(n)\mu(m)$.
2. *Se* $n > 1$ *allora* $\sum_{d|n} \mu(d) = 0$.

Dimostrazione.

(1) Se $n = 1$ o $m = 1$ il risultato è immediato. Supponiamo $n, m \neq 1$. $\mu(nm) = 0$ se e solo se $\mu(n) = 0$ oppure $\mu(m) = 0$, e questo è immediato dal fatto che m e n sono coprimi. Se invece n è prodotto di r primi distinti e m è prodotto di s primi distinti allora mn è prodotto di $r + s$ primi distinti, quindi $\mu(nm) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(n)\mu(m)$.
(2) Sia $n = p_1^{e_1}...p_r^{e_r}$ la fattorizzazione di n in primi, con $p_i \neq p_j$ se $i \neq j$, e $e_i > 0$ per ogni $i = 1, ..., r$. Se d divide n, $d = p_1^{f_1}...p_r^{f_r}$ con $f_i \in \{0, 1\}$ per ogni $i = 1, ..., r$ se e solo se $\mu(d) \neq 0$. Quindi

$$\sum_{d|n} \mu(d) = \sum_{d|p_1...p_r} \mu(d) = \sum_{i=0}^{r} (-1)^i \binom{r}{i} = (1-1)^r = 0$$

Infatti ci sono $\binom{r}{i}$ divisori di $p_1...p_r$ la cui fattorizzazione in primi consiste di i primi distinti (esattamente il numero dei sottoinsiemi di $\{1, ..., r\}$ di i elementi). Quando $i = 0$, $d = 1$. L'ultima uguaglianza deriva dallo sviluppo del binomio di Newton.

□

Teorema 32 (Formula di inversione di Moebius). *Sia G gruppo abeliano con notazione additiva, e sia $f : \mathbb{N} - \{0\} \to G$. Posto $F(n) := \sum_{d|n} f(d)$, per ogni $n \in \mathbb{N} - \{0\}$ si ha*

$$f(n) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$$

Dimostrazione. Detto d un divisore di n, sia $e = n/d$. Chiaramente se d descrive i divisori di n lo stesso fa e. Ora

$$\sum_{d|n} \mu(\frac{n}{d}) F(d) = \sum_{e|n} \mu(e) F(\frac{n}{e}) = \sum_{e|n} (\mu(e) \sum_{t|\frac{n}{e}} f(t)) = \sum_{e|n} (\sum_{t|\frac{n}{e}} \mu(e) f(t))$$

Ora $\{(t, e) \in \mathbb{N}^2 \mid e|n,\ t|\frac{n}{e}\} = \{(t, e) \in \mathbb{N}^2 \mid e|n,\ te|n\} = \{(t, e) \in \mathbb{N}^2 \mid t|n,\ e|\frac{n}{t}\}$. Di conseguenza

$$\sum_{e|n} (\sum_{t|\frac{n}{e}} \mu(e) f(t)) = \sum_{t|n} (\sum_{e|\frac{n}{t}} \mu(e)) f(t) = f(n)$$

Infatti per il lemma 27 nella sommatoria interna l'unico caso in cui ci sono addendi non nulli è quello per cui $n/t = 1$, ovvero $t = n$. □

Per esempio se $f = \varphi : \mathbb{N} - \{0\} \to \mathbb{Z}$ è la funzione di Euler $F(n) = \sum_{d|n} \varphi(d) = n$, quindi per la formula di inversione

$$\varphi(n) = \sum_{d|n} d\mu(\frac{n}{d})$$

Possiamo ora giungere dove volevamo:

Proposizione 30. *Se p è un primo e $n \geq 1$ allora*

$$N_p(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$$

In particolare $N_p(n) \geq 1$.

DIMOSTRAZIONE. Sia $f : \mathbb{N} - \{0\} \to \mathbb{Z},\ n \mapsto nN_p(n)$. Sappiamo che $F(n) = \sum_{d|n} f(d) = p^n$ perché $F(n)$ è esattamente il grado del prodotto di tutti i polinomi monici irriducibili di grado un divisore di n, che sappiamo essere uguale a $x^{p^n} - x$. Dalla formula di inversione

$$nN_p(n) = \sum_{d|n} \mu(\frac{n}{d})p^d$$

da cui il risultato. □

Per esempio $N_2(4) = \frac{1}{4}(\mu(4) \cdot 2 + \mu(2) \cdot 4 + \mu(1)2^4) = 3$, come sappiamo.

17. Il teorema dell'elemento primitivo

DEFINIZIONE 59 (Elemento primitivo). *Siano K un campo, L un'estensione semplice di K. Ogni $\alpha \in L$ tale che $L = K(\alpha)$ si dice elemento primitivo dell'estensione.*

LEMMA 28. *Sia L/K un'estensione semplice con $L = K(\alpha)$ e sia T un intercampo. Allora $T = K(a_0, ..., a_{n-1})$ dove $a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n$ è il polinomio minimo di α su T.*

DIMOSTRAZIONE. Sia $R := K(a_0, ..., a_{n-1}) \leq T$. Allora $a_0 + a_1x + ... + a_{n-1}x^{n-1}$ è irriducibile in $T[X]$, quindi anche in $R[X]$, e quindi $[L : R] = n = [L : T]$. Segue che $R = T$. □

TEOREMA 33. *Sia L/K un'estensione finita. Essa è semplice se e solo se $[L/K]$, l'insieme degli intercampi, è finito.*

DIMOSTRAZIONE. Proviamo la necessità. Scriviamo $L = K(\alpha)$ con α algebrico su K e di grado n, con polinomio minimo $f(x)$ su K. Per il lemma 28 un intercampo T è individuato dal polinomio minimo $g(x)$ di α rispetto a T, che divide $f(x)$. Basta allora osservare che solo un numero finito di polinomi divide $f(x)$.

Proviamo la sufficienza. Se K è finito allora anche L è finito e non abbiamo problemi: i generatori del gruppo moltiplicativo ciclico $L - \{0\}$ sono elementi primitivi per L/K. Supponiamo quindi K infinito. Dato $u \in L - K$, $K(u)/K$ è estensione finita: scegliamo un tale u in modo che il grado $[K(u) : K]$ sia il massimo possibile. Mostriamo che $K(u) = L$. Per assurdo esista $v \in L - K(u)$. Consideriamo gli intercampi $K(u + \alpha v)$ al variare di $\alpha \in K$: siccome $[L/K]$ è finito e K è infinito devono esistere $\alpha_1, \alpha_2 \in K$ distinti tali che $K(u + \alpha_1 v) = K(u + \alpha_2 v)$. Si ha

$$(\alpha_1 - \alpha_2)v = (u + \alpha_1 v) - (u + \alpha_2 v) \in K(u + \alpha_1 v).$$

Segue che $v \in K(u + \alpha_1 v)$ e quindi $u \in K(u + \alpha_1 v)$. Segue che

$$K(u) < K(u, v) \leq K(u + \alpha_1 v)$$

e questo contraddice la massimalità di $[K(u) : K]$. □

Come corollario otteniamo immediatamente che:

COROLLARIO 3. *Se L/K è un'estensione finita e semplice allora per ogni intercampo T l'estensione T/K è semplice.*

Il seguente teorema è di fondamentale importanza.

TEOREMA 34 (Teorema dell'Elemento Primitivo). *Ogni estensione finita separabile è un'estensione semplice.*

DIMOSTRAZIONE. Sia T/K un'estensione finita separabile. Siano $r = [T : K]$ e $\{u_1, ..., u_r\}$ una base di T su K. Per ogni $i = 1, ..., r$ sia $f_i(x)$ il polinomio minimo di u_i su K (che esiste perché l'estensione T/K è finita e quindi algebrica). Sia L un c.r.c. su K per il polinomio $f_1(x)...f_r(x)$. Allora per il teorema 29 L/K è un'estensione di Galois perché gli $f_i(x)$ sono irriducibili su K e separabili. Quindi $\mathcal{G}(L/K)$ è un gruppo finito di ordine $[L : K]$, in particolare ha un numero finito di sottogruppi, che sono in corrispondenza biunivoca con gli intercampi tramite le corrispondenze. Concludiamo usando il teorema 33. □

ESERCIZIO 90. *Sia K un campo infinito di caratteristica $p > 0$, e sia $L = K(u, v)$ con $u^p, v^p \in K$ e $[L : K] = p^2$. Mostrare che L/K non è semplice.*

18. Chiusure split

DEFINIZIONE 60. *Sia L/K estensione finita. $M \geq L$ si dice chiusura split di L su K se M è c.r.c. su K e nessun altro campo tra L e M è c.r.c. su K.*

PROPOSIZIONE 31. *Sia L/K estensione finita. Allora esiste una chiusura split per L su K, e due tali chiusure split sono L-isomorfe. Se L è separabile su K e M è una chiusura split per L su K allora M/K è di Galois.*

DIMOSTRAZIONE. Sia $L = K(v_1, ..., v_n)$ ove $\{v_1, ..., v_n\}$ sia base di L su K, e sia $f(x) := f_1(x)...f_n(x)$ dove $f_i(x)$ è il polinomio minimo di v_i su K. Sia M c.r.c. per $f(x)$ su L. Allora M è c.r.c. per $f(x)$ su K, e se $K \leq L \leq S \leq M$, dove S è un c.r.c. su K, allora poiché $u_1, ..., u_n \in S$ i polinomi $f_1(x), ..., f_n(x)$ ammettono uno zero in S, dunque si fattorizzano completamente in S (teorema 18). Quindi $S \leq M$ e S contiene un c.r.c. per $f(x)$ su L. Ne segue che $S = M$ per minimalità. Di conseguenza una qualunque chiusura split di L su K è un c.r.c. di $f(x)$ su L, quindi è L-isomorfo a M (teorema 17). Se L/K è separabile allora i fattori irriducibili di $f(x)$ sono separabili, quindi M/K è di Galois (teorema 29). □

Diremo **chiusura normale secondo Kaplasky** (o più brevemente "chiusura normale") una chiusura split di una estensione finita separabile. Si tratta di una estensione di Galois minimale.

COROLLARIO 4. *Sia L/K estensione di campi algebrica. Gli elementi di L separabili su K formano un campo.*

DIMOSTRAZIONE. Siano $a_1, a_2 \in L$ separabili su K. Sia M una chiusura split di $K(a_1, a_2)$ su K, e siano $f_1(x),\ f_2(x)$ i polinomi minimi rispettivamente di a_1 e a_2 su K. Allora $f(x) := f_1(x)f_2(x)$ è a fattori irriducibili separabili, e possiamo prendere come M un c.r.c. per $f(x)$ su K (si veda la dimostrazione della proposizione 31). Quindi M/K è di Galois finita. Sappiamo che un'estensione di Galois finita è separabile (teorema 25), quindi $a_1 - a_2,\ a_1 + a_2,\ a_1a_2,\ a_1a_2^{-1}$ sono separabili poiché appartengono a M. □

19. Traccia, norma, estensioni di Galois cicliche

DEFINIZIONE 61. *Sia K un campo. $\sigma_1, ..., \sigma_n \in \mathrm{Aut}(K)$ si dicono linearmente indipendenti su K se non esistono $a_1, ..., a_n \in K$ non tutti nulli tali che $a_1\sigma_1(c) + ... + a_n\sigma_n(c) = 0$ per ogni $c \in K$.*

PROPOSIZIONE 32. *Automorfismi distinti di un campo K sono linearmente indipendenti su K.*

DIMOSTRAZIONE. Siano, per assurdo, $\sigma_1, ..., \sigma_r \in \mathrm{Aut}(K)$ distinti, e $a_1, ..., a_r \in K$ non tutti nulli tali che $a_1\sigma_1(c) + ... + a_r\sigma_r(c) = 0$ per ogni $c \in K$. Inoltre sia r il minimo per cui ciò accade. Ciò implica che $a_i \neq 0$ per ogni $i = 1, ..., r$. Certamente $r \geq 2$ (l'applicazione nulla $K \to K$ non è automorfismo di K). Sia $b \in K$ tale che $\sigma_1(b) \neq \sigma_2(b)$. Allora si ha

$$a_1\sigma_1(bc) + ... + a_r\sigma_r(bc) = a_1\sigma_1(b)\sigma_1(c) + ... + a_r\sigma_r(b)\sigma_r(c) = 0.$$

Sottraiamo ora $\sigma_1(b)(a_1\sigma_1(c) + ... + a_r\sigma_r(c)) = 0$ ottenendo

$$a_2(\sigma_2(b) - \sigma_1(b))\sigma_2(c) + ... + a_r(\sigma_r(b) - \sigma_1(b))\sigma_r(c) = 0.$$

I coefficienti di questa combinazione lineare non sono tutti nulli perché $\sigma_1(b) \neq \sigma_2(b)$ e sono $r - 1$, quindi meno di r. Questo contraddice la minimalità di r. □

DEFINIZIONE 62 (Traccia e norma). *Sia L/K estensione di Galois finita con gruppo di Galois G. Dato $a \in L$ la traccia di a è per definizione*

$$\mathrm{Tr}(a) := \sum_{\sigma \in G} \sigma(a).$$

La norma di a è per definizione

$$N(a) := \prod_{\sigma \in G} \sigma(a).$$

Notiamo subito che se $a \in L$ la traccia e la norma di a sono elementi di K. Mostriamolo ad esempio per la traccia. Poiché L/K è di Galois basta (e bisogna) mostrare che $\mathrm{Tr}(a)$ è fissato da ogni $\gamma \in G$. Quindi sia $\gamma \in G$. Abbiamo

$$\gamma(\mathrm{Tr}(a)) = \gamma(\sum_{\sigma \in G} \sigma(a)) = \sum_{\sigma \in G} \gamma(\sigma(a)) = \sum_{\sigma \in G} \sigma(a) = \mathrm{Tr}(a).$$

Infatti $\{\gamma \circ \sigma \mid \sigma \in G\} = G$: Se $\delta \in G$ allora detto $\sigma := \gamma^{-1}\delta$ si ha $\gamma \circ \sigma = \delta$. Analogamente per $N(a)$.

OSSERVAZIONE 7. *Sia L/K estensione di Galois finita di grado n con gruppo di Galois G, e siano $a, b \in L$. Allora:*

1. $\mathrm{Tr}(a + b) = \mathrm{Tr}(a) + \mathrm{Tr}(b)$, $N(ab) = N(a)N(b)$.
2. *Se $a \in K$ allora* $\mathrm{Tr}(a) = n \cdot a$, $N(a) = a^n$.
3. *Se $a \in K$ allora* $\mathrm{Tr}(ab) = a\,\mathrm{Tr}(b)$.
4. *Se $\sigma \in G$ allora* $\mathrm{Tr}(\sigma(a)) = \mathrm{Tr}(a)$, $N(\sigma(a)) = N(a)$.
5. *La funzione* $\mathrm{Tr} : L \to K,\ a \mapsto \mathrm{Tr}(a)$ *è suriettiva.*

DIMOSTRAZIONE. Proviamo solo la quinta affermazione (le altre sono abbastanza immediate). Sia dunque $a \in K$. Per la proposizione 32 esiste $c \in L$ con $\mathrm{Tr}(c) \neq 0$. Sia $v := a(\mathrm{Tr}(c))^{-1}$. Allora $\mathrm{Tr}(vc) = v\,\mathrm{Tr}(c) = a$. □

Osserviamo inoltre che $\mathrm{Tr} : L \to K$ è omomorfismo di K-spazi vettoriali, e $N : L \to K$ è omomorfismo di gruppi moltiplicativi.
Ad esempio consideriamo l'estensione di Galois $\mathbb{C}/\mathbb{R}$. Dato $z = a + ib \in \mathbb{C}$,

$$\mathrm{Tr}(z) = a + ib + a - ib = 2a, \qquad N(z) = (a + ib)(a - ib) = a^2 + b^2.$$

Un'estensione di campi si dice ciclica se il suo gruppo di Galois è ciclico. Si dice abeliana se il suo gruppo di Galois è abeliano.

TEOREMA 35. *Sia L/K estensione di Galois finita di grado n e ciclica, e sia $G = \langle\sigma\rangle$ il suo gruppo di Galois. Sia $a \in L$. Allora* $\mathrm{Tr}(a) = 0$ *se e solo se esiste $b \in L$ tale che $a = b - \sigma(b)$.*

DIMOSTRAZIONE. La sufficienza è ovvia: $\mathrm{Tr}(b - \sigma(b)) = \mathrm{Tr}(b) - \mathrm{Tr}(\sigma(b)) = \mathrm{Tr}(b) - \mathrm{Tr}(b) = 0$. Proviamo la necessità. Sappiamo che $G = \{1, \sigma, ..., \sigma^{n-1}\}$. Se $n = 1$ allora $L = K$ e quindi $\mathrm{Tr}(a) = 0$ se e solo se $a = 0$. Sia quindi $n > 1$. Allora sappiamo che $\mathrm{Tr}(a) = a + \sigma(a) + ... + \sigma^{n-1}(a) = 0$. Poiché $\mathrm{Tr} : L \to K$ è suriettiva, esiste $c \in L$ tale che $\mathrm{Tr}(c) = 1$. Sia

$$b := ac + (a + \sigma(a))\sigma(c) + ... + (a + \sigma(a) + ... + \sigma^{n-2}(a))\sigma^{n-2}(c).$$

Allora

$$\begin{aligned} b - \sigma(b) = ac - \sigma(a)\sigma(c) + (a + \sigma(a))\sigma(c) - (\sigma(a) + \sigma^2(a))\sigma^2(c) + \\ +... + (a + \sigma(a) + ... + \sigma^{n-2}(a))\sigma^{n-2}(c) - (\sigma(a) + ... + \sigma^{n-1}(a))\sigma^{n-1}(c) = \\ = a\,\mathrm{Tr}(c) - a\sigma^{n-1}(c) - \sigma(a)\sigma^{n-1}(c) - ... - \sigma^{n-1}(a)\sigma^{n-1}(c) = \\ = a\,\mathrm{Tr}(c) - \sigma^{n-1}(c)\,\mathrm{Tr}(a) = a. \end{aligned}$$

□

TEOREMA 36. *Sia L/K estensione di campi con gruppo di Galois G e la caratteristica di K sia il primo p. Allora:*

1. *Se L/K è di Galois di grado p allora $L = K(u)$ con u zero di $x^p - x - a \in K[X]$ per qualche $a \in K$.*
2. *Se $L = K(u)$ con u zero di $x^p - x - a \in K[X]$ allora $L = K$ oppure L/K è di Galois di grado p.*

DIMOSTRAZIONE.

(1) Se L/K è di Galois di grado p allora $G = \langle\sigma\rangle$ è ciclico, il suo ordine essendo p. Inoltre $\mathrm{Tr}(1) = p \cdot 1 = 0$ e quindi per il teorema 35 esiste $u \in L$ tale che $1 = \sigma(u) - u$. In particolare $u \notin K$ (altrimenti $\sigma(u) = u$). Ne segue che $\sigma(u) = u + 1$. Inoltre $\sigma(u^p) = \sigma(u)^p = (u+1)^p = u^p + 1$. Quindi

$$\sigma(u^p - u) = \sigma(u^p) - \sigma(u) = u^p + 1 - u - 1 = u^p - u.$$

σ fissa $u^p - u$, quindi lo stesso fanno tutte le sue potenze, cioè tutti gli elementi di G. Poiché L/K è di Galois, $u^p - u = a \in K$. Quindi u è zero di $x^p - x - a \in K[X]$. Essendo L/K di Galois di grado p, non ci sono intercampi propri tra K e L (perché non ci sono sottogruppi propri di G con più di un elemento), quindi $L = K(u)$. Ne segue che il polinomio minimo di u su K ha grado p, quindi è proprio $x^p - x - a$. In particolare esso è irriducibile.

(2) Abbiamo $u^p - u - a = 0$. Se $i \in \mathbb{F}_p$ allora $(u + i)^p - (u + i) - a = u^p + i - u - i - a = u^p - u - a = 0$, quindi $u, u+1, ..., u+p-1$ sono tutti zeri di $x^p - x - a$, e sono distinti. Quindi $x^p - x - a = (x-u)(x-u-1)...(x-u-p+1)$ non ammette zeri multipli. $L = K(u)$ è c.r.c. per questo polinomio, quindi L/K è di Galois. Inoltre il polinomio minimo di u divide $x^p - x - a$, quindi $[L : K] \leq p$.
Ora se $\gamma \in G$, esso è determinato dal valore che assume in u, $\gamma(u)$, che è zero di $x^p - x - a$, dunque $\gamma(u) = u + i_\gamma$ per un unico $i_\gamma \in \mathbb{F}_p$. L'applicazione

$$G \to \mathbb{F}_p, \qquad \gamma \mapsto i_\gamma$$

è omomorfismo di gruppi (dove $\mathbb{F}_p$ è inteso come gruppo additivo), perché $i_{\gamma\tau} = i_\gamma + i_\tau$ per ogni $\gamma, \tau \in G$. Inoltre è chiaramente iniettivo. Ne segue che G è isomorfo a un sottogruppo del gruppo ciclico con p elementi, C_p, quindi $G = \{1_G\}$ oppure $|G| = p$. Nel primo caso $[L : K] = 1$ quindi $L = K$, $u \in K$ e $x^p - x - a$ si fattorizza in fattori lineari distinti in $K[X]$. Nel secondo caso $[L : K] = p$ quindi $x^p - x - a$ è irriducibile in $K[X]$.

□

In particolare se K è un campo di caratteristica p, il polinomio $x^p - x - a \in K[X]$ è irriducibile oppure si fattorizza in fattori lineari distinti.

TEOREMA 37 (90 di Hilbert). *Sia L/K estensione di Galois finita con gruppo di Galois $G = \langle\sigma\rangle$ ciclico. Un $a \in L$ ha norma 1 se e solo se esiste $0 \neq b \in L$ tale che $a = b \cdot \sigma(b)^{-1}$.*

DIMOSTRAZIONE. Sia $n = |G|$ e sia $G = \{1, \sigma, ..., \sigma^{n-1}\}$. Sia $a \in L$ con $N(a) = 1$. Se per qualche $b \neq 0$ in L si ha $a = b\sigma(b)^{-1}$ allora $N(a) = N(b\sigma(b)^{-1}) = N(b)N(\sigma(b)^{-1}) = N(b)N(\sigma(b))^{-1} = N(b)N(b)^{-1} = 1$. Proviamo il viceversa.
Poiché $1, \sigma, ..., \sigma^{n-1}$ sono distinti, essi sono linearmente indipendenti su K, quindi l'omomorfismo $\varphi : L \to L$ definito da

$$\varphi(c) = a\sigma^n(c) + a\sigma(a)\sigma(c) + ... + a\sigma(a)...\sigma^{n-1}(a)\sigma^{n-1}(c)$$

non è identicamente nullo. Scegliamo quindi $c \in L$ tale che $\varphi(c) = b \neq 0$. Per concludere basta mostrare che $\sigma(b) = a^{-1}b$. Si ha

$$\begin{aligned}\sigma(b) = \sigma(a)\sigma(c) + \sigma(a)\sigma^2(a)\sigma^2(c) + ... + \\ +\sigma(a)\sigma^2(a)...\sigma^{n-1}(a)\sigma^{n-1}(c) + a\sigma(a)...\sigma^{n-1}(a)c = \\ = a^{-1}(a\sigma(a)\sigma(c) + a\sigma(a)\sigma^2(a)\sigma^2(c) + \\ +... + a\sigma(a)\sigma^2(a)...\sigma^{n-1}(a)\sigma^{n-1}(c) + ac) = a^{-1}b.\end{aligned}$$

□

20. Campi ciclotomici

Esploriamo ora il terreno dei gruppi ciclici.

PROPOSIZIONE 33. *Sia G un gruppo ciclico. Allora $\mathrm{Aut}(G) \cong U(\mathbb{Z}/n\mathbb{Z})$ dove $n = 0$ se G è infinito, altrimenti $n = |G|$. Inoltre se $|G| = n$, $|\mathrm{Aut}(G)| = \varphi(n)$, dove φ è la funzione di Euler.*

DIMOSTRAZIONE. Sia $(G, +)$ un gruppo abeliano. Indichiamo con $\mathrm{End}(G)$ l'insieme degli endomorfismi di G, ovvero degli omomorfismi $G \to G$. $\mathrm{End}(G)$ è un anello rispetto a somma e composizione. Quindi $U(\mathrm{End}(G)) = \mathrm{Aut}(G)$, cioè $\mathrm{Aut}(G)$ è il gruppo degli elementi invertibili di $\mathrm{End}(G)$. Sia

$$\alpha : \mathbb{Z} \to \mathrm{End}(G)$$

$$m \mapsto m_\sigma$$

dove $m_\sigma : G \to G$, $g \mapsto m \cdot g$. α è un omomorfismo di anelli perché $(m + n)_\sigma = m_\sigma + n_\sigma$ e $(mn)_\sigma = m_\sigma \circ n_\sigma$, per ogni $m, n \in \mathbb{Z}$.

Se $G = \langle a \rangle$ è ciclico, e $\gamma \in \mathrm{End}(G)$ allora $\gamma(a) \in G$, quindi esiste $m \in \mathbb{Z}$ tale che $\gamma(a) = m \cdot a$. Ne segue che per ogni $n \in \mathbb{Z}$ si ha

$$\gamma(n \cdot a) = \gamma(a + ... + a) = \gamma(a) + ... + \gamma(a) = m \cdot a + ... + m \cdot a = n \cdot (m \cdot a) = \\ = (nm) \cdot a = (mn) \cdot a = m \cdot (n \cdot a) = m_\sigma(n \cdot a).$$

Quindi $\gamma = m_\sigma$. Di conseguenza α è suriettiva. Se G è infinito α è anche iniettiva, quindi $\mathbb{Z} \cong \mathrm{End}(G)$. Se invece $|G| = n$ allora è immediato che $ker(\alpha) = n\mathbb{Z}$, quindi $\mathrm{End}(G) \cong \mathbb{Z}/n\mathbb{Z}$. Quindi $\mathrm{Aut}(G) = U(\mathrm{End}(G)) \cong U(\mathbb{Z}/n\mathbb{Z})$. Gli elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$ corrispondono a quei $m \in \{0, 1, ..., n-1\}$ tali che $mq \equiv 1 \ mod(n)$ per qualche $q \in \mathbb{Z}$. In tal caso un eventuale fattore comune a m e n deve dividere 1, quindi è necessario che $(m, n) = 1$. D'altra parte se $(m, n) = 1$ allora abbiamo l'identità di Bézout $am + bn = 1$ per qualche $a, b \in \mathbb{Z}$, da cui segue che $am \equiv 1 \ mod(n)$. Quindi $|U(\mathbb{Z}/n\mathbb{Z})|$ è uguale al numero dei numeri interi compresi tra 1 e n, coprimi con n. È quindi uguale a $\varphi(n)$, dove φ è la funzione di Euler. □

Definizione 63 (Campi ciclotomici). *Sia K campo e sia $n \in \mathbb{N}$. Un c.r.c. per $x^n - 1$ su K si dice n-esimo campo ciclotomico su K.*

Notiamo subito che $x^n - 1$ ha zeri multipli se e solo se $n \cdot 1 = 0$, se e solo se $\chi(K)$ divide n. In questo caso $\chi(K) = p > 0$ e $n = mp^l$ con $(m, p) = 1$. Quindi $x^n - 1 = x^{mp^l} - 1 = (x^m - 1)^{p^l}$, quindi l'$n$-esimo campo ciclotomico coincide con l'm-esimo.
Possiamo quindi supporre che $\chi(K)$ non divida n. Sia L un n-esimo campo ciclotomico su K, e sia $A \subseteq L$ l'insieme degli zeri di $x^n - 1$ in L. A è un gruppo moltiplicativo ciclico di ordine n, e poiché $x^n - 1$ non ha zeri multipli, L/K è di Galois. I generatori di A come gruppo ciclico si chiamano radici primitive n-esime di 1. Se $A = \langle \omega \rangle$ allora $L = K(\omega)$.
Sia $G := \mathcal{G}(L/K)$. Poiché $L = K(\omega)$ ogni $\sigma \in G$ è determinato da $\sigma(\omega)$. Quindi l'omomorfismo

$$G \to \mathrm{Aut}(A)$$
$$\sigma \mapsto \sigma|_A$$

è iniettivo, infatti se $\sigma|_A$ è l'identità di A allora $\sigma(\omega) = \omega$ quindi $\sigma = \mathrm{Id}_G$. Di conseguenza G si immerge nel gruppo degli automorfismi del gruppo ciclico di ordine n, ovvero per la proposizione 33, $G \hookrightarrow U(\mathbb{Z}/n\mathbb{Z})$. In particolare, G è abeliano:

Osservazione 8. *Sia K un campo la cui caratteristica non divida $n \in \mathbb{N}$, e sia L un n-esimo campo ciclotomico su K. Allora l'estensione di Galois L/K è abeliana: il suo gruppo di Galois è isomorfo a un sottogruppo di $U(\mathbb{Z}/n\mathbb{Z})$.*

Ora sia M/K estensione di campi, e sia $0 \neq a \in K$. Supponiamo che per un dato $n \in \mathbb{N}$ i polinomi $x^n - 1$ e $x^n - a$ si decompongano in fattori lineari in $M[X]$. Sia $A \subseteq M$ l'insieme degli zeri di $x^n - 1$ in M, e sia $B \subseteq M$ l'insieme degli zeri di $x^n - a$ in M. Fissato $u \in B$ consideriamo $\delta : A \to B$, $\eta \mapsto u\eta$. Allora δ è una biiezione: se $u\eta_1 = u\eta_2$ allora $\eta_1 = \eta_2$, e se $v \in B$ allora $u^{-1}v \in A$ in quanto $(u^{-1}v)^n = u^{-n}v^n = a^{-1}a = 1$, e $\delta(u^{-1}v) = v$.

Proposizione 34. *Sia K un campo che contenga l'n-esimo campo ciclotomico (ove $n \in \mathbb{N}$), sia $a \in K$, sia u uno zero di $x^n - a$ in una opportuna estensione, e sia $L = K(u)$. Allora L è c.r.c. per $x^n - a$ su K, e $G := \mathcal{G}(L/K)$ è ciclico e il suo ordine divide n.*

DIMOSTRAZIONE. Sia A l'insieme delle radici n-esime di 1 in K. L è c.r.c. per $x^n - a$ su K perché $L = K(u) = K(u, \varepsilon u, ..., \varepsilon^{n-1}u)$ dove ε è una radice primitiva n-esima di 1. Se $\sigma \in G$ esiste un unico $\eta_\sigma \in A$ tale che $\sigma(u) = u\eta_\sigma$. Si vede facilmente che l'applicazione

$$\delta : G \to A$$
$$\sigma \mapsto \eta_\sigma$$

è omomorfismo di gruppi iniettivo. Quindi G, immergendosi in A, è ciclico e il suo ordine divide $|A| = n$. □

TEOREMA 38. *Sia L/K estensione di Galois finita, con gruppo di Galois G, ciclico di ordine n. Se K contiene un n-esimo campo ciclotomico allora $L = K(u)$ ove u è uno zero di un polinomio del tipo $x^n - a \in K[X]$ irriducibile in $K[X]$.*

DIMOSTRAZIONE. Sia $G = \langle\sigma\rangle$. Sia $\varepsilon \in K$ radice primitiva n-esima di 1. Allora $N(\varepsilon) = \varepsilon^n = 1$, quindi per il teorema 90 di Hilbert (teorema 37) esiste $u \in L$ tale che $\varepsilon = \sigma(u)u^{-1}$, ovvero $\sigma(u) = u\varepsilon$. Di conseguenza $\sigma(u^n) = \sigma(u)^n = (\varepsilon u)^n = u^n$ quindi ogni potenza di σ (i.e. ogni elemento di G) fissa u^n. L/K è di Galois, quindi $u^n \in K$. Ne segue che detto $a := u^n \in K$, u è zero di $x^n - a$. Sia ora $g(x) \in K[X]$ il polinomio minimo di u su K. Allora $g(x)$ divide $x^n - a$, e $u,\ \sigma(u) = u\varepsilon, ...,\ \sigma^{n-1}(u) = \varepsilon^{n-1}u$ sono n zeri distinti di $g(x)$. Di conseguenza $g(x) = x^n - a$, quindi $x^n - a$ è irriducibile in $K[X]$. Inoltre il grado di L su K è n, uguale al grado di $K(u)$ su K, quindi $L = K(u)$. □

21. Determinazione del gruppo di Galois

DEFINIZIONE 64 (Gruppo di Galois di un polinomio). *Sia K un campo e sia $f(x) \in K[X]$ di grado positivo. Sia M un c.r.c. per $f(x)$ su K. Il gruppo $\mathcal{G}_f := \mathcal{G}(M/K)$ si dice gruppo di Galois di $f(x)$. Esso è identificato a meno di isomorfismi: se M_0 è un altro c.r.c. per $f(x)$ su K allora $M_0 \cong M$.*

21.1. I polinomi ciclotomici. Determineremo ora il gruppo di Galois dei polinomi ciclotomici su $\mathbb{Q}$.

DEFINIZIONE 65. *Sia P il sottoinsieme di $\mathbb{C}$ che consiste delle radici primitive n-esime di 1 (ove $0 \neq n \in \mathbb{N}$). Sia*

$$\Phi_n(x) := \prod_{\eta \in P} (x - \eta)$$

$\Phi_n(x)$ si dice polinomio ciclotomico n-esimo.

PROPOSIZIONE 35. *Detto $0 \neq n \in \mathbb{N}$, si ha*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

DIMOSTRAZIONE. Se d divide n ogni radice primitiva d-esima di 1 è radice n-esima di 1. Viceversa se u è una radice n-esima di 1 allora è radice primitiva $|\langle u\rangle|$-esima di 1, e $|\langle u\rangle|$ divide n, essendo $\langle u\rangle$ un sottogruppo del gruppo delle radici n-esime di 1. I due polinomi in questione non hanno zeri multipli quindi sono uguali. □

Per esempio:

- $\Phi_1(x) = x - 1$.

- $\Phi_2(x) = (x^2-1)/(x-1) = x+1$.
- $\Phi_3(x) = (x^3-1)/(x-1) = x^2+x+1$.
- $\Phi_4(x) = (x^4-1)/(x-1)(x+1) = x^2+1$.
- $\Phi_5(x) = (x^5-1)/(x-1) = x^4+x^3+x^2+x+1$.
- $\Phi_6(x) = (x^6-1)/(x-1)(x+1)(x^2+x+1) = x^2-x+1$.

Se ε è una radice primitiva n-esima di 1 allora l'n-esimo campo ciclotomico è $L := \mathbb{Q}(\varepsilon)$, e l'estensione $L/\mathbb{Q}$ è di Galois essendo L c.r.c. su $\mathbb{Q}$ che ha caratteristica 0 quindi è perfetto. ε è zero di $\Phi_n(x)$. Abbiamo visto nell'osservazione 8 che G, il gruppo di Galois di L/K, è isomorfo a un sottogruppo di $U(\mathbb{Z}/n\mathbb{Z})$, quindi il suo ordine, uguale al grado $[L:K]$, divide $\varphi(n)$.
Mostriamo ora che per ogni $0 \neq n \in \mathbb{N}$ il polinomio ciclotomico n-esimo è monico e appartiene a $\mathbb{Z}[X]$. Certamente se $n = 1$ ciò è vero. Sia dunque $n \geq 2$. Ora, un prodotto di polinomi monici è monico, e

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n} \Phi_d(x)}$$

Per ipotesi induttiva ne consegue che $\Phi_n(x) \in \mathbb{Q}[X]$ e in realtà $\Phi_n(x) \in \mathbb{Z}[X]$ essendo $\Phi_n(x)$ il quoziente di una divisione tra polinomi monici, con resto 0.

Osservazione 9. *Se ε è una radice primitiva n-esima di 1 allora, detto P l'insieme delle radici primitive n-esime di 1, $P = \{\varepsilon^r \mid (r,n) = 1\}$. In particolare la cardinalità di P, uguale al grado di $\Phi_n(x)$, è $\varphi(n)$.*

Dimostrazione. Esercizio. □

Lemma 29. *Sia $0 \neq n \in \mathbb{N}$, e valga $\Phi_n(x) = f(x)g(x)$ in $\mathbb{Z}[X]$, con $f(x)$ monico e irriducibile in $\mathbb{Z}[X]$. Se $f(\eta) = 0$ e p è un primo che non divide n allora $f(\eta^p) = 0$.*

Dimostrazione. η^p è una radice primitiva n-esima di 1 per l'osservazione 9. Ne segue che $\Phi_n(\eta^p) = 0$. Supponiamo per assurdo che $f(\eta^p) \neq 0$. Allora certamente $g(\eta^p) = 0$, ovvero η è zero di $g(x^p)$. Quindi $f(x)$ divide $g(x^p)$, diciamo $g(x^p) = f(x)t(x)$ per qualche $t(x) \in \mathbb{Z}[X]$. Lo stesso rimane vero modulo p, usando l'omomorfismo di riduzione $\mathbb{Z}[X] \to \mathbb{F}_p[X]$. La classe di ogni coefficiente di $g(x^p)$ è fissata dall'endomorfismo di Frobenius, quindi

$$\bar{g}(x^p) = (\bar{g}(x))^p = \bar{f}(x)\bar{t}(x)$$

Sia $\psi(x) \in \mathbb{F}_p[X]$ un fattore irriducibile di $\bar{f}(x)$. Ne segue che $\psi(x)$ divide $\bar{g}(x)$, quindi $\psi(x)^2$ divide $\bar{f}(x)\bar{g}(x) = \overline{\Phi_n}(x)$ in $\mathbb{F}_p[X]$. Ma $\overline{\Phi_n}(x)$ divide $x^n - 1$, quindi in $\mathbb{F}_p$ $x^n - 1$ ha zeri multipli. Questo è assurdo perché $\chi(\mathbb{F}_p) = p$ non divide n. □

Ora se ε è uno zero di $\Phi_n(x)$ allora ogni altro zero di $\Phi_n(x)$ è del tipo $\eta = \varepsilon^{p_1 \cdots p_t}$ coi p_i primi che non dividono n (osservazione 9). Applicando il lemma t volte scopriamo che ogni η siffatto dev'essere zero di ogni fattore irriducibile di $\Phi_n(x)$ che ammette ε come zero, quindi $\Phi_n(x)$ è irriducibile in $\mathbb{Z}[X]$. Riassumendo:

Proposizione 36. *Per ogni $0 \neq n \in \mathbb{N}$ il polinomio $\Phi_n(x)$ è monico e irriducibile e appartiene a $\mathbb{Z}[X]$. Inoltre $\mathcal{G}_{x^n-1} \cong U(\mathbb{Z}/n\mathbb{Z})$.*

Dimostrazione. Per mostrare la seconda affermazione basta osservare che se ε è radice primitiva n-esima allora $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ è di Galois, quindi l'ordine del suo gruppo di Galois (sia esso G) è proprio il grado di $\Phi_n(x)$ (polinomio minimo di ε

su $\mathbb{Q}$), che è $\phi(n)$ per l'osservazione 9. Poiché G si immerge in $U(\mathbb{Z}/n\mathbb{Z})$ e ha lo stesso suo ordine (finito), tali due gruppi sono isomorfi. □

21.2. Gruppo di Galois dei polinomi. Dati un campo K e un polinomio $f(x) \in K[X]$, il gruppo di Galois di $f(x)$ è il gruppo di Galois di M/K dove M è c.r.c. per $f(x)$ su K. Tale gruppo è identificato a meno di isomorfismi perché due qualsivoglia c.r.c. su K per $f(x)$ sono isomorfi.

Ricordiamo che nella sezione relativa ai gruppi abbiamo studiato i reticoli dei sottogruppi di alcuni gruppi piccoli. Tali reticoli ci serviranno in quanto segue.

PROPOSIZIONE 37. *Sia K un campo. $f(x) \in K[X]$ abbia zeri tutti distinti, siano essi $\{x_1, ..., x_n\}$ in un c.r.c. M per $f(x)$ su K. Allora M/K è di Galois finita, e il gruppo di Galois di $f(x)$, sia esso $\mathcal{G}(M/K) = G$, si immerge in S_n. Consideriamo l'azione naturale di G su $\{x_1, ..., x_n\}$ data da $(\sigma, x_i) \mapsto \sigma(x_i)$. Tale azione è transitiva se e solo se $f(x)$ è irriducibile in $K[X]$.*

DIMOSTRAZIONE. G si immerge in S_n perché agisce fedelmente sugli n zeri di $f(x)$. Supponiamo che l'azione data sia transitiva, e sia $f_1(x)$ il polinomio minimo di x_1 su K. Allora per ogni $\sigma \in G$, $\sigma(x_1)$ è zero di $f_1(x)$. Quindi poiché G agisce transitivamente sugli zeri di $f(x)$, $f(x) = af_1(x)$ per qualche $a \in K$, quindi $f(x)$ è irriducibile.
Viceversa sia $f(x)$ irriducibile in $K[X]$. Dati x_i, x_j zeri di $f(x)$, M è c.r.c. per $f(x)$ sia su $K(x_i)$ che su $K(x_j)$, dunque l'isomorfismo $K(x_i) \to K(x_j)$ che estende l'identità di K e manda x_i in x_j ($f(x)$ è irriducibile: vedi teorema 16) si estende a un K-automorfismo di M (teorema 17), chiamiamolo σ. Allora $\sigma(x_i) = x_j$. □

Ora la caratteristica di K sia diversa da 2, e definiamo

$$\Delta := (x_1 - x_2)(x_1 - x_3)...(x_{n-1} - x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)$$

$D := \Delta^2$ si dice il discriminante di $f(x)$. Poiché ogni $\sigma \in G$ induce una permutazione degli x_i, Δ ne risente solo sottoforma di un eventuale cambio di segno, ovvero $\sigma(\Delta) \in \{\Delta, -\Delta\}$. Più esplicitamente se σ è pari, $\sigma(\Delta) = \Delta$, se σ è dispari, $\sigma(\Delta) = -\Delta$. Quindi per ogni $\sigma \in G$, $\sigma(D) = \sigma(\Delta^2) = \sigma(\Delta)^2 = (\pm\Delta)^2 = D$, quindi $D \in K$ perché M/K è di Galois. Sia ora $H := G \cap A_n$. Gli elementi di G che fissano ogni elemento di $K(\Delta)$ sono esattamente quelli che fissano Δ, ovvero $K(\Delta)' = H$. Poiché M/K è di Galois finita si ha $H' = K(\Delta)$ perché $K(\Delta)$ è chiuso.
Ora l'omomorfismo "segno" $G \to \{-1, 1\}$ ha come nucleo H, quindi se è suriettivo $[G : H] = 2$, se non lo è $G = H$. Di conseguenza $[G : H] \le 2$. Usando le corrispondenze, $[K(\Delta) : K] \le 2$. Inoltre $\Delta \in K$ se e solo se $G = H$, sempre per le corrispondenze. In tal caso (e solo in tal caso) D è un quadrato in K. Riassumendo:

PROPOSIZIONE 38. *Se $\chi(K) \neq 2$ e $f(x) \in K[X]$ ha zeri distinti, e M è c.r.c. per $f(x)$ su K, detto $G := \mathcal{G}(M/K)$ e detti Δ e D come sopra, si hanno i seguenti fatti:*

- *M/K è di Galois finita.*
- *G si immerge in S_n.*
- *$\Delta \in K$ se e solo se $G \subseteq A_n$, se e solo se D è un quadrato in K.*
- *$\Delta \notin K$ se e solo se $[K(\Delta) : K] = [G : G \cap A_n] = 2$.*

Prima di immergerci nello studio dei polinomi di grado "basso", enunciamo il seguente lemma, che raccoglie alcuni fatti tecnici che ci serviranno in seguito. Nel seguito il gruppo simmetrico S_n agisca nel modo naturale su $\{1, ..., n\}$.

LEMMA 30. *Si hanno i seguenti fatti:*

- *Gli unici sottogruppi transitivi di S_3 sono S_3 e A_3.*
- *L'unico sottogruppo di S_4 ciclico che viene normalizzato da $(3\ 4)$ è $\langle(1\ 3\ 2\ 4)\rangle$.*
- *Gli unici sottogruppi transitivi di S_4 sono $S_4,\ A_4,\ D_4,\ V,\ C_4$.*
- *S_4 è l'unico sottogruppo transitivo di S_4 che ha sottogruppi normali di indice 6; V è l'unico sottogruppo transitivo di S_4 contenuto in V; C_4 e D_4 sono gli unici sottogruppi transitivi di S_4 che contengono un sottogruppo normale di indice 2 contenuto in V.*
- *$V \leq D_4,\ V \lhd A_4 \lhd S_4,\ S_4/V \cong S_3,\ V \cong C_2 \times C_2$. Se $G \leq S_4$ allora $G \cap V \trianglelefteq G$.*

21.2.1. *Grado 3.* Sia K un campo e sia $f(x) \in K[X]$ irriducibile e separabile in $K[X]$, di grado 3. Per le proposizioni 37, 38, e per il lemma 30, le uniche possibilità per $G := \mathcal{G}_{f(x)}$ sono S_3 e A_3, e $G \cong A_3$ se e solo se D è un quadrato in K.
Sia ora $\chi(K) \notin \{2, 3\}$. Diciamo $f(x) = x^3 + bx^2 + cx + d \in K[X]$. Allora $g(x) := f(x - \frac{b}{3})$ è della forma $x^3 + px + q$ per qualche $p, q \in K$. Ora u è zero di $f(x)$ se e solo se $u + \frac{b}{3}$ è zero di $g(x)$, e se u_i, u_j sono due zeri di $f(x)$ allora $(u_i + \frac{b}{3}) - (u_j + \frac{b}{3}) = u_i - u_j$. Ne segue che $f(x)$ e $g(x)$ hanno lo stesso discriminante.

OSSERVAZIONE 10. *Nelle notazioni di cui sopra, il discriminante di $f(x)$ è*

$$D = -4p^3 - 27q^2.$$

DIMOSTRAZIONE. È sufficiente fare i conti. Sia $g(x) = (x - v_1)(x - v_2)(x - v_3)$ dove i v_i sono gli zeri di $g(x)$ in M. Allora da $g(x) = x^3 + px + q$ segue

$$x^3 + px + q = x^3 - (v_1 + v_2 + v_3)x^2 + (v_1v_2 + v_2v_3 + v_1v_3)x - v_1v_2v_3.$$

Quindi $v_1 + v_2 + v_3 = 0$, $v_1v_2 + v_1v_3 + v_2v_3 = p$, $-v_1v_2v_3 = q$. Osserviamo che in particolare $q = -v_1v_2v_3 \neq 0$, altrimenti uno zero di $g(x)$ sarebbe 0, quindi apparterrebbe a K e $g(x)$ non sarebbe irriducibile, quindi nemmeno $f(x)$. Ora,

$$\begin{aligned}
D &= \Delta^2 = (v_1 - v_2)^2(v_2 - v_3)^2(v_1 - v_3)^2 \\
&= ((v_1 + v_2)^2 - 4v_1v_2)((v_2 + v_3)^2 - 4v_2v_3)((v_1 + v_3)^2 - 4v_1v_3) \\
&= (v_3^2 + 4\frac{q}{v_3})(v_1^2 + 4\frac{q}{v_1})(v_2^2 + 4\frac{q}{v_2}) = \frac{1}{v_1v_2v_3}(v_3^3 + 4q)(v_1^3 + 4q)(v_2^3 + 4q) \\
&= -\frac{1}{q}(-pv_3 + 3q)(-pv_1 + 3q)(-pv_2 + 3q) \\
&= -\frac{1}{q}(p^2v_1v_3 - 3pqv_3 - 3pqv_1 + 9q^2)(-pv_2 + 3q) \\
&= -\frac{1}{q}(-p^3v_1v_2v_3 + 3p^2qv_1v_3 + 3p^2qv_2v_3 - 9pq^2v_3 + 3p^2qv_1v_2 - 9pq^2v_1 + \\
&\quad -9pq^2v_2 + 27q^3) \\
&= -\frac{1}{q}(qp^3 + 3p^3q + 27q^3) = -p^3 - 3p^3 - 27q^2 = -4p^3 - 27q^2,
\end{aligned}$$

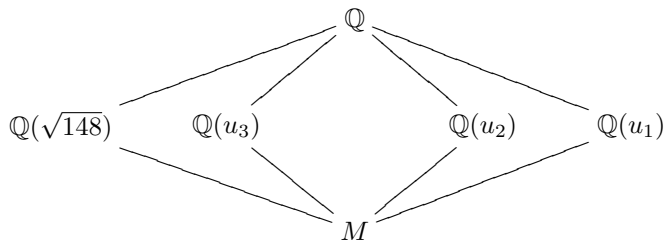
come volevamo. □

ESEMPIO: Sia $f(x) := x^3 - 3x + 1 \in_{irr} \mathbb{Q}[X]$. Che $f(x)$ sia irriducibile lo si vede osservando che non ammette zeri in $\mathbb{Z}$ perché essi dovrebbero dividere 1, ma $f(1) \neq 0 \neq f(-1)$. In questo caso $p = -3$ e $q = 1$, quindi $D = -4(-3)^3 - 27 \cdot 1^2 = 3 \cdot 27 = 81 = 9^2$. Di conseguenza $\mathcal{G}_{f(x)} \cong A_3 \cong C_3$, quindi non ci sono intercampi propri tra un qualsiasi c.r.c. M per $f(x)$ su $\mathbb{Q}$ e $\mathbb{Q}$. Quindi se $u \in M$ è uno zero di $f(x)$, $M = \mathbb{Q}(u)$.

ESEMPIO: Sia $f(x) := x^3 + 3x^2 - x - 1 \in \mathbb{Q}[X]$. $g(x) = f(x-1) = (x-1)^3 + 3(x-1)^2 - (x-1) - 1 = x^3 - 3x^2 + 3x - 1 + 3x^2 - 6x + 3 - x + 1 - 1 = x^3 - 4x + 2$. Per il criterio di Eisenstein $g(x)$ è irriducibile in $\mathbb{Q}[X]$. In questo caso $p = -4$, $q = 2$ quindi $D = -4(-4)^3 - 27 \cdot 2^2 = 148$ non è un quadrato in $\mathbb{Q}$. Di conseguenza $\mathcal{G}_{f(x)} \cong S_3$.

ESEMPIO: L'esempio precedente in $\mathbb{F}_7[X]$. Tramite una verifica diretta notiamo che $g(x) = x^3 - 4x + 2$ non ammette zeri in $\mathbb{F}_7$, dunque è irriducibile in $\mathbb{F}_7[X]$. Inoltre $D = 148 = 1$, di conseguenza il gruppo di Galois è A_3 perché 1 è un quadrato in $\mathbb{F}_7$.

ESEMPIO: Sia M un c.r.c. su $\mathbb{Q}$ per $g(x) := x^3 - 4x + 2$, irriducibile in $\mathbb{Q}[X]$ con gruppo di Galois S_3. Si ha $\Delta = \sqrt{148}$. Detti $u_1,\ u_2,\ u_3$ gli zeri di $g(x)$ in M, il reticolo degli intercampi di $M/\mathbb{Q}$ è



Lo si è ricavato dal reticolo dei sottogruppi di S_3.

ESEMPIO: Se il polinomio irriducibile di grado 3 $f(x) \in \mathbb{Q}[X]$ ha un solo zero reale, allora esistono $a, b, c \in \mathbb{R}$, con $b \neq 0$, tali che gli zeri di $f(x)$ siano $a+ib, a-ib, c$. Ne consegue che

$$D = (a + ib - (a - ib))^2(a + ib - c)^2(a - ib - c)^2 = -4b^2((a - c)^2 + b^2)^2 < 0$$

Quindi il gruppo di Galois di $f(x)$ è isomorfo a S_3. Inoltre $[M : \mathbb{Q}] = 6$ e $[\mathbb{Q}(\Delta) : \mathbb{Q}] = 2$, quindi $[M : \mathbb{Q}(\Delta)] = 3$. Se invece gli zeri di $f(x)$ sono tutti reali allora $D > 0$. Anche in questo caso $[M : \mathbb{Q}(\Delta)] = 3$, infatti se $[M : \mathbb{Q}] = 3$ allora $\Delta \in \mathbb{Q}$. Essendo $M/\mathbb{Q}$ di Galois, anche $M/\mathbb{Q}(\Delta)$ è di Galois e ha grado 3, quindi il suo gruppo di Galois è ciclico avendo ordine 3.

ESEMPIO: Sia $f(x) := (x^3 - 2)(x^2 - 5) \in \mathbb{Q}[X]$. Un c.r.c. su $\mathbb{Q}$ è $M := \mathbb{Q}(\sqrt{5}, \sqrt[3]{2}, i\sqrt{3})$. Se T è l'intercampo c.r.c. per $x^3 - 2$ allora T' è isomorfo al gruppo di Galois di $x^2 - 5$, che è C_2. Se L è l'intercampo c.r.c. per $x^2 - 5$ allora L' è isomorfo al gruppo di Galois di $x^3 - 2$, che è isomorfo a S_3 perché il discriminante di $x^3 - 2$ è minore di zero. Detto $G := \mathcal{G}_{f(x)}$ si ha quindi che $C_2, S_3 \leq G$. Inoltre essendo T e L c.r.c. per polinomi irriducibili, essi sono stabili in M/K, quindi T' e L' sono normali in G. Inoltre $T \cup L$ genera M, quindi $T' \cap L' = \{1_G\}$. In ultimo, ogni $\sigma \in G$ si scrive come prodotto di un $\gamma \in L'$ e di un $\delta \in T'$, quindi $G = L'T'$. Segue che G è isomorfo al prodotto diretto $S_3 \times C_2$.

21.2.2. *Grado 4.* Nel seguito useremo pesantemente il lemma 30.
Sia $f(x) \in K[X]$ irriducibile di grado 4, diciamo $f(x) = x^4 + bx^3 + cx^2 + dx + e$,

separabile con zeri $x_1, x_2, x_3, x_4 \in M$, ove M è un c.r.c. per $f(x)$ su K. Allora $\mathcal{G}_{f(x)} =: G \leq S_4$ è transitivo sugli zeri, e $G \cap V \trianglelefteq G$. Siano ora:

$$\alpha := x_1x_2 + x_3x_4,\ \beta := x_1x_3 + x_2x_4,\ \gamma := x_1x_4 + x_2x_3$$

Dal fatto che gli x_i sono distinti segue subito che α, β e γ sono distinti. È chiaro che se $\sigma \in G \cap V$ allora σ fissa α, β e γ. Viceversa se $\sigma \notin G \cap V$ allora σ muove uno tra α, β, γ, infatti se $\sigma \notin G$ allora σ è di uno dei seguenti tipi:

- Trasposizione. Per esempio se $\sigma = (1\ 2)$ allora $\beta \mapsto \gamma \mapsto \beta$.
- 3-ciclo. Per esempio se $\sigma = (1\ 2\ 3)$ allora $\alpha \mapsto \gamma \mapsto \beta \mapsto \alpha$.
- 4-ciclo. Per esempio se $\sigma = (1\ 2\ 3\ 4)$ allora $\gamma \mapsto \alpha \mapsto \gamma$.

Ne consegue che $K(\alpha, \beta, \gamma)' = G \cap V$, e $(G \cap V)' = K(\alpha, \beta, \gamma)$ essendo M/K di Galois. Quindi essendo $K(\alpha, \beta, \gamma)$ stabile in M/K, per il teorema 28 si ha

$$G/(G \cap V) \cong \mathcal{G}(K(\alpha, \beta, \gamma)/K)$$

Il polinomio

$$(x - \alpha)(x - \beta)(x - \gamma) \in K(\alpha, \beta, \gamma)[X]$$

si dice risolvente cubica di $f(x)$. I conti dimostrano che la risolvente cubica di $f(x) = x^4 + bx^3 + cx^2 + dx + e$ è

$$x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[X]$$

Le possibilità per G sono i sottogruppi di S_4 transitivi sugli zeri, ovvero S_4, A_4, D_4, V, C_4. Le possibilità per $G/(G \cap V)$ sono invece S_3, C_3, C_2, $\{1\}$, essendo $G/(G \cap V)$ isomorfo al gruppo di Galois della risolvente cubica di $f(x)$. Abbiamo tre casi possibili:

- $|G/(G \cap V)| = 6$. Allora $G = S_4$ essendo S_4 l'unico sottogruppo transitivo di S_4 che ha sottogruppi normali di indice 6.
- $|G/(G \cap V)| = 1$. Allora $G = V$, essendo V l'unico sottogruppo transitivo di S_4 contenuto in V, ed essendo $G \subseteq V$.
- $|G/(G \cap V)| = 2$. Allora se $|G \cap V| = 2$ allora $G \cong C_4$, se $|G \cap V| = 4$ allora $G \cong D_4$. Infatti C_4 e D_4 sono gli unici sottogruppi transitivi di S_4 che contengono un sottogruppo normale di indice 2 contenuto in V. Inoltre $G \cap V \cong \mathcal{G}(M/K(\alpha, \beta, \gamma))$, quindi:
  - $G \cong D_4$ se e solo se $G \cap V = V$ (essendo $V \leq D_4$), se e solo se $f(x)$ è irriducibile in $K(\alpha, \beta, \gamma)[X]$ (essendo V l'unico sottogruppo di V transitivo sugli zeri di $f(x)$).
  - $G \cong C_4$ se e solo se $|G \cap V| = 2$, se e solo se $f(x)$ è riducibile in $K(\alpha, \beta, \gamma)[X]$.

Esempio: Sia $f(x) := x^4 - 4x + 2 \in \mathbb{Q}[X]$. Per il criterio di Eisenstein, $f(x)$ è irriducibile in $\mathbb{Q}[X]$, quindi separabile. La risolvente cubica è $x^3 - 8x - 16$, irriducibile, e il suo discriminante è $-4(-8)^3 - 27(-16)^2 < 0$. Quindi il gruppo di Galois della risolvente cubica è S_3 e quindi $G/(G \cap V) \cong S_3$ e $|G/(G \cap V)| = 6$. Quindi $G \cong S_4$.

Esempio: Sia $f(x) := x^4 + 4x + 2 \in \mathbb{Q}[X]$. $f(x)$ è irriducibile per il criterio di Eisenstein, ed è quindi separabile. La risolvente cubica è $x^3 - 4x^2 - 8x + 32 = (x - 4)(x^2 - 8)$. Ne segue che $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{2})$. Il grado di $\mathbb{Q}(\alpha, \beta, \gamma)$ su $\mathbb{Q}$ è 2, quindi $|G/(G \cap V)| = 2$. $f(x)$ è riducibile su $\mathbb{Q}(\sqrt{2})$ perché $f(x) = (x^2 + 2 - \sqrt{2})(x^2 + 2 + \sqrt{2})$, di conseguenza $G \cong C_4$.

ESEMPIO: Sia $f(x) := x^4 - 10x^2 + 4 \in \mathbb{Q}[X]$, irriducibile perché non ha zeri in $\mathbb{Z}$ e non è prodotto di due polinomi di secondo grado in $\mathbb{Z}[X]$ (la verifica è diretta, facendo i conti). La risolvente cubica si fattorizza come $(x-4)(x+4)(x+10)$. Quindi $|G/(G \cap V)| = 1$ e quindi $G = V$.

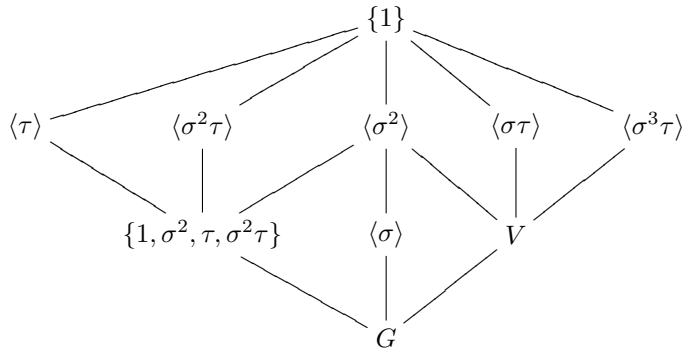
ESEMPIO: Sia $f(x) := x^4 - 2 \in \mathbb{Q}[X]$, irriducibile per il criterio di Eisenstein quindi separabile. La risolvente cubica è $x^3 + 8x$, e una fattorizzazione dimostra che $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(i\sqrt{2})$. Di conseguenza $[\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}] = 2 = |G/(G \cap V)|$. Una fattorizzazione in $\mathbb{R}[X]$ di $f(x)$ mostra che $f(x)$ è irriducibile in $\mathbb{Q}(i\sqrt{2})[X]$, quindi $G \cong D_4$. Sia M un c.r.c. per $f(x)$ su $\mathbb{Q}$, diciamo $M = \mathbb{Q}(u_1, u_2, u_3, u_4)$ dove gli u_i sono gli zeri di $f(x)$ in M. Detto $u := \sqrt[4]{2}$, possiamo porre $u_1 = u$, $u_2 = -u$, $u_3 = iu$, $u_4 = -iu$, essendo i una radice primitiva quarta dell'unità. M è un c.r.c. su $\mathbb{Q}$, quindi è stabile nell'estensione $\mathbb{C}/\mathbb{Q}$. Di conseguenza il coniugio di $\mathbb{C}$ ristretto a M è un $\mathbb{Q}$-automorfismo di M, e corrisponde alla trasposizione $\tau := (3\ 4)$. Ora, l'unico sottogruppo di S_4 ciclico che viene normalizzato da τ è quello generato da $\sigma := (1\ 3\ 2\ 4)$. Ne segue che

$$G = \langle (1\ 3\ 2\ 4),\ (3\ 4) \rangle$$

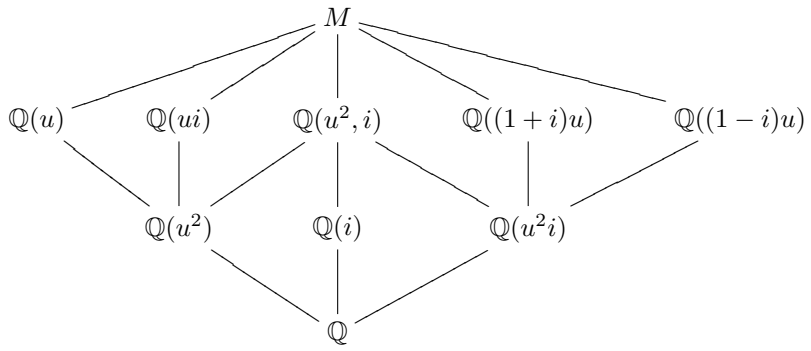
Inoltre è immediato che $M = \mathbb{Q}(u, i)$. Abbiamo la seguente tabella:

$\circ$	1	τ	σ	σ^2	σ^3	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
u	u	u	ui	$-u$	$-ui$	ui	$-u$	$-ui$
i	i	$-i$	i	i	i	$-i$	$-i$	$-i$

Il reticolo dei sottogruppi di G è il seguente:



Il reticolo degli intercampi di $M/\mathbb{Q}$ è il seguente:



22. Il teorema fondamentale dell'algebra

Ricordiamo la definizione di campo algebricamente chiuso.

DEFINIZIONE 66 (Campo algebricamente chiuso). *Un campo F si dice algebricamente chiuso se verifica una delle seguenti condizioni equivalenti.*

- *Ogni polinomio irriducibile di $F[X]$ ha grado 1.*
- *Ogni polinomio di grado positivo di $F[X]$ si fattorizza in $F[X]$ in fattori lineari.*
- *Se L/F è un'estensione algebrica di F allora $L = F$. In altre parole F è privo di estensioni algebriche proprie.*

Osserviamo che se F è un campo algebricamente chiuso e $K \leq F$ allora l'insieme degli elementi di F algebrici su K (la "chiusura algebrica relativa" di K in F) costituiscono un campo algebricamente chiuso.

ESEMPIO: L'insieme degli elementi di $\mathbb{C}$ algebrici su $\mathbb{Q}$ costituiscono un campo algebricamente chiuso.

DEFINIZIONE 67 (Chiusura algebrica). *Una chiusura algebrica di un campo K è un'estensione M/K con M algebricamente chiuso.*

TEOREMA 39 (Teorema fondamentale dell'algebra). *Il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso.*

DIMOSTRAZIONE. Malgrado il nome, non esistono dimostrazioni puramente algebriche. In questa dimostrazione faremo uso dei seguenti due fatti dimostrabili agevolmente in analisi usando il teorema del valor medio.

- Ogni numero reale non negativo ammette una radice quadrata in $\mathbb{R}$.
- Ogni polinomio di $\mathbb{R}[X]$ di grado dispari ammette uno zero reale.

Dal secondo punto segue che $\mathbb{R}$ non ammette estensioni di grado dispari, poiché una tale estensione dovrebbe essere semplice (per il teorema dell'elemento primitivo) e quindi corrisponderebbe ad un polinomio irriducibile di grado dispari.

Osserviamo innanzitutto che $\mathbb{C}$ non ha estensioni di grado 2, perché in $\mathbb{C}$ ogni elemento è un quadrato: questo è facilmente deducibile dal fatto che ogni reale non negativo è un quadrato in $\mathbb{R}$.

Osserviamo che dato $f(x) \in \mathbb{C}[X]$, $f(x)$ ammette una radice in $\mathbb{C}$ se e solo se il suo polinomio coniugato $\overline{f}(x)$ ammette una radice in $\mathbb{C}$ (la radice originaria coniugata). Quindi se troviamo uno zero del prodotto $f(x)\overline{f}(x)$ allora lui o il suo coniugato è uno zero di $f(x)$. Siccome $f(x)\overline{f}(x) \in \mathbb{R}[X]$, siamo ridotti a mostrare che ogni polinomio reale ammette uno zero in $\mathbb{C}$.

Per concludere basta quindi mostrare che ogni estensione M di $\mathbb{C}$ che sia un'estensione di Galois di $\mathbb{R}$ ha grado 1 su $\mathbb{C}$. Sia $G := \mathcal{G}(M/\mathbb{R})$, e l'ordine di G sia $2^e \cdot m$, con m dispari. Sia H un 2-sottogruppo di Sylow di G. Allora $[G : H] = m$, ovvero $[H' : \mathbb{R}] = m$, quindi $H'/\mathbb{R}$ ha grado dispari, e quindi $H' = \mathbb{R}$, cioè $m = 1$. Segue che $|G| = 2^e$ e G è un 2-gruppo. Se $e > 1$ allora $\mathcal{G}(M/\mathbb{C})$ è un gruppo di ordine 2^{e-1} e ammette un sottogruppo L di indice 2 (ogni p-gruppo finito ammette un sottogruppo di indice p: si vedano gli esercizi sui gruppi), quindi L' è un'estensione di $\mathbb{C}$ di grado 2, assurdo. Quindi $e = 1$, ovvero $M = \mathbb{C}$. □

23. Risolubilità per radicali

Problema: dato un campo K, esiste una "formula esplicita" che involve solo operazioni di campo ed estrazioni di radici e che fornisce tutte le soluzioni di una arbitraria equazione polinomiale $f(x) = 0$, con $f(x) \in K[X]$?

Siano K un campo, F una sua estensione. Una **torre di radici** tra K e F è una sequenza finita di campi

$$K = K_0 \leq K_1 \leq ... \leq K_t = F$$

con $K_{i+1} = K_i(u_i)$ tale che ${u_i}^{n_i} \in K_i$ per qualche $n_i \in \mathbb{N} - \{0\}$ per ogni $i = 0, ..., t-1$.

Un'**estensione** F/K si dice **radicale** se esiste una torre di radici tra K e F.

Dato $f(x) \in K[X]$ di grado positivo, l'**equazione** $f(x) = 0$ si dice **risolubile per radicali** se esistono $K \leq E \leq F$ tali che F/K sia radicale ed E sia c.r.c. per $f(x)$ su K.

LEMMA 31. *Se L/K è finita e separabile e M è chiusura split per L su K allora M è generato dai $\sigma(L)$ al variare di σ in $\mathcal{G}(M/K) = G$.*

DIMOSTRAZIONE. Poiché L/K è finita e separabile, M/K è di Galois essendo c.r.c. su L di un polinomio irriducibile di $K[X]$. Ne segue che il sottocampo di M generato dai $\sigma(L)$ al variare di σ in G, chiamiamolo S, essendo stabile in M/K è tale che S/K sia di Galois. Quindi S è c.r.c. su K di un polinomio a fattori irriducibili separabili. In particolare S è c.r.c. su K, quindi su L, quindi $S = M$ per minimalità di M. □

Nel seguito faremo uso dei risultati elencati nella seguente proposizione.

PROPOSIZIONE 39. *Sia F/K una estensione di campi.*

1. *Se F/K è radicale e $K \leq L \leq F$ allora F/L è radicale.*
2. *Se F/K è radicale allora è finita e quindi algebrica.*
3. *Se F_1, F_2 sono intercampi di un'estensione M/K e F_1/K, F_2/K sono radicali allora $(F_1 \cup F_2)/K$ è radicale.*
4. *Se F/K è radicale e separabile e N è una chiusura split di F su K allora N/K è radicale.*

DIMOSTRAZIONE.

(1) Se
$$K = K_0 \leq K_0(u_0) \leq K_0(u_0, u_1) \leq ... \leq K_0(u_0, ..., u_t) = F$$
è una torre di radici tra K e F allora
$$L = L_0 \leq L_0(u_0) \leq L_0(u_0, u_1) \leq ... \leq L_0(u_0, ..., u_t) = F$$
è una torre di radici tra L e F.

(2) Se
$$K = K_0 \leq K_0(u_0) \leq K_0(u_0, u_1) \leq ... \leq K_0(u_0, ..., u_t) = F$$
è una torre di radici tra K e F con ${u_i}^{n_i} \in K_i$ per qualche $n_i \in \mathbb{N}^*$ per $i = 0, ..., t-1$, $[K(u_0, ..., u_k) : K(u_0, ..., u_{k-1}] \leq n_k$ quindi $[F : K] \leq n_0 ... n_{t-1}$.

(3) Basta aggiungere in sequenza le radici di F_1/K seguite dalle radici di F_2/K.

(4) Per il lemma 31 e per il punto precedente basta mostrare che se $\sigma \in \mathcal{G}(N/K)$ l'estensione $\sigma(F)/K$ è radicale. Questo è immediato.

□

Ora capiremo lo stretto legame che c'è tra estensioni radicali e gruppi risolubili. Prima due lemmi.

LEMMA 32. *Siano F/K un'estensione di campi, $K \leq L \leq F$ un c.r.c. su K e $G := \mathcal{G}(L/K)$. Allora L è stabile in F/K. Sia M un c.r.c. su K e sia U l'insieme degli zeri di $x^n - 1$, dato $n \in \mathbb{N} - \{0\}$. Allora $\mathcal{G}(M/K)$ è risolubile se e solo se $\mathcal{G}(M(U)/K(U))$ è risolubile.*

DIMOSTRAZIONE. La prima asserzione segue dal fatto che L è generato su K dagli zeri di un polinomio a coefficienti in K. Proviamo la seconda. Poniamo $\mathcal{G}(M(U)/K(U)) = T \leq R = \mathcal{G}(M(U)/K)$.

Necessità. $G := \mathcal{G}(M/K)$ sia risolubile. Consideriamo la restrizione a M, $\varphi : T \to G$. Si tratta di un ben definito omomorfismo iniettivo di gruppi. Quindi T è risolubile, essendo isomorfo ad un sottogruppo di G che è risolubile.

Sufficienza. $\mathcal{G}(M(U)/K(U))$ sia risolubile. $K(U)$ è stabile in $M(U)/K$, essendo c.r.c. su K, quindi $T = K(U)'$ è un sottogruppo normale di R. Sia $\varphi : R \to \mathcal{G}(K(U)/K)$ la restrizione a $K(U)$. Come prima, φ è un omomorfismo, e stavolta è suriettivo in quanto $M(U)$ è c.r.c. su $K(U)$ di un polinomio a coefficienti in K, quindi ogni $\beta \in \mathcal{G}(K(U)/K)$ si estende a $M(U)$. Inoltre $\ker(\varphi) = T$, quindi $R/T \cong \mathcal{G}(K(U)/K)$, che è abeliano perché è il gruppo di Galois di un'estensione ciclotomica. Segue che R è risolubile, in quanto T e R/T lo sono. Ora la restrizione a M da R a $\mathcal{G}(M/K)$ definisce un isomorfismo $R/M' \cong \mathcal{G}(M/K)$, quindi $\mathcal{G}(M/K)$ è risolubile. □

LEMMA 33. *Sia M/K un'estensione radicale con M c.r.c. su K. Allora $\mathcal{G}(M/K)$ è risolubile.*

DIMOSTRAZIONE. Detti $n_1, ..., n_r$ gli interi che compaiono in una torre di radici tra K e M, detto $n := \prod_{i=1}^{r} n_i$, e detto U l'insieme degli zeri di $x^n - 1$, per il lemma 32 basta provare che $\mathcal{G}(M(U)/K(U))$ è risolubile. Possiamo quindi assumere che $U \subseteq K$. Siano $u_0, ..., u_{r-1}$ radici dell'estensione radicale M/K. Procediamo per induzione su r. Se $M = K(u_0)$ allora u_0 è zero di $x^n - {u_0}^n \in K[X]$ (si osservi che ${u_0}^n = ({u_0}^{n_0})^{n_1 \cdots n_{r-1}} \in K$), quindi $G := \mathcal{G}(M/K)$ è ciclico e quindi risolubile (si veda la proposizione 34).

Supponiamo ora $r > 1$. $N := \mathcal{G}(M/K(u_0)) = K(u_0)'$ è risolubile per ipotesi induttiva. $K(u_0)$ è c.r.c. su K di $x^n - {u_0}^n$, quindi è stabile in M/K e $N \trianglelefteq \mathcal{G}(M/K)$. Inoltre $G/N \cong \mathcal{G}(K(u_0)/K)$ è ciclico e quindi risolubile. Segue che N e G/N sono risolubili, quindi G è risolubile. □

TEOREMA 40. *Sia M/K un'estensione di campi separabile. Se $K \leq L \leq M$ e M/K è radicale allora $\mathcal{G}(L/K)$ è risolubile.*

DIMOSTRAZIONE. Poiché $\mathcal{G}(L/K) = \mathcal{G}(L/K'')$ e L/K'' è di Galois, possiamo assumere che l'estensione L/K sia di Galois. Inoltre se N è una chiusura split di M/K allora N/K è radicale (per la proposizione 39), quindi possiamo assumere che M sia un c.r.c. su K. Si osservi che poiché $\mathcal{G}(L/K) \cong \mathcal{G}(M/K)/L'$, per concludere basta mostrare che $\mathcal{G}(M/K)$ è risolubile. Questo segue dal lemma 33. □

Vediamo ora una sorta di viceversa del precedente teorema.

TEOREMA 41. *Sia M/K una estensione di Galois finita con $G := \mathcal{G}(M/K)$ risolubile, e la caratteristica di K non divida $|G|$. Allora esiste una estensione radicale F/K con $K \leq M \leq F$.*

DIMOSTRAZIONE. Sia $n := |G|$, e sia $N := K(U)$, dove U è l'insieme degli zeri di $x^n - 1$. Si osservi che per l'assunzione fatta sulla caratteristica il polnomio $x^n - 1$ è separabile. È immediato che N è estensione radicale di K (si prendano come radici gli elementi di U). Sia $F := M(N) = M(U)$. Basta provare che F/N è radicale, perché allora F/K è radicale perché lo sono F/N e N/K, e $K \leq M \leq F$. Poiché $x^n - 1$ è separabile l'estensione $M(N)/N$ è di Galois. Per il lemma 32 $\mathcal{G}(M(N)/N)$ si immerge in $\mathcal{G}(M/K)$ quindi è risolubile e il suo ordine divide n. Segue che la caratteristica di N (uguale alla caratteristica di K) non divide $|\mathcal{G}(M(N)/N)|$. Siamo quindi ricondotti al caso in cui $U \subseteq K$, cioè $N = K$ e $F = M$.

Essendo G un gruppo risolubile finito ammette una serie a fattori ciclici,

$$G = G_1 \trianglerighteq G_2 \trianglerighteq ... \trianglerighteq G_m = \{1_G\}.$$

Passando ai corrispondenti intercampi,

$$K = K_1 < K_2 < ... < K_m = M,$$

ove $K_i' = G_i$, $G_i' = K_i$ per $i = 1, ..., m$. La normalità dei sottogruppi implica la stabilità dei corrispondenti intercampi, quindi poiché M/K è di Galois K_{i+1}/K_i è di Galois e $[K_{i+1} : K_i] = |G_i : G_{i+1}| = n_i$ per ogni $i = 1, ..., m-1$. Per mostrare che la serie ottenuta è una torre di radici basta applicare il teorema 38 alle estensioni K_{i+1}/K_i. □

Osserviamo che la tesi del teorema vale in caratteristica zero. Se K ha caratteristica positiva il problema è l'esistenza di c.r.c. di polinomi del tipo $x^p - x - a \in K[X]$. Più precisamente:

PROPOSIZIONE 40. *Sia M/K un'estensione di Galois finita con gruppo di Galois risolubile. Allora esistono un'estensione F/M e una catena di campi*

$$K = K_0 \leq K_1 \leq ... \leq K_t = F$$

con $K_{i+1} = K_i(u_i)$, ${u_i}^{n_i} \in K_i$ per un opportuno n_i oppure u_i è zero di $x^p - x - a_i \in K[X]$ per un opportuno a_i, tutto ciò per ogni $i = 0, ..., t-1$.

DIMOSTRAZIONE. Posposta. □

Ricordiamo che dati un campo K e un polinomio $f(x) \in K[X]$ il gruppo di Galois di $f(x)$ è il gruppo di Galois di un c.r.c. M per $f(x)$ su K. Sia $n := \deg(f(x)) > 0$. Poiché il grado di M su K divide $n!$ (cf. il teorema 15), per i teoremi 40 e 41 se la caratteristica di K non divide $n!$ l'equazione $f(x) = 0$ è risolubile per radicali se e solo se il gruppo di Galois di $f(x)$ è risolubile.

Vediamo un esempio di applicazione. Nel seguito per un polinomio $f(x)$ indichiamo il gruppo di Galois di $f(x)$ con $\mathcal{G}_f$.

PROPOSIZIONE 41. *Sia $f(x)$ un polinomio irriducibile di $\mathbb{Q}[X]$ di grado primo p, e $f(x)$ abbia esattamente due zeri non reali. Allora $\mathcal{G}_f \cong S_p$.*

In particolare siccome S_n è non risolubile per ogni $n \geq 5$ (contenendo il gruppo semplice non abeliano A_n), ogni polinomio irriducibile di $\mathbb{Q}[X]$ di grado primo con esattamente due zeri non reali non è risolubile per radicali.

DIMOSTRAZIONE. Sia M un c.r.c. per $f(x)$ su $\mathbb{Q}$. Allora $M/\mathbb{Q}$ è di Galois perché K ha caratteristica zero, e $G := \mathcal{G}_f = \mathcal{G}(M/\mathbb{Q})$. $f(x)$ è separabile (siamo in caratteristica zero) e G agisce fedelmente sui p zeri di $f(x)$, quindi si immerge in S_p. Per la formula dei gradi se u è uno zero di $f(x)$ allora

$$[M : K] = [M : K(u)][K(u) : K] = [M : K(u)]p,$$

quindi $p = \deg(f(x))$ divide $|G|$. Allora G contiene un elemento di ordine p, cioè (identificando G a un sottogruppo di S_p) un p-ciclo.

Inoltre M è stabile nell'estensione $\mathbb{C}/\mathbb{Q}$, quindi il coniugio di $\mathbb{C}$ induce un automorfismo (diverso dall'identità, altrimenti $f(x)$ avrebbe solo zeri reali) di M, che corrisponde ad una trasposizione in S_p (ricordiamo infatti che gli zeri non reali di $f(x)$ sono solo due).

Segue che G visto come sottogruppo di S_p contiene un p-ciclo e una trasposizione. Non è difficile mostrare che il solo sottogruppo di S_p che contiene un p-ciclo e una trasposizione è S_p. Quindi $G = S_p$. □

ESERCIZIO 91. *Mostrare che i seguenti polinomi di $\mathbb{Q}[X]$ non sono risolubili per radicali:*

$$x^5 - 10x - 2, \qquad x^5 - 4x + 2, \qquad x^5 - 6x + 3.$$

Sia K un campo. Siano $t_1, ..., t_n$ indeterminate distinte simultanee su K, e sia

$$f(x) := x^n - t_1 x^{n-1} + t_2 x^{n-2} - ... + (-1)^n t_n.$$

L'equazione "$f(x) = 0$" si dice "**equazione generale di grado** n". Nel seguito mostreremo che $\mathcal{G}_f \cong S_n$ se $n \geq 5$, e che quindi se la caratteristica di K non divide $n!$ l'equazione generale di grado $n \geq 5$ non è risolubile (perché il gruppo S_n non è risolubile se $n \geq 5$).

Siano $x_1, ..., x_n$ indeterminate distinte su K, e siano $E := K(x_1, ..., x_n)$, $S := K(s_1, ..., s_n)$ dove $s_1, ..., s_n$ sono le funzioni simmetriche elementari. Ricordiamo che

$$g(x) := \prod_{i=1}^{n}(x - x_i) = x^n - s_1 x^{n-1} + ... + (-1)^n s_n.$$

E è c.r.c. su S per $g(x)$, E/S è di Galois e $\mathcal{G}(E/S) \cong S_n$, come già visto (teorema 30). Sia M un c.r.c. per $f(x)$ su $K(t_1, ..., t_n)$, e in $M[X]$ si abbia

$$f(x) := (x - y_1)...(x - y_n),$$

con $y_1, ..., y_n \in K(t_1, ..., t_n)$. Consideriamo i seguenti K-omomorfismi:

$$\sigma : K[t_1, ..., t_n] \to K[s_1, ..., s_n], \qquad t_i \mapsto s_i,$$

$$\tau : K[x_1, ..., x_n] \to K[y_1, ..., y_n], \qquad x_i \mapsto y_i.$$

Ora $t_1, ..., t_n$ non sono altro che le funzioni simmetriche elementari di $y_1, ..., y_n$, quindi $\tau \circ \sigma$ è l'identità su $K[t_1, ..., t_n]$. Segue che σ è iniettiva (se $\sigma(h) = 0$ allora $0 = \tau(\sigma(h)) = h$) ed è suriettiva per definizione, quindi σ è un isomorfismo e si estende ad un isomorfismo $K(t_1, ..., t_n) \to K(s_1, ..., s_n)$, e questo si estende ad un isomorfismo $\overline{\sigma} : K(t_1, ..., t_n)[X] \to K(s_1, ..., s_n)[X]$ (si osservi che esso manda $f(x)$ in $g(x)$), che si estende ad un isomorfismo $M \to E$ dei rispettivi c.r.c. (teorema 17). Dunque $\mathcal{G}_f \cong \mathcal{G}_g$. Dalla proposizione 21 segue allora il seguente teorema.

TEOREMA 42. *L'equazione generale di grado n su $K(t_1, ..., t_n)$ è irriducibile in $K(t_1, ..., t_n)[X]$ e ha radici distinte. Il suo gruppo di Galois è S_n.*

In particolare:

TEOREMA 43 (Abel-Ruffini). *L'equazione generale di grado n non è risolubile per radicali in caratteristica zero se $n \geq 5$.*

24. Costruibilità

Ricordiamo che un punto del piano si dice "costruibile (con riga e compasso)" se, fissata un'unità di misura, è possibile raggiungere tale punto dall'origine solo tracciando righe con un righello (senza misurazione) e circonferenze con un compasso. Si dimostra che, fissata l'unità di misura usuale sulla retta reale, un elemento di $\mathbb{C}$ è costruibile se e solo se esiste una catena finita di campi

$$\mathbb{Q} = F_0 \leq F_1 \leq F_2 \leq ... \leq F_n = F$$

tale che $[F_{i+1} : F_i] \leq 2$ per ogni $i = 1, ..., n-1$ e $z \in F$. Da questo si può dedurre che z è costruibile se e solo se esiste una torre di radici quadrate tra $\mathbb{Q}$ e un sovracampo contenente z.

PROPOSIZIONE 42. *$z \in \mathbb{C}$ è costruibile se e solo se z è algebrico su $\mathbb{Q}$ e la chiusura split L di $\mathbb{Q}[z]$ su $\mathbb{Q}$ ha come grado su $\mathbb{Q}$ una potenza di 2.*

DIMOSTRAZIONE. Necessità. $z \in \mathbb{C}$ sia costruibile. Allora esiste una torre di radici quadrate

$$\mathbb{Q} = F_0 \leq F_1 \leq ... \leq F_n = F \ni z,$$

quindi la chiusura normale E di F su $\mathbb{Q}$ è raggiungibile da $\mathbb{Q}$ mediante una torre di radici quadrate, e $[E : \mathbb{Q}]$ è una potenza di 2. Poiché $L \subseteq E$, anche $[L : \mathbb{Q}]$ è una potenza di 2.

Sufficienza. Valga $[L : \mathbb{Q}] = 2^r = |\mathcal{G}(L/K)|$. Se $r = 0$ allora $L = \mathbb{Q}$ quindi $z \in \mathbb{Q}$ è costruibile. Se $n \geq 1$ allora $G := \mathcal{G}(L/\mathbb{Q})$ è un 2-gruppo, quindi ha una serie a fattori di ordine 2, sia essa

$$G = G_0 \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_r = \{1\}.$$

Applicando le corrispondenze di Galois troviamo una torre di radici quadrate tra $\mathbb{Q}$ e L (cf. la proposizione 39). □

Non ogni elemento di grado una potenza di 2 è costruibile. Facciamo un esempio di un elemento di $\mathbb{C}$ di grado 4 su $\mathbb{Q}$ e non costruibile:

PROPOSIZIONE 43. *Ogni zero di $f(x) = x^4 - 4x + 2$ (irriducibile in $\mathbb{Q}[X]$) è un elemento di grado 4 non costruibile.*

DIMOSTRAZIONE. Che $f(x)$ sia irriducibile lo si vede direttamente scrivendo le candidate fattorizzazioni e uguagliando i coefficienti. Gli zeri di $f(x)$ hanno grado 4 su $\mathbb{Q}$, siano essi α_1, α_2, α_3, α_4. Due di essi sono reali e gli altri due no, diciamo che quelli reali sono α_1 e α_3, e diciamo che $\alpha_2 = \overline{\alpha_1}$ e $\alpha_4 = \overline{\alpha_3}$. Fattorizziamo $f(x)$ su $\mathbb{R}$: scriviamo

$$f(x) = (x^2 + ax + b)(x^2 + cx + d) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4).$$

Svolgendo i calcoli si ottiene $c = -a$, $b + d = a^2$, $a(d - b) = -4$ e $bd = 2$. Poiché $a = -(\alpha_1 + \alpha_2)$, $b = \alpha_1\alpha_2$, $c = -(\alpha_3 + \alpha_4)$ e $d = \alpha_3\alpha_4$, dalle relazioni scritte deduciamo che se un α_i è costruibile allora lo è anche il suo coniugato $\overline{\alpha_i}$, e quindi

lo sono anche a, b, c, d. Quindi se per assurdo un α_i è costruibile allora anche $t := b + d$ è costruibile. Ora,

$$t(t^2 - 8) = a^2((b + d)^2 - 8) = a^2((b + d)^2 - 4bd) = a^2(b - d)^2 = 16,$$

quindi t è zero del polinomio $x^3 - 8x - 16$, irriducibile su $\mathbb{Z}$, dunque su $\mathbb{Q}$. $b + d$ risulta essere un elemento costruibile di grado 3, assurdo (3 non è una potenza di 2). □

Osserviamo per la cronaca che $\mathcal{G}_{x^4-4x+2} \cong S_4$.

Occupiamoci ora dei poligoni regolari. L'n-agono regolare, il poligono regolare con n lati, non è altro che l'insieme degli zeri di $x^n - 1$ in $\mathbb{C}$, quindi siccome l'insieme degli elementi costruibili è chiuso per la moltiplicazione (è un campo) l'n-agono regolare è costruibile se e solo se le radici primitive n-esime di 1, cioè gli zeri del polinomio ciclotomico $\Phi_n(x)$, sono costruibili. Ora detta η una radice primitiva n-esima di 1, l'estensione $\mathbb{Q}(\eta)/\mathbb{Q}$ è di Galois di grado $\deg(\Phi_n(x)) = \varphi(n)$.

Ricordiamo che un numero primo si dice "**primo di Fermat**" se è della forma $2^t + 1$. Si osservi a questo proposito che se $2^t + 1$ è primo allora t è una potenza di 2.

TEOREMA 44. *Dato un intero positivo n, l'n-agono regolare è costruibile con riga e compasso se e solo se $n = 2^m p_1 p_2 ... p_t$, coi p_i primi di Fermat distinti e $m \in \mathbb{N}$.*

DIMOSTRAZIONE. Si tratta di trovare gli n per cui una radice primitiva n-esima di 1 (chiamiamola η) è costruibile, ovvero

$$\varphi(n) = [\mathbb{Q}(\eta) : \mathbb{Q}] = 2^l$$

per qualche $l \in \mathbb{N}$ (per la proposizione 42: si osservi che $\mathbb{Q}(\eta)/\mathbb{Q}$ è di Galois). Sia $n = {p_1}^{e_1} ... {p_r}^{e_r}$ la fattorizzazione in primi di n. Allora la richiesta diventa

$$(p_1 - 1){p_1}^{e_1 - 1} ... (p_r - 1){p_r}^{e_r - 1} = 2^l.$$

Questo succede se e solo se $p_i - 1 = 2^{t_i}$ per qualche $t_i \in \mathbb{N}$ per $i = 1, ..., r$, e $e_i \leq 1$ se $p_i \neq 2$. Ne segue quanto asserito. □

Per esempio il 7-agono regolare non è costruibile, mentre il 17-agono regolare è costruibile.

25. Altri risultati

Ricordiamo che un "**corpo**", o "**anello con divisione**", è un anello unitario A in cui ogni elemento a diverso da zero ammette inverso moltiplicativo, cioè un $b \in A$ tale che $ab = ba = 1$. Un campo non è altro che un corpo commutativo.

TEOREMA 45 (Wedderburn). *Ogni corpo finito è un campo.*

DIMOSTRAZIONE. Sia D un corpo finito, e sia

$$K := \{a \in D \mid ad = da \ \forall d \in D\} = Z(D)$$

il centro moltiplicativo di D. Allora $Z(D)$ è un campo finito, siano p la sua caratteristica e $q = p^l$ il suo ordine. D è spazio vettoriale su K con la moltiplicazione per scalare data dalla moltiplicazione in D, quindi $|D| = q^n$ dove $n = \dim_K(D)$. Per concludere basta mostrare che $K = D$, cioè $n = 1$. Se $a \in D$ allora $C_D(a) = \{d \in D \mid ad = da\}$ è un sottocorpo di D, D è spazio vettoriale su $C_D(a)$ e $C_D(a)$

è spazio vettoriale su K, quindi $|C_D(a)| = q^r$, $|D| = (q^r)^t = q^n$, da cui r divide n. Consideriamo i gruppi moltiplicativi finiti $D^* := D - \{0\}$ (di ordine $q^n - 1$), $C_D(a)^* = C_{D^*}(a) = C_D(a) - \{0\}$ (di ordine $q^r - 1$). D^* agisce su se stesso per coniugio, e per l'equazione delle classi

$$q^n - 1 = |D^*| = |K^*| + \sum_i |D^* : C_{D^*}(a_i)| = q - 1 + \sum_i (q^n - 1)/(q^{r_i} - 1),$$

dove gli a_i sono rappresentanti di classi di coniugio con più di un elemento, $|C_D(a_i)| = q^{r_i}$ e $1 \leq r_i < n$ divide n, per ogni i.

Sappiamo che $x^{r_i} - 1$ divide $x^n - 1$ per ogni i, scriviamo $x^n - 1 = l_i(x)(x^{r_i} - 1)$. Segue che $\Phi_n(x)$ (il polinomio ciclotomico n-esimo) divide ogni $l_i(x) = (x^n - 1)/(x^{r_i} - 1)$. Ma allora $\Phi_n(q)$ divide $q^n - 1$ e ogni $(q^n - 1)/(q^{r_i} - 1)$, e quindi dall'equazione delle classi che abbiamo esibito si ottiene che $\Phi_n(q)$ divide $q - 1$. È facile verificare che se η è radice primitiva n-esima di 1 allora $|q - \eta| \geq q - 1$, quindi siccome $\Phi_n(q) = \prod_\eta (q - \eta)$ si ottiene che $\Phi_n(q) = q - 1$, ovvero $n = 1$. □

Esistono invece corpi infiniti che non sono campi, per esempio il corpo dei quaternioni reali, lo spazio vettoriale Q di dimensione 4 su $\mathbb{R}$ con base $\{1, i, j, k\}$ e con la moltiplicazione definita da

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

CAPITOLO 4

Topologia, anelli e schemi affini

Indice analitico