Teoria di Galois
ad Interim

La jupe blanche
BALTHUS

Da dove viene e dove va questo testo. Essenzialmente, in un cestino. A parte gli scherzi: si tratta di niente più che dei soliti appunti generati dal bisogno, che non si meritavano (perché la materia è parecchio bella, perché spicca per simmetria: ma è talmente classica e meglio trattata altrove, che il ruolo di questa nota si può ridurre ad essere puntiforme ovunque fuori dal corso) di restare dei semplici manoscritti passati di mano in mano.

Ringrazio l'autore originale delle note, il gentile *Galuappunti*, precedentemente noto come *Bertappunti*; non sa che le ho volute riprodurre, se gli capiteranno in mano spero capisca che gli errori aggiuntivi sono tutti miei: ci ho messo parecchio a inventarmene di credibili!

Indice

1 Preliminari.

L'idea è studiare la sinergia tra

$$\left\{ \begin{array}{c}\text{zeri in } E \text{ di} \\ \text{polinomi in } F[X]\end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c}\text{estensioni di} \\ \text{campi } E|F\end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c}\text{automorfismi di} \\ E \text{ che fissano } F.\end{array} \right\} \tag{1}$$

1.1 Convenzioni.

Tutti gli anelli sono commutativi e il loro semigruppo moltiplicativo è unitario; gli omomorfismi di anelli rispettano tale identità (questo in generale non è vero; è vero se $\varphi\colon A \to B$ è non banale e B è integro, oppure se φ è suriettivo: $\varphi(1_A) \cdot z = \varphi(1_A) \cdot \varphi(x) = \varphi(1_A \cdot x) = \varphi(x) = z$ per ogni $z \in B$, dunque $\varphi(1_A) = 1_B$).

Definizione 1.1 : L'anello degli interi $\mathbb{Z}$ è l'oggetto iniziale della categoria **CRing**, dunque esiste un unico omomorfismo $\eta_R\colon \mathbb{Z} \to R$, per ogni anello commutativo. Se R è integro, $\ker \eta_R$ è un ideale primo di $\mathbb{Z}$. Ora possono accadere due cose

- $\ker \eta_R = (0)$, dunque dentro R c'è una copia di $\mathbb{Z}$;
- $\ker \eta_R = (p)$, dunque $\operatorname{im} \eta_R \cong \mathbb{Z}/p\mathbb{Z}$.

L'intero p che genera $\ker \eta_R$ si dice *caratteristica di* R. Se η_R è iniettivo si dice che R ha caratteristica zero.

Qualora il codominio di η_R sia un campo F, ed η_F è iniettiva, essa si estende in modo unico (per la proprietà universale del campo dei quozienti) ad un monomorfismo tra i rispettivi campi delle frazioni; in tal senso

> Ogni campo F di caratteristica zero è un'estensione di $\mathbb{Q}$.

Se η_F non è iniettiva, lo stesso ragionamento porta a dedurre che

> Ogni campo F di caratteristica p è un'estensione di $\mathbb{Z}/p\mathbb{Z}$.

1.2 Endomorfismo di Frobenius.

Sia A un anello commutativo di caratteristica $p > 0$. Definiamo l'endomorfismo di Frobenius $\pi\colon A \to A\colon a \to a^p$. Si osservi che

- Esso è davvero un endomorfismo, dato che $\operatorname{char} A = p$;
- Se A è integro, π è iniettivo;
- Se A è un insieme finito, è un campo finito, e π è un automorfismo;
- È possibile determinare i punti fissi di π?

Rispondiamo solo all'ultima domanda, ciò che resta è evidente. Ora, $x \in A$ è lasciato fisso da π se e solo se $a^p = a$, se e solo se $a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ (confondiamo, ora e sempre, $\mathbb{Z}/p\mathbb{Z}$ con la sua copia omormorfa in A; e chiramente lo zero è un punto fisso "banale"). Non vi sono altri punti fissi perché in un dominio di integrità un polinomio $p(X)$ ha al massimo $\deg p$ radici, e i $p-1$ elementi di $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ le esauriscono tutte).

Domanda. Se A è un campo infinito di caratteristica $p > 0$, il Frobenius deve essere suriettivo? In generale no: consideriamo $\mathbb{Z}/p\mathbb{Z}(X)$ e mostriamo che $\pi^{\leftarrow}(X) = \varnothing$. Per assurdo, se $\pi(f(X)/g(X)) = X$ dovrebbe essere $f(X)^p = g(X)^p X \in \mathbb{Z}/p\mathbb{Z}[X]$. Prendendo i gradi da ambo le parti, però si ha l'assurdo

$$p \deg f(X) = \deg(f(X)^p) = \deg(g(X)^p X) = p \deg(g(X)) + 1 \tag{2}$$

(a sinistra c'è un multiplo di p, a destra no). Questo è assurdo, dunque π non è suriettivo. □

Sia ora F un campo fissato, e $K|F$ una sua estensione. Definiamo il morfismo di *valutazione*

$$\sigma_u \colon F[X] \to K \colon f(X) \mapsto f(u) \tag{3}$$

per ogni $u \in K$. Si possono presentare due casi:

- σ_u è iniettivo; allora $u \in K$ si dice *trascendente* (su F);
- σ_u non è iniettivo, e $\ker \sigma_u$ è generato da un unico polinomio monico. In questo caso u si dice *algebrico* su F, e il generatore monico di $\ker \sigma_u$ si dice *polinomio minimo* di u su F e si indica con $\min_F(u)$.

Ora, ogni monomorfismo di anelli integri si estende, per funtorialità, ad un omomorfismo non banale tra i campi delle frazioni, dunque nel caso in cui u sia F-trascendente $\operatorname{im} \sigma_u \cong F(u) \cong F(X)$; nel caso in cui u sia F-algebrico il primo teorema di isomorfismo assicura che $F[u] \cong F[X]/(\min_F(u))$; d'altra parte ora la minimalità di $\min_F(u)$ implica che esso sia irriducibile, dunque l'ideale $(\min_F(u))$ è massimale, ergo $F[u] = F(u)$ è un campo. Si osservi che

$$|F(u) : F| = \deg(\min_F(u)) = n \tag{4}$$

Una base di $F(u)$ come F-spazio vettoriale è fatta da $\{1, u, u^2, \ldots, u^{n-1}\}$; u^n si scrive come una loro combinazione, e i combinatori sono esattamente i coefficienti di $\min_F(u)$.

2 Estensioni di omomorfismi.

Dato $\varphi \colon F \to \Omega$ morfismo di campi, e $\alpha \notin F$, ci potremmo chiedere quanti modi esistono di estendere φ ad $F(\alpha)$, ossia quanti $\overline{\varphi} \colon F(\alpha) \to \Omega$ esistono, tali che $\overline{\varphi} \circ \iota \colon F \hookrightarrow F(\alpha) \to \Omega$ coincida con φ.

È facile osservare che un tale $\overline{\varphi}$ è completamente determinato da $\overline{\varphi}(\alpha)$, dato che $\overline{\varphi}\big(\sum a_i\alpha^i\big) = \sum a_i\overline{\varphi}(\alpha)^i$.

Proposizione 2.1. Se α è F-trascendente, allora $\overline{\varphi}(\alpha)$ è F-trascendente.

Dimostrazione. Supponiamo per assurdo che $p(\overline{\varphi}(\alpha)) = 0$. Allora $0 = p(\overline{\varphi}(\alpha)) = \overline{\varphi}(p(\alpha))$, dunque $p(\alpha) = 0$ (ogni morfismo di campi non banale è iniettivo), d'altra parte abbiamo supposto α F-trascendente, assurdo. □

Proposizione 2.2. Se $\gamma \in \Omega$ è $\varphi(F)$-trascendente, esiste $\overline{\varphi}\colon F(\alpha) \to \Omega$ tale che $\overline{\varphi}(\alpha) = \gamma$.

Dimostrazione. La composizione dei tre isomorfismi

$$F[\alpha] \to F[X] \to \varphi(F)[X] \to \varphi(F)[\gamma] \tag{5}$$

ne dà uno $F[\alpha] \to \varphi(F)[\gamma]\colon \alpha \mapsto \gamma$. Dunque esiste un immersione $F[\alpha] \hookrightarrow \Omega$ *per ogni modo* di scegliere un elemento $\varphi(F)$-trascendente come immagine di α.

Se α è F-algebrico, $f = \min_F(\alpha)$, allora c'è un isomorfismo

$$F[X] \to \varphi(F)[X] \tag{6}$$

che chiamiamo ancor φ. Ora, $\varphi(f)$ è irriducibile su $\varphi(F)$, perché f lo era su F; è facile osservare che ogni $\overline{\varphi}\colon F(\alpha) \to \Omega$ che estende φ deve mandare α in un'altra radice di $\varphi(f(X))$. Dunque se γ è zero di $\varphi(f(X))$ si hanno gli isomorfismi

$$F(\alpha) \cong \tfrac{F[X]}{(f(X))} \cong \tfrac{\varphi(F)[X]}{(\varphi(f))} \cong \varphi(F)(\gamma) \subset \Omega \tag{7}$$

e dunque ancora un monomorfismo $F(\alpha) \hookrightarrow \Omega$. In conclusione, se α è F-algebrico, φ si estende ad $F(\alpha) \hookrightarrow \Omega$ in tanti modi quanti sono gli zeri *distinti* di $\min_F(\alpha)$. □

Abbiamo stabilito, in sintesi, delle biiezioni

$$\left\{ \begin{smallmatrix}\text{estensioni di } \varphi \\ \text{a } \overline{\varphi}\colon F(\alpha)\to\Omega\end{smallmatrix} \right\} \longleftrightarrow \left\{ \begin{smallmatrix}\gamma\in\Omega \\ F\text{-trascendenti}\end{smallmatrix} \right\} \tag{8}$$

$$\left\{ \begin{smallmatrix}\text{estensioni di } \varphi \\ \text{a } \overline{\varphi}\colon F(\alpha)\to\Omega\end{smallmatrix} \right\} \longleftrightarrow \left\{ \begin{smallmatrix}\gamma\in\Omega \\ \text{zeri di} \varphi(\min_F(\alpha))\end{smallmatrix} \right\} \tag{9}$$

a seconda che α sia F-trascendente o F-algebrico.

Osservazione 1. La risposta *dipende* da Ω: consideriamo $\alpha = \sqrt[3]{2}$, $F = \mathbb{Q}, \Omega = \mathbb{C}$. Allora il numero di estensioni di $\mathrm{id}_\mathbb{Q}$ a $\mathbb{Q}(\alpha) \to \mathbb{C}$ è 3, e precisamente l'identità, $\alpha \mapsto \omega\alpha, \omega \mapsto \omega^2\alpha$, dove $\omega^3 = 1$ è una radice terza primitiva dell'unità.

Se però scegliamo $\Omega = \mathbb{R}$, otteniamo solo l'identità (l'unica radice di $\min_F(\alpha)$ *su* $\mathbb{R}$ è α).

Esercizio 1. Ogni morfismo di anelli $\mathbb{Q} \to F$, dove F è un campo di caratteristica zero, coincide con l'inclusione insiemistica. In particolare $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}) \cong 1$. Allo stesso modo ogni morfismo di anelli $\mathbb{Z}/p\mathbb{Z} \to F$, con F campo di caratteristica p, coincide con l'inclusione insiemistica. In particolare $\mathrm{Aut}_{\mathbb{Z}/p\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) \cong 1$

Non esistono morfismi diversi da quello nullo, tra campi di caratteristiche differenti[1].

Questa la parte facile. Ora ci facciamo la stessa domanda rispetto ad $\mathbb{R}$, riguardato come estensione di $\mathbb{Q}$ (si può vedere come completamento alla Cauchy rispetto alla norma euclidea, nell'ambito della teoria dei completamenti di campi ordinati).

Supponiamo allora di avere $\sigma \in \mathrm{Aut}(\mathbb{R})$ tale che $\mathbb{Q} \hookrightarrow \mathbb{R} \xrightarrow{\sigma} \mathbb{R}$ coincide con l'inclusione $\mathbb{Q} \hookrightarrow \mathbb{R}$. Si osservi che

- σ *deve essere monotona*; perché ogni $\alpha \in \mathbb{R}_{>}$ è un quadrato in $\mathbb{R}$, dunque $\sigma(\alpha) = \sigma(a)^2 > 0$ (perché in un campo ordinato i quadrati sono positivi).
- σ *è continua nella topologia euclidea*; perché lo è ogni funzione monotona $\mathbb{R} \to \mathbb{R}$ ($\sigma^{\leftarrow}(]a,b[) =]\sigma^{\leftarrow}(a), \sigma^{\leftarrow}(b)[$).
- σ *è l'identità*; perché ogni $x \in \mathbb{R}$ si scrive come limite di una successione di razionali:

$$\sigma(x) = \sigma\left(\lim_{n\to\infty} q_n\right) = \lim_{n\to\infty} \sigma(q_n) = \lim_{n\to\infty} q_n = x.$$

2.1 Campi di spezzamento.

Definizione 2.1 : Sia $f \in F[X]$, $E|F$ una estensione. E si dice *campo di spezzamento* di $f(X)$ se

- f si spezza in un prodotto di fattori lineari in $E[X]$;
- $E \cong F(\alpha_1, \ldots, \alpha_n)$, se $f(X) = c(X - \alpha_1)\ldots(X - \alpha_n)$.

Proposizione 2.3. Se $f(X) \in F[X]$, con $\deg f > 0$, allora esiste $K|F$, $K \cong F(\alpha)$, con α radice di f.

Dimostrazione. Sia g un fattore irriducibile di f in $F[X]$. L'anello $K = F[X]/(g)$ è un campo, e $\alpha = X + (g(X))$ ha le proprietà richieste: se indichiamo con $\overline{f}$ l'immagine di f mediante $F[X] \to K[X]$ otteniamo

$$\overline{f}(\alpha) = g(X)h(X) + (g) \equiv 0 \pmod{g(X)}. \tag{10}$$

□

Proposizione 2.4. Sia $f(X) \in F[X]$, $\deg f = n > 0$. Allora esiste un campo di spezzamento $E|F$ per $f(X)$, il cui grado divide $n!$.

[1] Supponiamo che esista $f\colon F \to E$, con $\mathrm{char}\, F = p \neq q = \mathrm{char}\, E$. Allora per unicità $f \circ \eta_F = \eta_E$, ma allora $\eta_E(p) = f(\eta_F(p)) = 0$, dunque $p \in q\mathbb{Z}$, dunque $q \mid p$, assurdo.

Dimostrazione. Se $f(X)$ è irriducibile su F, ragioniamo per induzione su n. La base è banalmente vera, al grado 1, scegliendo $E = F$. Per il risultato precedente poi esiste un'estensione dove $f(X) = (X - \alpha)g(X)$, e $\deg g = n - 1$. Allora per ipotesi induttiva, esiste $E_g|F(\alpha)$ dove $g(X)$ spezza linearmente, e $|E_g : F(\alpha)|$ divide $(n-1)!$. Per la formula dei gradi, ora,

$$|E : F| = |E_g : F(\alpha)||F(\alpha) : F| \tag{11}$$

divide $(n-1)!n = n!$

Resta da vedere che $E = \text{Split}_F(f(X))$: questo però è banale alla luce del fatto che $f = (X-\alpha)g(X) = c(X-\alpha)(X-\epsilon_1)\dots(X-\epsilon_{n-1})$ in E_g.

Supponiamo ora che $f(X)$ sia riducibile. Allora $f = gh$, con $\deg g = r, \deg h = s$. Se $L = \text{Split}_F(g(X))$, $E = \text{Split}_L(h(X))$ (esistono per induzione); in $E[X]$ $f(X)$ si spezza in fattori lineari, ed $E = F(\alpha_1, \dots, \alpha_n)$; per la formula dei gradi, se $|E : L|$ divide $s!$, $|L : F|$ divide $r!$, allora $|E : F|$ divide $r!s!$, che d'altra parte divide $n!$ (perché $\frac{n!}{r!s!} = \frac{(r+s)!}{r!s!} = \binom{n}{r}$ è intero). □

Esempio 2.1 : Siano F un campo e p un primo, determiniamo $E = \text{Split}_F(X^p - 1)$. Anzitutto, se definiamo $U = \{z \in E \mid z^p = 1\}$ è chiaro che $|U| \leq p$ (è il teorema di Ruffini, se R è un anello integro, $p(X) \in R[X]$ ha al pù $\deg p$ zeri). Ci sono solo due casi

- $U = 1$ è il gruppo banale;
- $U = C_p$ è il ciclico con p elementi.

Non vi sono altri casi perché se esiste $\bar{z}$ tale che $\bar{z}^p = 1$ ma di ordine minore di p, tale ordine deve dividere p, dunque $\bar{z} = 1$.

La morale di questo esempio è che aggiungendo ad F qualsiasi $z \in U \setminus \{1\}$ ottengo tutto E.

Dividiamo la discussione in due casi. Anzitutto, se $\text{char}\, F = p$, per Frobenius

$$X^p - 1 = (X-1)^p \tag{12}$$

dunque $U = 1$ ed $E = F$. Viceversa, se supponiamo che $X^p - 1$ abbia come unica soluzione 1, uguagliando i coefficienti in $X^p - 1 = (X-1)^p$ si ottiene che $p \cdot 1 = 0$, e dunque $\text{char}\, F \mid p$. A questo punto però, p essendo primo, si conclude che $\text{char}\, F = p$. Si è dunque provato che $U = 1 \iff \text{char}\, F = p$.

Supponiamo ora che $\text{char}\, F \neq p$ (zero o un primo differente). Allora per quanto detto prima $U \cong C_p$ e $E \cong F(\zeta)$ dove ζ è qualsiasi elemento di $U \setminus \{1\}$.

Esempio 2.2 : Determiniamo $E = \text{Split}_F(X^p - X - t)$, se F è un generico campo di caratteristica p.

Si osservi che se $f(a) = 0$, allora $f(a+k) = 0$ per ogni $k \in \mathbb{Z}/p\mathbb{Z}$ (si usa Frobenius).

Dunque se conosciamo uno zero li conosciamo tutti (e sappiamo che sono tutti distinti); perciò $E \cong F(a)$.

Ovviamente se $a \in F$, $\text{Split}_F(f(X)) = F$, e altrimenti $|\text{Split}_F(f(X)) : F| = p$, dato che $\deg f(X) = p$ (va mostrato che $f(X)$ è irriducibile per dirlo: supponiamo che $f = gh$ con fattori non banali: allora in $E[X]$ si ha $f(X) = \prod_{k\in\mathbb{Z}_p}(X - (a + k))$, e allora g si ottiene prendendo solo alcuni di questi fattori lineari: $g(X) = (X - (a + k_1)) \dots (X - (a + k_r))$ per certi $k_i \in \mathbb{Z}/p\mathbb{Z}$). Ora, $g(X) = X^r - \big(\sum(a + k_i)\big)X^{r-1} + \dots = X^r + \big(ra + \sum k_i\big)X^{r-1} + \dots$

A questo punto $ra + \sum k_i \in F$, e $\sum k_i \in F$ implica che $ra \in F$, e siccome $r < p$, r ammette un inverso in $\mathbb{Z}/p\mathbb{Z}$; ma allora $r^{-1}ra = a \in F$, assurdo.

Dunque una qualsiasi radice di $f(X)$ genera il suo campo di spezzamento.

Teorema 2.1 : Sia $f(X) \in F[X]$, $E|F$ una estensione generata da zeri di f (non necessariamente *tutti*), e $\Omega|F$ una estensione in cui $f(X)$ si spezza in fattori lineari. Allora

- Esistono $\varphi\colon E \to \Omega$ che fissano F (ossia $\varphi|_F = \text{id}_F$);
- Detto H l'insieme di tali estensioni, $\#H \leq |E : F|$;
- La disuguaglianza sopra è un'uguaglianza se $f(X)$ non ha radici ripetute in Ω;
- Se E, E' sono campi di spezzamento per $f(X)$, tutti i φ del punto (i) sono isomorfismi che fissato F.

Corollario. $\text{Split}_F(f(X))$ non è un oggetto universale, perché non è unico a meno di un *unico* isomorfismo di campi.

Dimostrazione. Sia $E = F(a_1, \dots, a_r)$. Sia $g_1(X) = \min_F(a_1)$; chiaramente $g_1 \mid f$: allora si può mandare a_1 in un altro zero di questo polinomio, in al più $\deg g_1$ modi (l'uguaglianza vale sse non ha radici ripetute). Inducendo facilmente sul numero di fattori irriducibili in cui $f(X)$ si spezza si ottengono i primi tre punti.

Dimostriamo l'ultimo punto. In base ad (1), esiste $\varphi\colon E \to \Omega$ che fissa F, e per ogni $K|F$ ogni $\sigma\colon K \to L$ che fissa F è un omomorfismo di F spazi vettoriali (iniettivo non appena è non banale). Allora

$$|E : F| = |\varphi(E) : F| \leq |\Omega : F| \tag{13}$$

Ripetendo lo stesso ragionamento, scambiati i ruoli di Ω, E (se entrambi sono campi di spezzamento questo si può fare) si ottiene che

$$|\Omega : F| = |E : F| \tag{14}$$

dunque Ω, E sono spazi vettoriali della stessa dimensione. Ma φ è un mono tra loro, si conclude. □

Corollario. Sia $E|F$ una estensione finita, ed $L|F$ un'altra estensione. Allora $|\hom_F(E,L)| \leq |E:F|$ (può anche essere zero).

Dimostrazione. Se E ha grado finito, risulta $E \cong F(\beta_1,\ldots,\beta_n)$. Se ora $g_i = \min_F(\beta_i)$, e definiamo $f = \prod g_i \in F[X]$, $\Omega = \text{Split}_L(f)$, per il risultato precedente $|\hom_F(E,\Omega)| \leq |E:F|$, e ogni freccia $E \to L$ è anche una freccia $E \to \Omega$ (ovvio); allora

$$|\hom_F(E,L)| \leq |\hom_F(E,\Omega)| \leq |E:F|. \tag{15}$$

□

In conclusione, $|E:F|$ comanda il numero degli F-omomorfismi da E ad una *qualsiasi* estensione $L|F$.

Osservazione 2. Sia $\text{Aut}(K|L)$ l'insieme degli automorfismi di K che fissano L. Allora

$$|\text{Aut}(K|L)| \leq |K:L| \tag{16}$$

(Si deduce dal corollario precedente se $F = L$, $E = K$).

Corollario. Sia $E = \text{Split}_F(f(X))$, per $f(X) \in F[X]$. Allora $|\text{Aut}(E|F)| \leq |E:F|$, e vale l'uguaglianza se e solo se $f(X)$ non ha radici ripetute.

Esempio 2.3 : $\text{Aut}(\mathbb{C}|\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, generato dal coniugio.

Osservazione 3. Se $f \in F[X]$, $f = \prod g_i^{m_i}$ la sua fattorizzazione in irriducibili su F, allora $\text{Split}_F(f) = \text{Split}_F(f_{\text{red}})$, dove $f_{\text{red}} = \prod g_i$ (una inclusione è ovvia, l'altra segue dal fatto che ho comunque messo tutte le radici). Dunque quello che conta non è che f abbia radici semplici, ma che i suoi *fattori irriducibili* le abbiano.

3 Questioni di separabilità.

Uno si chiede quindi: fattori irriducibili distinti possono avere radici in comune? La risposta è no: supponiamo che g, h siano fattori irriducibili di f; allora se essi condividono una radice, diciamo α, $\min_F(\alpha)$ divide sia g che h. Questo però è assurdo (non sarebbero irriducibili).

Osservazione 4. Fattori irriducibili distinti di $f \in F[X]$ non hanno radici comuni, *in nessuna estensione* di F.

Definizione 3.1 : Un polinomio $f \in F[X]$ si dice *separabile* se ogni fattore irriducibile di f_{red} ha radici distinte.

Il corollario precedente si può allora rifrasare come

Corollario. Sia $E = \text{Split}_F(f(X))$, per $f(X) \in F[X]$. Allora $|\text{Aut}(E|F)| \leq |E:F|$, e vale l'uguaglianza se e solo se $f(X)$ è separabile.

Teorema 3.1 : Sia $f \in F[X]$ un polinomio irriducibile. Le seguenti affermazioni sono equivalenti.

- Esiste $K|F$ dove f ha uno zero multiplo;
- $(f, f') \neq c \in F \setminus \{0\}$;
- char $F = p > 0$, e $f \in F[X^p]$;
- tutti gli zeri di f in $\text{Split}_F(f)$ sono multipli.

Dimostrazione. Che $4 \Rightarrow 1$ è ovvio.

$1 \Rightarrow 2$. Se $f(X) = (X-a)^m g(X)$ in $K[X]$, per $m > 1$, facendo la derivata formale si ha $f'(X) = m(X-a)^{m-1}g(X) + (X-a)^m g'(X)$, dunque $(X-a)$ divide entrambi f, f', e ovviamente divide $\gcd(f, f')$.

Osservazione 5. Abbiamo fatto la derivata in $K[X]$, dunque a priori $\frac{f(X)}{X-a}, \frac{f'(X)}{X-a} \notin F[X]$. Ma abbiamo provato che irriducibili coprimi di f non hanno zeri comuni in nessuna estensione di F, dunque per la contronominale inversa (f, f') non può essere un invertibile, perché i due polinomi non sono coprimi (a è radice di entrambi).

$2 \Rightarrow 3$. Sia $d = (f, f')$ non costante in $F[X]$. Se f è irriducibile in $F[X]$, allora f, d sono associati.

Ora, $d \mid f' \Rightarrow f|f'$: se $f' \neq 0$, però, esso ha grado minore di $\deg f$ (per la precisione ha grado $\deg f - 1$). Questo è assurdo. Allora deve essere $f' = 0$, ma anche questo è assurdo in caratteristica zero, perché f non era un polinomio costante (il fatto che $f = \sum a_i X^i$ e $f' = \sum i a_i X^{i-1} = 0$, in caratteristica zero implica che $a_i = 0$ per ogni $i \geq 1$). Resta dunque l'unico caso in cu char $F = p > 0$, ed $f \in F[X^p]$, perché $ia_i = 0$ in caratteristica p implica che $a_i = 0$ per ogni i non multiplo di p: allora

$$f(X) = a_0 + a_p X^p + \cdots + a_{rp} X^{rp}. \tag{17}$$

$3 \Rightarrow 4$. Se $f = g(X^p)$, nel campo di spezzamento di g si ha

$$g(X) = (X - a_1)^{m_1} \dots (X - a_r)^{m_r} \tag{18}$$

$$f(X) = (X^p - a_1)^{m_1} \dots (X^p - a_r)^{m_r} \tag{19}$$

Le radici di f sono gli zeri di $X^p - a_i$, che in caratteristica p è un polinomio con una sola radice di molteplicità p (Frobenius). □

Osservazione 6. In un campo di caratteristica zero tutti i polinomi sono separabili.

Osservazione 7. Un polinomio si dice separabile se, ricordiamo, i suoi fattori irriducibili non hanno zeri ripetuti in un prescritto campo di spezzamento; tale campo va specificato, perché a priori i fattori irriducibili possono cambiare. D'altra parte questa imprecisione è innocua: se $f \in F[X]$ è separabile in $K|F$, è separabile anche in F, e viceversa.

Dimostrazione. Sia $\prod g_i(X)^{m_i} = g(X) \in F[X]$ irriducibile, con radici semplici in $K|F$; g_{red} ha fattori irriducibili che hanno tutti radici semplici, e non ne hanno di comuni in $\text{Split}_F(g)$. Dunque g è separabile anche in $K|F$. □

Teorema 3.2 : Un campo F si dice *perfetto* se ogni polinomio $f \in F[X]$ è separabile. Il campo F è separabile se e solo se, alternativamente

- ha caratteristica zero;
- ha caratteristica $p > 0$ ed $F = F^{\sqrt{p}} = \{\alpha \in F \mid \exists a : a^p = \alpha\}$.

Dimostrazione. Il primo caso è stato già provato. Per quanto riguarda il secondo, se $\text{char } F = p$ ed $F \supsetneq F^{\sqrt{p}}$ esiste $a \in F$ che non è una potenza p-esima. Allora $X^p - a$ non ha radici in $F[X]$; per Frobenius, ora, in $F(b)$, dove b è una radice p-esima di a, si ha $X^p - a = (X - b)^p$, dunque c'è solo una radice di molteplicità p; se dimostriamo che questo polinomio è irriducibile segue la tesi, perché F non è perfetto.

Supponiamo che $f = gh$, con $1 \leq \deg g < p$. Allora $g \mid X^p - a$, dunque $g = (X - b)^r$ in $F(b)$, per qualche $r < p$. Ora anche $b^p = a \in F$, dunque $b^r, b^p \in F$. Però adesso p è primo, dunque per Bézout esistono interi u, v tali che $ur + vp = 1$. Questo però è assurdo (implicherebbe $b = (b^r)^u (b^p)^v \in F$.

Supponiamo da ultimo $\text{char } F = p > 0$, ed $F = F^{\sqrt{p}}$. Sia $f \in F[X]$ con zeri multipli. Allora $f(X) = g(X^p)$ per qualche $g(X)$ non costante. Siccome poi $F = F^{\sqrt{p}}$ ogni coefficiente a_i di $g(X)$ si scrive come una potenza p-esima: allora

$$f(X) = a_0 + a_1 X^p + \cdots + a_r X^{rp} \tag{20}$$
$$= b_0^p + b_1^p X^p + \cdots + b_r^p X^{rp} \tag{21}$$
$$= (b_0 + b_1 X + \cdots + b_r X^r)^p \in F[X] \tag{22}$$

dunque f è riducibile in $F[X]$. □

Osservazione 8. I campi di caratteristica positiva perfetti sono tutti e soli quelli dove il Frobenius è un isomorfismo (ossia dove è suriettivo). In particolare tutti i campi finiti sono perfetti.

4 Corrispondenza di Galois.

4.1 La connessione di Galois tra campi e gruppi di F-automorfismi.

Sia $K|L$ un'estensione di campi. Definiamo $\Phi(K|L) = \{E \mid L \leq E \leq K\}$ l'insieme dei campi intermedi tra L e K, ossia l'insieme dei sottocampi di K che contengono L. Definiamo poi $\text{Aut}(K|L)$ come l'insieme di tutti gli automorfismi di K che sono l'identità ristretti ad L; sia infine $\mathfrak{S}(K|L)$ il

reticolo dei sottogruppi di $\mathrm{Aut}(K|L)$. $\Phi(K|L), \mathfrak{S}(K|L)$ sono ovviamente ordinati dall'inclusione insiemistica.

Definiamo le due corrispondenze

$$\begin{aligned} \varphi\colon \Phi(K|L) &\longrightarrow \mathfrak{S}(K|L) \\ E &\longmapsto \mathrm{Aut}(K|E), \\ \psi\colon \mathfrak{S}(K|L) &\longrightarrow \Phi(K|L) \\ G &\longmapsto \mathrm{Fix}(G), \end{aligned} \tag{23}$$

$\mathrm{Fix}(G)$ essendo l'insieme $\{a \in K \mid \sigma a = a \ \forall \sigma \in G\}$.

Osservazione 9. Si osservi che

- $\mathrm{Fix}(G)$ è un campo che contiene L (tutte le verifiche sono immediate);
- Se $L \leq E \leq E' \leq K$, allora $\varphi(E') \leq \varphi(E)$;
- Se $\langle 1 \rangle \leq G \leq H \leq \mathrm{Aut}(K|L)$ allora $\psi(H) \leq \psi(G)$.

Si noti anche che per definizioni

$$G \leq \varphi\psi(G) \tag{24}$$

$$E \leq \psi\varphi(E) \tag{25}$$

Alla luce di questo è immediato provare che

$$E \leq \psi(G) \iff G \leq \varphi(E) \tag{26}$$

e dunque che riguardando $\Phi(K|L), \mathfrak{S}(K|L)$ come categorie, φ, ψ sono funtori aggiunti (*connessioni di Galois*).

> Siamo interessati a studiare il caso in cui questa aggiunzione è un'equivalenza di categorie.

Il problema non è peregrino, dato che a volte questa aggiunzione non lo è:

Esempio 4.1 : Consideriamo l'estensione $E = \mathbb{Q}(\sqrt[4]{2})|\mathbb{Q} = F$. Il polinomio $\min_{\mathbb{Q}}(\sqrt[4]{2}) = X^4 - 2$ è irriducibile su $\mathbb{Z}[X]$ per il criterio di Eisenstein (esiste un primo che divide esattamente il termine noto, e nessun altro coefficiente: tale primo è chiaramente 2). Ora, da quanti e quali automorfismi di $\mathbb{Q}(\sqrt[4]{2})$ è fatto $\mathrm{Aut}(E|F)$? $\sqrt[4]{2}$ può essere mandato in $\pm\sqrt[4]{2}$ (non in $i\sqrt[4]{2}$, perché non stanno in E). In ambo i casi $\sqrt{2} = \left(\sqrt[4]{2}\right)^2$ viene mandato in sè stesso, dunque $\mathrm{Fix}(\mathrm{Aut}(E|F)) \supseteq \mathbb{Q}(\sqrt{2})$, e anzi vi coincide. Dunque $\mathrm{Fix}(\mathrm{Aut}(E|F)) \supsetneq \mathbb{Q}$.

Esempio 4.2 : Siano $F = \mathbb{Q}$, $\alpha = \sqrt[3]{5}$ ed $E = \mathbb{Q}(\alpha)$. $E|F$ ha grado primo, dunque non vi sono campi intermedi; $\#\Phi(E|F) = 2$, ma $\#\mathfrak{S}(E|F)$ è banale perché $\mathrm{Aut}(E|F) = \langle 1 \rangle$. Infatti ogni $\sigma\colon E \to E$ tale che $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ è tale che $\sigma(a + \alpha b) = a + \sigma(\alpha)b$. D'altra parte se $\sigma(\alpha) = -\alpha$, avremmo $-5 = \sigma(\alpha)^3 = \sigma(\alpha^3) = \sigma(5) = 5$, assurdo.

Esempio 4.3 : Se $\text{char}\, F = p > 0$ ed $F \supsetneq F^{\sqrt{p}}$ (quindi F non è perfetto) prendiamo $a \in F \setminus F^{\sqrt{p}}$. Allora $f(X) = X^p - a = (X-b)^p$. In $E = F(b)$ la radice p-esima di a può essere mandata solo in un'altra radice di $f(X)$, ossia solo in sè stessa.

La morale è che in generale $\text{Fix}(\text{Aut}(E|F)) \supsetneq F$, e le situazioni in cui questo si verifica avranno un nome speciale: i campi E estensioni di F tali che $\text{Fix}(\text{Aut}(E|F)) = F$ si diranno *estensioni di Galois* di F.

Definizione 4.1 : Sia $E|F$ una estensione di grado finito. E si dice *estensione di Galois* su F se $\text{Fix}(\text{Aut}(E|F)) = F$.

Osservazione 10. Se $E|F$ è di Galois la corrispondenza suddetta è una biiezione che rispetta indici e gradi, e i sottogruppi normali di $\text{Aut}(E|F)$ (che in questo caso si scrive $\text{Gal}(E|F)$ vanno in estensioni intermedie di F che sono ancora di Galois su F: da una parte non tutte lo sono; tra vediamo un controesempio, e dall'altra è facile dimostrare che se $E|F$ è di Galois e $K|F$, allora $E|K$ è di Galois).

Esempio 4.4 : Sia $F = \mathbb{Q}$, $E = \text{Split}_F(X^3 - 2)$. $|E : F| = 6$, dato che $E \cong \mathbb{Q}(\sqrt[3]{2}, \omega_3)$, dove ω_3 è una radice di $X^2 + X + 1$, e $|E : F|$ divide $3! = 6$ ed è multiplo di $3 = |\mathbb{Q}(\sqrt[3]{2} : F)$ e di $2 = \mathbb{Q}(\omega_3) : F$.

Sia ora $G = \text{Aut}(E|F)$. È un insieme con 6 elementi, dato che è il campo di spezzamento di un polinomio separabile. D'altra parte non vi sono molti gruppi di ordine 6, a meno di isomorfismo. Se osserviamo che l'identità di $\mathbb{Q}$ si estende in due modi,

$$\begin{cases} \text{id} \colon \omega_3 \mapsto \omega_3 \\ \tau \colon \omega_3 \mapsto \overline{\omega_3} \end{cases} \tag{27}$$

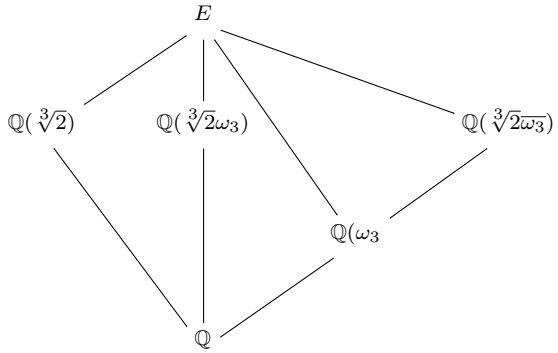
e ognuno di questi si estende in tre modi ad un automorfismo di tutto E,

$$\begin{cases} \text{id} \colon \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ p \colon \sqrt[3]{2} \mapsto \omega_3 \sqrt[3]{2} \\ \bar{p} \colon \sqrt[3]{2} \mapsto \overline{\omega_3} \sqrt[3]{2} \end{cases} \tag{28}$$

allora notiamo che G non è abeliano, e che quindi $\text{Aut}(E|F) \cong S_3$.

Il fatto che nell'ultimo esempio $\text{Fix}(\text{Aut}(E|F)) = F$ assicura che la corrispondenza di Galois è un antiisomorfismo di reticoli e che dunque in tale corrispondenza gli indici di sottogruppi corrispondono a gradi di estension intermedie.

I reticoli in esame si possono rappresentare in un diagramma come quello che segue (quello relativo ai sottogruppi è identico).



(29)

Certamente $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{2}\omega_3)$, ma a priori potremmo stare contando due volte le stesse estensioni. Per esempio può essere che $\mathbb{Q}(\sqrt[3]{2}\omega) = \mathbb{Q}(\sqrt[3]{2}\overline{\omega})$; mostriamo che non è così, supponendolo per assurdo.

Si avrebbe $\frac{\sqrt[3]{2}\omega}{\sqrt[3]{2}\overline{\omega}} \in \mathbb{Q}(\sqrt[3]{2}\omega)$, dunque $\omega \in \mathbb{Q}(\sqrt[3]{2}\omega)$[2]. Dunque $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}\omega)$, e $E = \mathbb{Q}(\sqrt[3]{2}\omega)$. D'altra parte questo è assurdo, perché riguardati come $\mathbb{Q}$-spazi vettoriali essi hanno dimensioni diverse.

Osservazione 11. Sia $f(X)$ un polinomio separabile su F, ed $E = \mathrm{Split}_F(f(X))$. Allora $|\operatorname{Aut}(E|F)| = |E : F|$. Ora, sia $f(X) = \prod g_i(X)^{m_i}$, con $g_i \in F[X]$ irriducibili distinti. I g_i hanno tutti radici semplici in E, e non ne hanno in comune; $E = \mathrm{Split}_F(g(X))$, dove $g = f_{\text{red}} = \prod g_i$ e g ha tutti zeri semplici.

Lemma 4.1 [ARTIN]**:** Sia E un campo, e $G \leq \operatorname{Aut}(E)$ un sottogruppo *finito*. Poniamo $F = \operatorname{Fix}(G)$. Allora $|E : F| \leq |G|$ (e in particolare E è un'estensione finita di F).

Dimostrazione. (L'idea di Artin è anche esteticamente molto valevole: no, così, per dire...).

Sia $G = \{\sigma_1, \ldots, \sigma_m\}$; se dimostriamo che il massimo numero di vettori linearmente indipendenti di E su F non è superiore a m si conclude.

Supponiamo quindi di avere $n > m$ vettori $\alpha_1, \ldots, \alpha_n \in E$, e consideriamo il sistema lineare di matrice

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \ddots & & \\ \vdots & & \ddots & \\ \sigma_m(\alpha_1) & & & \sigma_m(\alpha_n) \end{pmatrix} \tag{30}$$

[2]Perché $\frac{\omega}{\overline{\omega}} = \frac{\omega^2}{|\omega|^2} = -\frac{\omega}{|\omega|^2} - \frac{1}{|\omega|^2}$. Inoltre $\mathbb{Q}(\sqrt[3]{2}\omega) \ni (\sqrt[3]{2}\omega)^{-1} = \frac{\overline{\omega}}{\sqrt[3]{2}}$, dunque $\frac{\overline{\omega}}{\sqrt[3]{2}}\frac{\omega}{\overline{\omega}} = \frac{\omega}{\sqrt[3]{2}} \in \mathbb{Q}(\sqrt[3]{2}\omega)$. Infine, $\frac{\omega}{\sqrt[3]{2}}\sqrt[3]{2}\overline{\omega} = |\omega|^2 \in \mathbb{Q}(\sqrt[3]{2}\omega)$, e allora $|\omega|^2\left(-\frac{\omega}{|\omega|^2} - \frac{1}{|\omega|^2}\right) = -\omega - 1 \in \mathbb{Q}(\sqrt[3]{2}\omega)$, da cui si conclude.

Tale sistema lineare ha soluzioni non nulle in E. Ora, se c'è almeno una soluzione non nulla in F, dato che possiamo supporre che una delle σ_i sia id_E, otteniamo la dipendenza lineare cercata.

Scegliamo una soluzione $(c_1, \dots, c_n) \neq (0, \dots, 0)$ con il massimo numero possibile di zeri nelle entrate. A meno di permutare le c_i supponiamo che $c_1 \neq 0$, e sostituiamo $(c_1, \dots, c_n)$ con $(1, c_2', \dots, c_n')$, dove $c_i' = \frac{c_i}{c_1}$. Mostriamo che tale vettore ha entrate tutte in F. Se esiste $c_i \notin F$ infatti esiste $\tau \in G$ che la lo fissa: $\tau(c_i) \neq c_i$. Ora è il momento di usare il *trucco di Artin*: applicando τ a

$$\begin{cases} \sigma_1(\alpha_1)c_1 + \cdots + \sigma_1(\alpha_n)c_n \\ \vdots \\ \sigma_m(\alpha_1)c_1 + \cdots + \sigma_m(\alpha_n)c_n \end{cases} \tag{31}$$

otteniamo

$$\begin{cases} \sigma_1(\alpha_1)\tau c_1 + \cdots + \sigma_1(\alpha_n)\tau c_n \\ \vdots \\ \sigma_m(\alpha_1)\tau c_1 + \cdots + \sigma_m(\alpha_n)\tau c_n \end{cases} \tag{32}$$

In un gruppo però la traslazione a sinistra è una permutazione, dunque le righe sono le stesse di prima in ordine diverso. Allora anche $(\tau c_1, \dots, \tau c_n)$ risolve il sistema; allora anche il vettore $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} - \begin{pmatrix} \tau c_1 \\ \vdots \\ \tau c_n \end{pmatrix}$ ne è soluzione. Questa soluzione è diversa da zero: $\tau c_i \neq c_i$. E d'altra parte ha più zeri di prima: tutti quelli da cui partivamo (perché $\tau(0) = 0$) più uno in prima posizione ($\tau(1) = 1$).

Questo è assurdo: ne segue che tutti i c_i stanno in F, e quindi ne segue la dipendenza voluta. □

Osservazione 12. Il Lemma di Artin è la parte difficile della doppia inclusione $|E : F| = |G| < \infty$: infatti se $\#\{F\text{-automorfismi di } E\} \leq |E : F| \leq |G|$, d'altra parte certamente $|G| \leq \#\{F\text{-automorfismi di } E\}$. Dunque ecco l'uguaglianza: nelle ipotesi del Lemma di Artin

$$\mathrm{Aut}(E|\,\mathrm{Fix}(G)) = G$$

(e, nelle ipotesi del Lemma di Artin, E è di Galois su F).

Esercizio 2. Studiamo $\mathrm{Aut}(F(t)|F)$, dove F è un campo qualsiasi e t un F-trascendente (dunque $E = F(t) \cong \left\{ \frac{f(X)}{g(X)} \mid f(X) \in F[X],\ g(X) \in F[X] \setminus \{0\} \right\}$).

Come noto, dato $\varphi\colon E \to E$ esso è completamente determinato dall'immagine di t, che deve essere un F-trascendente. La domanda diventa allora: chi sono gli F-trascendenti in E?

Sia $u = \frac{f(t)}{g(t)} \in E$ (wlog supponiamo $(f, g) = 1$). Se u è algebrico su F esistono scalari $a_0, \ldots, a_n \in F$ tali che

$$a_0 + a_1 \frac{f(t)}{g(t)} + \ldots a_m \frac{f(t)^m}{g(t)^m} = 0 \tag{33}$$

ovvero

$$a_0 g(t)^m + a_1 f(t) g(t)^{m-1} + \cdots + a_{m-1} f(t)^{m-1} g(t) + a_m f(t)^m = 0 \tag{34}$$

Ora, $g(t)$ divide 0 e divide quest'ultimo coso, quindi deve dividere $a_m f(t)^m$, ma $(g, f) = 1$; quindi $g(t) \in F^\times$. Ragionando così anche per $f(t)$ otteniamo $f(t) \in F$.

Allora gli F-algebrici di E sono tutti e soli gli elementi di F; dunque i trascendenti sono tutti e soli gli elementi di $F(t) \setminus F$. Ora, $\varphi\colon E \to E$ in generale non è un epimorfismo: se $\varphi(t) = u$, in generale $|F(t) : F(u)| > 1$. Come determinarlo? Mostriamo che t è $F(u)$-algebrico. Innanzitutto, se $g(t)u - f(t) = 0$, allora t è radice di $g(X)u - f(X) \in F(u)[X]$. Ora, se $f(X) = \sum^m a_i X^i$, $g(X) = \sum^n b_j X^j$, il termine di grado massimo è

$$\begin{cases} m > n & -a_m \\ m = n & (b_n u - a_n) \\ m < n & b_n \end{cases} \tag{35}$$

e in tutti e tre i casi è diverso da zero (nel secondo, perché altrimenti $u = \frac{a_n}{b_n} \in F$).

Allora $g(X)u - f(X)$ è il polinomio minimo di t su $F(u)$, e

$$|F(t) : F(u)| = \max\{\deg f, \deg g\} \tag{36}$$

La suriettività di φ è garantita solo quando $|F(t) : F(u)| = \max\{\deg f, \deg g\} = 1$, ossia quando $g(X)u - f(X)$ è di grado 1. In sintesi

$$\begin{aligned} F(t) \cong F(u) &\iff |F(t) : F(u)| = 1 && (37)\\ &\iff \max\{\deg f, \deg g\} = 1 && (38)\\ &\iff \deg f, \deg g \leq 1 && (39)\\ &\iff u = \frac{at + b}{ct + d},\ (a, c) \neq (0, 0). && (40) \end{aligned}$$

In base a questo, $GL(2, F) \to \mathrm{Aut}(F(t)|F)$ è un epimorfismo di gruppi di nucleo F, dunque si conclude che $\mathrm{Aut}(F(t)|F) \cong PGL(2, F)$.

4.2 Caratterizzazione delle estensioni di Galois.

Sia $E|F$ di grado finito. Se E è di Galois su F, allora $\mathrm{Aut}(E|F) = F$, dunque per ogni $a \in E \setminus F$, esiste $\sigma \in \mathrm{Aut}(E)$ che sposta a.

Teorema 4.1 : Le seguenti condizioni sono equivalenti:

- $E = \text{Split}_F(f(X))$, per un polinomio $f \in F[X]$ separabile;
- $F = \text{Fix}(G)$, per qualche $G \leq \text{Aut}(E)$ finito;
- $|E : F|$ è finito, ed E è estensione normale e separabile su F;
- $E|F$ è di Galois.

(ricordiamo che $K|F$ si dice *separabile* su F se è un'estensione algebrica e per ogni $u \in K$, $\min_F(u)$ è un polinomio separabile; ancora, $K|F$ è *normale* su F se per ogni $u \in K$, $\min_F(u)$ sifattorizza completamente in K, ossia per ogni $u \in K$, K contiene tutte le radici di $\min_F(u)$.

Dimostrazione. $1 \Rightarrow 4$. Sia $n = \deg f$. Allora $|E : F|$ divide $n!$, dunque è finito. Sia poi $F' = \text{Fix}(\text{Aut}(E|F))$: chiaramente $F \subseteq F'$. Ora $E = \text{Split}_{F'}(f)$ (perché $f \in F[X] \subseteq F'[X]$) ed f è separabile su F'. Allora se $|\text{Aut}(E|F)| = |E : F| \geq |E : F'| = |\text{Aut}(E|F')|$ è chiaro che $\text{Aut}(E|F') \subseteq \text{Aut}(E|F)$; d'altra parte $F' = \text{Fix}(\text{Aut}(E|F))$, dunque $|E : F'| = |\text{Aut}(E|F)| = |E : F|$. Ma allora $F \cong F'$.

$4 \Rightarrow 2$. Per ipotesi si ha la prima parte, e ancora dato che $E|F$ è di Galois, $|E : F|$ è finito, dunque $G = \text{Aut}(E|F)$ è finito, e sottogruppo di $\text{Aut}(E)$.

$2 \Rightarrow 3$. Per il Lemma di Artin $|E : F| \leq |G|$, dunque $E|F$ è una estensione finita. Sia ora $\alpha \in E$; G agisce naturalmente su E: consideriamo l'orbita di α rispetto a questa azione. È certamente un insieme finito, diciamo di $m \leq |G|$ elementi (l'uguaglianza si ha se l'azione è fedele). Sia ora $g = \prod(X - \alpha_i) \in E[X]$. Per ogni $\tau \in G$, $\tau(\alpha_i) = \alpha_j$, dunque $\tau(g(X)) = g(X)$, perché τ fissa tutti i coefficienti di $g(X)$. Da ciò tutti i coefficienti di g sono in F, e g ha per costruzione radici semplici. Ovviamente $g(\alpha) = 0$, e allora se mostriamo che $g = \min_F(\alpha)$ abbiamo finito. Se $f = \min_F(\alpha)$; allora $\sigma(f(\alpha))f(\sigma(\alpha)) = 0$ per ogni $\sigma \in G$: dunque $f|g$, e $g|f$ per minimalità. Dunque (essendo monici) i due polinomi coincidono.

$3 \Rightarrow 1$. Sappiamo che $|E : F| < \infty$, $E = F(\beta_1, \ldots, \beta_r)$ dove i β_i sono tutti algebrici su F. Sia $g_i = \min_F(\beta_i)$, ed $f = \prod g_i$. Ogni g_i è prodotto di fattori lineari distinti in $E[X]$ (E separabile su F), e ora il prodotto di tutti i g_i è separabile. Per minimalità, $E = \text{Split}(f)$.

Le altre implicazioni seguono. □

Alla luce di questo risulta evidente perché in $F \leq M \leq E$ non sempre $M|F$ sia di Galois. Se non si allarga abbastanza F, possono non esserci tutte le radici. In un caso concreto, $\mathbb{Q}(\sqrt[3]{2}, \omega_3)|\mathbb{Q}$ è di Galois, così come $\mathbb{Q}(\sqrt[3]{2}, \omega_3)|\mathbb{Q}(\sqrt[3]{2})$, ma non lo è $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ (non è normale).

$F(t)$ è di Galois su F? Supponendo che t sia F-trascendente, può essere $F(t)|F$ di Galois? Vanno distinti due casi.

- *F è un campo finito*: allora $|F| = q = p^n$ per qualche primo p. Ora, $|GL(2,F)| = (q^2-1)(q^2-q)$, dunque $|PGL(2,F)| = (q^2-1)(q-1)$. Per il Lemma di Artin $|F(t) : \text{Fix}(\text{Aut}(F(t)|F))| \leq |GL(2,F)|$, in particolare deve essere finito. D'altra parte $|F(t) : F| = \infty$, dunque $F(t)|F$ non è di Galois.

- *F è un campo infinito*: gli elementi di $G = \text{Aut}(F(t)|F)$ sono del tipo $t \mapsto \frac{at+b}{ct+d}$. Consideriamo $\tau_b \colon t \mapsto t+b$; chi sono gli elementi di $F(t)$ invarianti rispetto a tutti i $\tau_b, b \in F$? Se $\frac{f(t+b)}{g(t+b)} = \frac{f(t)}{g(t)}$, allora $g(t)f(t+b) = f(t)g(t+b)$, dunque $g(t)f(t+X) - f(t)g(t+X)$ è il polinomio nullo in $F[X]$ (ha infiniti zeri). Se $f = \sum^m a_i t^i$, $g = \sum^n b_j t^j$, allora $g(t)f(t+b) = f(t)g(t+b)$ implica che $g(t)a_m X^m \neq 0, f(t)b_n X^n \neq 0$, dunque $n = m$, e da questo $g(t)a_m = f(t)b_n$ implica che $f/g = u \in F$. Allora se u è fissato da tutti i τ_b sta in F. A maggior ragione se u è tenuto fermo da tutto $\text{Aut}(F(t)|F)$ sta in F: ergo $\text{Fix}(\text{Aut}(F(t)|F)) = F$, ed $F(t)|F$ è di Galois.

Studiamo ora più da vicino la connessione di Galois enunciata prima. Se $E|F$ è di Galois, diciamo $\text{Aut}(E|F) := \text{Gal}(E|F)$. Dati $H_1, H_2 \leq \text{Gal}(E|F)$, essi sono $\text{Gal}(E|\,\text{Fix}(H_i))$, perché $E|\,\text{Fix}(H_i)$ è di Galois. Dunque $|E : \text{Fix}(H_i)| = |H_i|$. D'altra parte se $H_1 \leq H_2$ abbiamo

$$\begin{cases} \frac{|H_1|}{|H_2|} = |H_1 : H_2| & \text{(thm. di Lagrange)} \\ \frac{|E:\text{Fix}(H_2)|}{|E:\text{Fix}(H_1)|} = |\,\text{Fix}(H_1) : \text{Fix}(H_2)| & \text{(formula dei gradi).} \end{cases} \tag{41}$$

Viceversa, dati $M_1 \geq M_2$ campi intermedi tra E ed F esistono $H_1 < H_2 \leq \text{Gal}(E|F)$ tali che $\text{Gal}(E|M_i) = H_i$, e ci si riconduce al caso precedente.

Cosa accade ai sottogruppi normali? Se $\sigma, \tau \in \text{Gal}(E|F)$, ed $a \in E$, si ha $\tau a = a \iff \sigma\tau a = \sigma a = \sigma\tau\sigma^{-1}(\sigma a)$, dunque ad ogni $a \in \text{Fix}(H)$ corrisponde uno e un solo elemento di $\text{Fix}(\sigma H \sigma^{-1}) = \sigma\,\text{Fix}(H)$. Di converso, lasciando variare i campi intermedi $F \leq M \leq E$ si ha

$$\text{Aut}(E|\sigma M) = \sigma\,\text{Aut}(E|M)\sigma^{-1} \tag{42}$$

Allora nella corrispondenza di Galois il coniugio di $H \leq \text{Gal}(E|F)$ mediante σ corrisponde all'immagne tramite l'elemento per cui si coniuga del campo $\text{Fix}(H)$. Alla luce di questo, appare chiaro che $H = \text{Gal}(E|M) \trianglelefteq G$ se e solo se $\sigma M = M$ per ogni $\sigma \in \text{Gal}(E|F)$.

La domanda quindi diventa: quali sono i sottocampi di E, contenenti F, e tali che ogni $\sigma \in \text{Gal}(E|F)$ li manda in sè stessi? I campi estremali in questo senso sono chiaramente E, F; per trovare gli altri ragioniamo come segue.

Se $F < M$ propriamente, per ogni $a \in M \setminus F$ esiste $\sigma \in \text{Gal}(E|F)$ tale che $\sigma a \neq a$. Tale σ è un automorfismo di M (per l'ipotesi $\sigma M = M$), ed è l'identità ristretta ad F. Dato che $a \in M \setminus F \Rightarrow \exists \sigma a \neq a$, allora

Fix(Aut$(M|F)) = F$, ed $M|F$ è di Galois. Dunque $\sigma M = M$ per ogni σ, ed $M|F$ è di Galois.

Viceversa, sia $E|F$ di Galois, $E \geq M|F$ di Galois, $\sigma \in \text{Gal}(E|F)$. $M = F(\alpha_1, \ldots, \alpha_n)$, dove le α_i sono le radici di un polinomio separabile. Ora, $\sigma(M) = \sigma(F)(\sigma\alpha_1, \ldots, \sigma\alpha_n) = F(\alpha_1, \ldots, \alpha_n) = M$ (σ è l'identità u F e si limita a permutare le radici del polinomio f tale che $M = \text{Split}(f)$).

In effetti è ragionevole pensare che

$$\{H \mid H \trianglelefteq \text{Gal}(E|F)\} \longleftrightarrow \{M \mid M|F \text{ è di Galois}\} \tag{43}$$

Da ultimo, si ha $\text{Gal}(M|F) \cong \text{Gal}(E|F)/\text{Gal}(E|M)$ (la restrizione ad M induce un epimorfismo $\text{Gal}(E|F) \to \text{Gal}(M|F)$ che ha nucleo esattamente $\text{Gal}(E|M)$).

5 Radici n-esime di $a \in F$.

Ci occupiamo di polinomi della forma $X^n - a$, per $a \in F$ campo prescritto.

- Il caso $a = 0$ si esaurisce facilmente, dato che $\text{Split}_F(X^n) = F$, ed F è sempre di Galois su sè stessa (con gruppo di Galois banale).
- Nel caso $a = 1$, ci poniamo tre problemi distinti:
  - Come descrivere $E = \text{Split}_F(X^n - 1)$?
  - $E|F$ è di Galois?
  - Se non lo è, come descrivere Aut$(E|F)$?

  Anzitutto, $E^\times \geq U = \{z \in E \mid z^n = 1\}$ come sottogruppo moltiplicativo, e tale sottogruppo è ciclico (generato da quelle che si chiamano *radici primitive* dell'unità). Dunque $E = F(\zeta)$, dove ζ è una tale radice primitiva.

  Poi, per studiare la separabilità di $f(X) = X^n - 1$ dobbiamo dividere più casi. Supponiamo dapprima che $\text{char}\, F \in \{0, p\}$, dove $p \nmid n$. In tal caso $f'(X) = nX^{n-1}$, che ha solo zero come radice, e però $f(0) \neq 0$ in F. Dunque $X^n - 1$ è separabile.

  Supponiamo ora che $\text{char}\, F = p$, ed $n = p^k m$. Allora $X^n - 1 = (X^m - 1)^{p^k}$, che certamente ha radici multiple. D'altra parte ci si riconduce al caso precedente, perché si può supporre di aver raccolto la massima potenza di p che divide n, e dunque $X^m - 1 = f_{\text{red}}$ è separabile. Dunque in ambo i casi, $E|F$ è di Galois.

  Resta da studiare come sia fatto Gal$(E|F)$. Un automorfismo di $F(\zeta)$ che fissa F manda ζ in un'altra radice del suo polinomio minimo, che è $1 + X + \cdots + X^{n-1}$, in particolare $\sigma \in \text{Gal}(E|F)$ permuta $U = \mathbb{Z}/n\mathbb{Z}$. È facile notare che la mappa di gruppi $G \hookrightarrow \text{Aut}(U)$ rende $G = \text{Gal}(E|F)$ un sottogruppo di Aut(U) (è un monomorfismo,

perché $\sigma(\zeta) = \zeta \iff \sigma = \mathrm{id}_G$). Dunque $\mathrm{Gal}(E|F)$ si identifica a un sottogruppo di $\mathrm{Aut}(U) \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$; in particolare è un sottogruppo di un gruppo abeliano con $\phi(n)$ (Eulero) elementi.

Non è detto che sia suriettivo! Essenzialmente, non è detto che radici distinte di 1 abbiano lo stesso polinomio minimo, ossia non è detto che $1+X+\cdots+X^{n-1}$ sia irriducibile su F: ora, siccome si può mandare ζ *solo* in un'altra radice di $\min_F(\zeta)$, la mappa non è un epimorfismo.

- Consideriamo da ultimo il polinomio $f(X) = X^n - a$; supponiamo che$F$ contenga tutte le radici n-esime di 1 (in particolare questo implica che $\mathrm{char}\, F \nmid n$), e che $E \cong \mathrm{Split}_F(f)$. Allora

  – $E|F$ è di Galois;

  – $E \cong F(b)$ con $b^n = a \in F$;

  – $\mathrm{Gal}(E|F)$ è ciclico e il suo ordine divide n.

Dimostrazione. $1 + 2$. Se b è una radice n-esima di a, tutte le altre radici sono $\{b\zeta^k \mid k = 1, \dots, n\}$. Infatti se $u^n = a$ allora $\left(\frac{u}{b}\right)^n = 1$ e $u/b = \zeta^k$ per qualche $0 \leq k \leq n-1$. Il viceversa è evidente.

Dunque $X^n - a$ ha in E n radici distinte: considerando questo e il fatto che $\zeta \in F$, si ottiene la tesi.

Il terzo punto si mostra notando che se $\sigma \in \mathrm{Gal}(E|F)$, esso manda b in un'altra radice di $X^n - a$: allora $\sigma b = bz$ per qualche $z \in U$. Definiamo

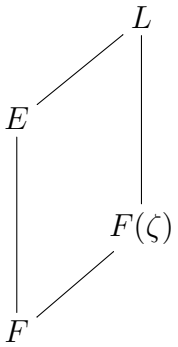
$$\begin{aligned} \alpha\colon \mathrm{Gal}(E|F) &\longrightarrow U \\ \sigma &\longmapsto \sigma(b)/b = z \end{aligned} \tag{44}$$

(b è fissato). Si nota facilmente che questo è un omomorfismo di gruppi, e che è iniettivo. Dunque si conclude ricordando che ogni sottogruppo di Uè abeliano (perché ciclico) e il suo ordine divide n. □

Esercizio 3. A quali condizioni α è un isomorfismo?

Supponiamo $\mathrm{char}\, F = 0$ e che F non contenga tutte le radici n-esime di 1. Se $E = \mathrm{Split}_F(X^n - a)$, chiaramente $E|F$ è di Galois. Vogliamo trovare

Gal$(E|F)$ e usiamo questo trucco. Consideriamo



(45)

dove $L \cong \text{Split}_E(X^n - 1)$. Si osservi che $L|F(\zeta)$, $L|F$ sono anch'esse di Galois (la prima è $\text{Split}_{F(\zeta)}(X^n - a)$, e Gal$(L|F(\zeta))$ è ciclico di ordine $\mid n$; la seconda è $\text{Split}_F((X^n - 1)(X^n - a))$, e $U = \{z \mid z^n = 1\}$ è ciclico generato da ζ, radice primitiva). Inoltre $F(\zeta)|F$ è di Galois (visto prima) e ha gruppo abeliano (in quanto sottogruppo di un abeliano: anch'esso visto prima).

Inoltre, $\frac{\text{Gal}(L|F)}{\text{Gal}(L|F(\zeta))} \cong \text{Gal}(F(\zeta)|F)$. Sia ora $G = \text{Gal}(L|F)$; il sottogruppo che corrisponde a $L|F(\zeta)$ è Gal$(L|F(\zeta)) = H \trianglelefteq G$ (è normale perché l'estensione intermedia $F(\zeta)|F$ è di Galois) e $G/H \cong \text{Gal}(F(\zeta)|F)$ è abeliano.

Allo stesso modo se $E|F$ è di Galois, $F < E \leq L$ corrisponderà a un sottogruppo normale di G, e Gal$(E|F) \cong \frac{\text{Gal}(L|F)}{\text{Gal}(L|E)}$, un quoziente di G per un sottogruppo K ciclico.

Esempio 5.1 : Consideriamo $F = \mathbb{Q}$ e il polinomio $X^5 - 2$, irriducibile su $\mathbb{Q}$. Allora $E = \text{Split}_F(X^5 - 2) \cong \mathbb{Q}(\sqrt[5]{2}, \zeta)$. $E|\mathbb{Q}$ è di Galois, e $|\,\text{Gal}(E|\mathbb{Q})| = d = |E : \mathbb{Q}|$. Ora, $4, 5 \mid d = |E : \mathbb{Q}(\zeta)| \cdot |\mathbb{Q}(\zeta : \mathbb{Q}|$ e d'altra parte $|E : \mathbb{Q}| \leq 20$. Quindi $d = 20$.

Sappiamo che $H = \text{Gal}(E|\mathbb{Q}(\zeta))$ ha ordine 5, dunque è ciclico; $G/H \cong$ Gal$(\mathbb{Q}(\zeta)|\mathbb{Q})$ allora è abeliano di ordine $4 = |G/H| = |\,\text{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})| = |\mathbb{Q}(\zeta) : \mathbb{Q}|$, e quindi è un sottogruppo di $U(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$.

6 Polinomi ciclotimici.

Consideriamo $X^n - 1 \in \mathbb{Q}[X]$. Come fattorizzarlo? La discussione precedente mette in luce che nel suo campo di spezzamento

$$X^n - 1 = \prod_{z \in U}(X - z) \tag{46}$$

È facile notare che $z \in U$ se e solo se z è un elemento di ordine finito, che divide n: ciò permette di riscrivere

$$X^n - 1 = \prod_{z \in U}(X - z) = \prod_{d|n} \prod_{\text{ord}(z)=d}(X - z) = \prod_{d|n} \Phi_d(X) \tag{47}$$

Si determinano facilmente a mano i primi elementi della successione $\{\Phi_n(X)\}$:

$$\Phi_1(X) = X - 1 \tag{48}$$
$$\Phi_2(X) = X + 1 \tag{49}$$
$$\Phi_3(X) = X^2 + X + 1 \tag{50}$$
$$\Phi_4(X) = X^2 + 1 \tag{51}$$

e gli altri si ricavano ricorsivamente a partire dalla relazione

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)} \tag{52}$$

Si osservi che

- Se n è primo, $\Phi_n(X) = \sum_{k=0}^{n-1} X^k$.
- $\Phi_n(X)$ ha sempre coefficienti interi.
- Ogni $\Phi_n(X)$ è irriducibile su $\mathbb{Q}$.
- $\deg \Phi_n(X) = \phi(n)$.

Prove confuse di questi fatti: il primo si dimostra a partire dalla definizione ricorsiva. Il secondo per induzione: è vero nei primi casi, e se supponiamo sia vero per $m < n$ abbiamo $X^n - 1 = \Phi_n(X) \prod_{d||n} \Phi_d(X)$. Ora, sia $X^n - 1$ che $\Phi_d(X)$ hanno coefficienti interi, dunque deve averli $\Phi_n(X)$ (per assurdo).

Mostriamo l'irriducibilità su $\mathbb{Q}$: nel caso n sia primo, la tesi segue usando il criterio di Eisenstein e la sostituzione $x \mapsto x + 1$.

Mostriamolo in generale per $n > 1$.

Dimostrazione. Supponiamo che $\Phi_n(X) = g(X)h(X)$ con $g, h \in \mathbb{Z}[X]$ monici di grado maggiore di zero. Mostriamo che $g(X) = \Phi_n(X)$.

Sappiamo che g ha almeno uno zero complesso, dunque esiste $\zeta \in U$ tale che $g(\zeta) = 0$.

Se sapessimo che $g(\zeta) = 0$ implica $g(\zeta^p) = 0$ per ogni $p \nmid n$ avremmo finito, per ovvi motivi: gli zeri di $\Phi_n(X)$ sono tutti e soli gli ζ^k con $(k, n) = 1$, e se $k = \prod p_i^{s_i}$, e ζ è zero di g, allora lo è ζ^k, e a questo punto $g = \Phi_n$ (a meno di un segno).

Supponiamo allora che $g(\zeta) = 0$ ma $g(\zeta^p) \neq 0$, per $p \nmid n$. Allora in $\Phi_n(X) = g(X)h(X)$, ζ^p è radice di $h(X)$. Sia $h(X) = \sum^r b_i X^i$; allora ζ è zero di $h(X^p)$. Se ζ è zero sia di g che di $h(X^p)$, il Lemma di Gauss implica che esiste $k \in \mathbb{Z}[X]$ monico e di grado positivo, che divide entrambi.

Ora, riduciamo tutto modulo p: $\overline{h(X^p)} = \overline{h(X)}^p$; dunque $\bar{k} \mid \bar{h}^p$, $\bar{k} \mid \bar{g}$ (riducendolo modulo p il grado di k non può abbassarsi perché era monico).

Dunque $\bar{g}, \bar{h}$ hanno un divisore comune, diciamo $\bar{\ell}$, in $\mathbb{Z}/p\mathbb{Z}[X]$. Ora, $\overline{\Phi_n(X)} = \bar{g}_1 \bar{h}_1 \bar{\ell}^2 \mid X^n - 1$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Però questo implicherebbe che

$\overline{\Phi_n(X)}$ ha zeri doppi, e questo è assurdo (se $p \nmid n$, $X^n - 1$ ha zeri semplici in $\mathbb{Z}/p\mathbb{Z}$). □

Cosa abbiamo detto finora:

- $E = \text{Split}_{\mathbb{Q}}(X^n - 1)$; $E \cong \mathbb{Q}(\zeta)$, ζ radice primitiva di 1;
- $|E : \mathbb{Q}| = \deg \Phi_n(X) = \phi(n)$;
- $\text{Gal}(E|\mathbb{Q}) \cong H \leq U(\mathbb{Z}/n\mathbb{Z})$.

La seconda e terza constatazione implicano che $\text{Gal}(E|\mathbb{Q}) \cong U(\mathbb{Z}/n\mathbb{Z})$ perché $|\text{Gal}(E|\mathbb{Q})| = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Estensioni del tipo $\mathbb{Q}(\zeta)|Q$ si dicono *ciclotomiche*:

$$\text{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong U(\mathbb{Z}/n\mathbb{Z}) \tag{53}$$

Struttura di $U(\mathbb{Z}/n\mathbb{Z})$. Cominciamo osservando che

$$U(\mathbb{Z}/mn\mathbb{Z}) \cong U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z}) \tag{54}$$

dunque basta studiare il caso $U(\mathbb{Z}/p^k\mathbb{Z})$.

Supponiamo per ora che $p \neq 2$. Allora

$$|U(\mathbb{Z}/p^k\mathbb{Z})| = \phi(p^k) = p^{k-1}(p-1) \tag{55}$$

Si osservi anche che $(p^{k-1}, p-1) = 1$.

Osservazione 13. Si ricordi che ogni gruppo abeliano finito G si rompe nel prodotto diretto delle sue parti p-primarie, al variare dei primi che compaiono nella fattorizzazione di $|G|$, ossia

$$G \cong \prod_{i=1}^r \Sigma_{p_i} \tag{56}$$

se $|G| = \prod_{i=1}^r p_i^{a_i}$ e $\Sigma_{p_i} = \{g \in G \mid \text{ord}_G g = p_i^n \ \exists n \in \mathbb{N}\}$.

Definiamo ora $A, B \leq U(\mathbb{Z}/p^k\mathbb{Z})$ come

$$A = \{u \in U \mid u^{p-1} = 1\} \tag{57}$$
$$B = \{u \in U \mid \text{ord}_U u = p^n\} \tag{58}$$

Chiaramente $B = \Sigma_p \leq U(\mathbb{Z}/p^k\mathbb{Z})$ è la parte p-primaria di $U(\mathbb{Z}/p^k\mathbb{Z})$, dunque $U(\mathbb{Z}/p^k\mathbb{Z}) \cong A \times B$. Definiamo poi $T = \{u \in U \mid u \equiv 1 \pmod p\}$.

$T \leq U$, e $|T| = p^{k-1}$ perché $T = \{1 + pr \mid 0 \leq r < p^{k-1}\}$. Se mostriamo che $\text{ord}(1+p) = p^{k-1}$ mostriamo due cose:

- T è ciclico (ha un elemento di ordine pari a $|T|$);

- $T = B$, dato che $1 + p$ sta in B, T sta in un sottogruppo della sua stessa cardinalità.

Dunque B è ciclico.

Dimostrazione. Per induzione su n si può provare che $(1+p)^{p^n} \equiv 1 \pmod{p^{n+1}}$, e $(1+p)^{p^n} \not\equiv 1 \pmod{p^{n+2}}$; da questo segue che se $n = k-1$, $(1+p)^{p^{k-1}} \equiv 1 \pmod{p^k}$, e se $n = k-2$, $(1+p)^{p^{k-2}} \not\equiv 1 \pmod{p^k}$.

La base dell'induzione è evidente. Il passo induttivo segue dal fatto che $(1+p)^{p^{n-1}} = 1 + hp^n$, con $p \nmid h$. Ora,

$$(1+p)^{p^n} = (1+hp^n)^{p^n} \tag{59}$$

$$= 1 + php^n + \binom{p}{2}(hp^n)^2 + \dots \tag{60}$$

$$= 1 + hp^{n+1} + p^{n+2}v \tag{61}$$

$$\equiv 1 \pmod{p^{n+1}} \tag{62}$$

$$\not\equiv 1 \pmod{p^{n+2}} \tag{63}$$

perché $p \nmid h$. Dunque $U(\mathbb{Z}/p^k\mathbb{Z}) \cong A \times T$. □

Ora, definiamo $\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ come la mappa $t \mapsto t + p\mathbb{Z}$. Da questa viene indotta una mappa tra i gruppi degli invertibili (che è suriettiva, in questo caso: $(p\mathbb{Z})^c$ è un sistema moltiplicativo in $\mathbb{Z}$).

Allora c'è un omomorfismo suriettivo di gruppi $A \times T \twoheadrightarrow U(\mathbb{Z}/p\mathbb{Z})$, di nucleo esattamente T. Con ciò la sequenza di gruppi

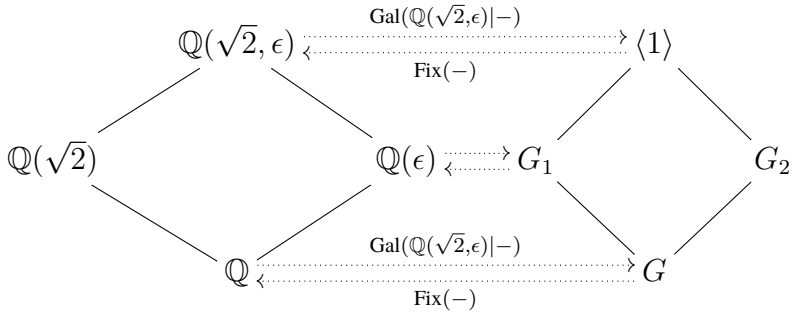
$$1 \to T \to A \times T \to U(\mathbb{Z}/p\mathbb{Z}) \to 1 \tag{64}$$

è esatta, e dunque $A \cong (A \times T)/T \cong U(\mathbb{Z}/p\mathbb{Z})$ è ciclico di ordine $p-1$.

Alcuni gruppi famosi sono gruppi di Galois. Il problema di Galois inverso è: dato un gruppo G esistono campi $E|F$ tali che $\mathrm{Gal}(E|F) \cong G$? In generale la risposta è "boh".

- $C_2 \cong \mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q})$, dove $\alpha \notin \mathbb{Q}$ è radice di un polinomio di grado 2. L'estensione è di Galois perché $aX^2 + bX + c = 0$ implica che $x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a}$, e dunque il minimo campo che contiene $\sqrt{\Delta}$ contiene anche il suo inverso.
- $C_2 \times C_2 \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q})$, dato che $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathrm{Split}_{\mathbb{Q}}((X^2-2)(X^2-3))$, e il gruppo di Galois di questa estensione è facilmente isomorfo al gruppo di Klein.
- $C_4 \cong \mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q})$, dove $\epsilon^5 = 1$ è radice primitiva. Allora $\mathrm{Gal}(\mathbb{Q}(\epsilon)|\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong C_4$, generato da 2 o 3.

- $C_2 \times C_2 \times C_2 \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})|\mathbb{Q})$, dato che $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathrm{Split}_{\mathbb{Q}}((X^2-2)(X^2-3)(X^2-5))$; in effetti in generale $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n})|\mathbb{Q}) \cong \prod_{i=1}^{n} C_2$, se $p_1,\ldots,p_n$ sono primi distinti.
- $C_2 \times C_4 \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\epsilon)|\mathbb{Q})$: le corrispondenze $\mathrm{Fix}(-)$ e $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\epsilon)|-)$ mettono in relazione i reticoli di campi e sottogruppi in questo modo:



  $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\epsilon)|\mathbb{Q}) \cong G_1 \times G_2$ perché $G_1G_2 =$ e $G_1 \cap G_2 = \langle 1\rangle$($\iff \mathrm{Fix}(G_1) \cap \mathrm{Fix}(G_2) = \mathbb{Q}$).
- Per trovare $E|\mathbb{Q}$ tale che $\mathrm{Gal}(E|\mathbb{Q}) \cong C_8$ si procede come segue: sia ζ una radice primitiva 2^5-esima dell'unità. Si noti che $|\mathbb{Q}(\zeta) : \mathbb{Q}| = |\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})| = 2^4 = 16$, e $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong C_2 \times B$, dove B è ciclico di ordine 8, ed è quindi esattamente il gruppo cercato. B è normale in $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$, dunque nella corrispondenza di Galois $E = \mathrm{Fix}(B)|\mathbb{Q}$ è di Galois, e $\mathrm{Gal}(E|\mathbb{Q}) \cong \frac{\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\zeta)|E)} \cong B$.

Osservazione 14. $E \cong \mathbb{Q}(\zeta+\zeta^{-1}) \cong \mathrm{Fix}(\langle\tau\rangle)$, dove $\tau\colon \zeta \mapsto \zeta^{-1}$. Ancora, $E \cong \mathbb{Q}(\zeta) \cap \mathbb{R}$.

7 Alcune nozioni di teoria dei gruppi.

7.1 Gruppi risolubili.

Ricordiamo che se G è un gruppo ciclico, $|G| \leq |\mathbb{N}|$ (in particolare non esistono gruppi ciclici di cardinalità maggiore del numerabile).

- Se G è finito, $|G| = n$, allora $G \cong (\mathbb{Z}/n\mathbb{Z},+)$;
- Se G è numerabile, $G \cong (\mathbb{Z},+)$.

Vale il seguente

Teorema 7.1 [Classificazione dei gruppi abeliani finiti]**:** Se G è un gruppo abeliano finito, allora esso si rompe nella somma diretta di gruppi ciclici, secondo la fattorizzazione in primi di $|G|$:

$$G \cong \bigoplus_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \tag{65}$$

dove $\sum n_i = |G|$.

Definizione 7.1 [Gruppo risolubile]**:** Un gruppo G si dice risolubile se esiste una catena finita di suoi sottogruppi

$$G = H_0 \geq H_1 \geq \cdots \geq H_r = \langle 1 \rangle \tag{66}$$

tale che

- $H_i \trianglelefteq H_{i-1}$;
- H_{i-1}/H_i è abeliano.

Ogni gruppo abeliano è risolubile: basta prendere la catena $G \geq \langle 1 \rangle$.
Un gruppo risolubile non abeliano è S_3: basta prendere la catena

$$S_3 \geq A_3 \geq \langle 1 \rangle \tag{67}$$

perché $A_3 \trianglelefteq S_3$ e $S_3/A_3 \cong C_2$ è ciclico, e $A_3/\langle 1 \rangle \cong A_3 \cong C_3$ anche.
Anche S_4 è risolubile: basta prendere la catena

$$S_4 \geq A_4 \geq V_4 \geq \langle 1 \rangle \tag{68}$$

Proposizione 7.1. Se $n \geq 5$, il gruppo simmetrico su n elementi non è risolubile.

Dimostrazione. Posposta. È un corollario del fatto che A_n è semplice, per $n \geq 5$; un gruppo semplice non abeliano non può essere risolubile (è ovvio dalla definizione). □

Esiste un criterio per stabilire la risolubilità di un gruppo che usa la *serie derivata* di G:

Definizione 7.2 : Se G è un gruppo, definiamo il *commutatore* di $x, y \in G$ come

$$[x, y] = x^{-1}y^{-1}xy \tag{69}$$

(moralmente $[x, y]$ misura lo scarto che esiste tra xy e yx, dato che $[x, y] = 1 \iff xy = yx$.)

Definizione 7.3 : Per due generici sottoinsiemi $H, K \subseteq G$ definiamo

$$[H, K] := \langle [h, k] \mid h \in H,\ k \in K \rangle \tag{70}$$

Osservazione 15. $\eta([x, y]) = [\eta(x), \eta(y)]$ per ogni omomorfismo d gruppi $\eta \colon G \to H$. In particolare $\alpha([x, y]) = [\alpha(x), \alpha(y)]$ per ogni $\alpha \in \mathrm{Aut}(G)$. Ancora più in particolare $g^{-1}[x, y]g = [g^{-1}xg, g^{-1}yg]$ per ogni $g, x, y \in G$.

Definizione 7.4 : Definiamo il *gruppo derivato di* G come

$$G' = G^{(1)} = [G, G] \leq G \tag{71}$$

Osservazione 16. $G' \trianglelefteq G$ e anzi è un sottogruppo *caratteristico* (i.e. non è fissato solo dal coniugio ma da tutti gli automorfismi di G).

Teorema 7.2 : Il quoziente G/G' è abeliano; inoltre, se $N \trianglelefteq G$ è tale che G/N è abeliano, allora $G' \leq N$.

Dimostrazione. Per quanto riguarda il primo punto

$$\begin{aligned}(a[G,G])\,(b[G,G]) &= ab[G,G] && (72)\\ &= abb^{-1}a^{-1}ba[G,G] && (73)\\ &= ba[G,G] && (74)\\ &= (b[G,G])\,(a[G,G])\,. && (75)\end{aligned}$$

Per il secondo punto, se G/N è abeliano $abN = baN$ implica che $a^{-1}b^{-1}ab \in N$ per ogni $a, b \in G$, dunque $[G,G] \leq N$ (ne contiene tutti i generatori). □

Definizione 7.5 : Definiamo l'n-esimo *derivato* di G induttivamente: $G^{(0)} := G$, $G^{(n)} := \left(G^{(n-1)}\right)'$.

Osservazione 17. $G^{(n)} \trianglelefteq G$ per ogni $n \geq 0$: segue dal fatto che se $H \trianglelefteq G$ e $K \leq H$ è caratteristico in H, allora $K \trianglelefteq G$.

Dimostrazione. Per ogni $g \in G$ l'automorfismo di coniugio restringe a un automorfismo di H che deve fissare K; dunque $i_g|_H(K) = K \ \forall g \in G$, ossia $g^{-1}Kg = K$ per ogni $g \in G$. □

Esiste una catena discendente

$$G \geq G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(n)} \geq \ldots \tag{76}$$

detta *serie derivata* di G.

Teorema 7.3 : Un gruppo G è risolubile se e solo se la sua serie derivata è stazionaria e raggiunge $\langle 1 \rangle$.

Dimostrazione. $\Leftarrow$ è ovvio: la serie derivata èlacatena richiesta.

Viceversa, supponiamo che esista una catena

$$G = H_0 \geq H_1 \geq \cdots \geq H_r = \langle 1 \rangle \tag{77}$$

tale che $H_{i+1} \trianglelefteq H_i$, e H_i/H_{i+1} abeliano. Allora $H_i \geq G^{(i)}$, perché per $i = 0$ è vero, e se supponiamo $H_n \geq G^{(n)}$ abbiamo $H_{n+1} \trianglelefteq H_n$, e H_n/H_{n+1} abeliano: questo implica che $H_{n+1} \geq H_n' \geq \left(G^{(n)}\right)' = G^{(n+1)}$; perciò $H_r = \langle 1 \rangle \geq G^{(r)}$ e la serie derivata si ferma. □

Proposizione 7.2. La serie derivata è "quella che arriva ad $\langle 1 \rangle$ più in fretta possibile" tra le catene che risolvono G (dimostrazione: omessa). In questo senso definiamo *lunghezza di risolubilità* il minimo intero r (fissato a ∞ se questo insieme è vuoto) tale che $G^{(r)} = \langle 1 \rangle$.

Sia A un gruppo abeliano finito; esso si spezza nel prodotto di ciclici: $A \cong \prod_{i=1}^{n} A_i$. Consideriamo la catena ottenuta togliendo uno ad uno gli A_i:

$$A \geq A_2 \times \cdots \times A_n \geq A_3 \times \cdots \times A_n \geq A_n \geq \langle 1 \rangle \tag{78}$$

Chiaramente ogni $\tilde{A}_k = \prod_{i \geq k}^{n} A_i$ è normale in A e i quozienti $\tilde{A}_k / \tilde{A}_{k+1} \cong A_k$ sono abeliani (perché ciclici).

Con ciò in mente consideriamo un gruppo G finito e risolubile: nella catena

$$G \geq H_1 \geq \cdots \geq H_r = \langle 1 \rangle \tag{79}$$

per il teorema di corrispondenza i sottogruppi di G/N sono i sottogruppi $H \geq N$, dunque nel quoziente $A = H_i / H_{i+i}$, che è abeliano finito, si trova una catena in cui tutti i quozienti sono ciclici

- perché è così nel caso G abeliano;
- perché se G è risolubile H_i / H_{i+i} è abeliano, e dunque esiste una catena
$$H_i / H_{i+i} \geq T_1 / H_{i+i} \geq \cdots \geq T_r / H_{i+i} \tag{80}$$
(corrispondente a $H_{i+1} \leq T_1 \leq \cdots \leq T_r = H_i$).

Teorema 7.4 : Sia G un p-gruppo (se G è finito vuol dire che $|G| = p^n$ per qualche primo p e $n \geq 1$; se G è infinito vuol dire che ogni $g \in G$ ha ordine una potenza di p). Allora il centro $Z(G)$ di G non è banale.

Dimostrazione. Omessa (noiosa). □

Corollario. Ogni p-gruppo finito G è risolubile.

Dimostrazione. Sia $Z(G)$ il centro di G. Se $Z(G) = G$ si conclude; d'altra parte se $Z^{(1)} := Z(G) \lneq G$, $G/Z(G)$ è ancora un p-gruppo non banale, dunque ha centro non banale: questo centro corrisponde a un sovragruppo di $Z(G)$ in G, diciamo $Z^{(2)}$; d'altra parte $Z\big(G/Z(G)\big) \cong Z^{(2)}/Z(G) = Z^{(2)}/Z^{(1)}$ è abeliano, e si procede così induttivamente. □

Esempio 7.1 : I gruppi S_3 e D_8 sono risolubili:

$$\begin{array}{ccc} S_3 & & D_8 \\ | & & | \\ A_3 & & \langle r \rangle \\ | & & | \\ 1 & & \langle r^2 \rangle \\ & & | \\ & & 1 \end{array} \tag{81}$$

7.2 Gruppi nilpotenti.

Definizione 7.6 : Un gruppo G si dice *nilpotente* se ammette una catena

$$G \geq H_1 \geq \cdots \geq H_r = 1 \tag{82}$$

tale che

- $H_i \trianglelefteq G$ per ogni $i = 1, \ldots, r$;
- $H_i/H_{i+1} \leq Z(G/H_{i+1})$ per ogni $i = 1, \ldots, r$;

Osservazione 18. Se G è abeliano, è nilpotente, e dunque è risolubile. Tutte le implicazioni sono strette: S_3 è risolubile ma non nilpotente ($A_3 \not\leq Z(S_3) = \langle 1 \rangle$); D_8 è nilpotente, non abeliano ($Z(D_8) = \langle r^2 \rangle$).

Corollario. I p gruppi finiti sono nilpotenti oltre che risolubili.

Teorema 7.5 : Sia G un gruppo finito. Allora sono equivalenti le due condizioni

- G è nilpotente;
- $G \cong \prod_{i=1}^{n} P_i$, dove P_i è un p_i-gruppo.

Dimostrazione. Omessa. □

Sia $H \trianglelefteq G$. Allora

- $H \leq Z(G)$ se e solo se $[H, G] = \langle 1 \rangle$;
- $H \trianglelefteq G$ se e solo se $[H, G] \leq H$.

Dimostrazione. Per il primo punto, $H \leq Z(G)$ se e solo se $hg = gh$ per ogni $g \in G$, ossia se e solo se $[h, g] = 1$ per ogni $h \in H, g \in G$.

Per il secondo punto, $H \trianglelefteq G$ implica che $ghg^{-1} \in H$, da cui $ghg^{-1}h^{-1} \in H$, da cui $[g, h] \in H$ per ogni g, h, dunque $[G, H] \leq H$. Il viceversa consiste nel percorrere a rovescio le implicazioni. □

Ricordiamo che che il *normalizzatore* di $H \leq G$ in G è definito da

$$N_G(H) := \{g \in G \mid g^{-1}Hg = H\} \tag{83}$$

(è lo stabilizzatore di H per l'azione naturale di coniugio sul reticolo dei sottogruppi di G). Il sottogruppo $N_G(H)$ è tale che $H \trianglelefteq N_G(H) \leq G$, ed è il massimo sottogruppo con tale proprietà.

Ora, se $H, K \leq G$ troviamo che

$$K \leq N_G(H) \iff [H, K] \leq H \tag{84}$$

Dimostrazione. Se $[H, K] \leq H$ allora $H \trianglelefteq K$, dunque per massimalità si conclude che $K \leq N_G(H)$. Viceversa se $k^{-1}hk \in H$ per ogni $k \in K$, $h \in H$ allora $[k, h] \in H$, dunque $[H, K] \leq H$. □

Ricordando la definizione di gruppo nilpotente, possiamo osservare che l'unica condizione $[H_i, G] \leq H_{i+1}$ sussume entrambe quelle date ($\{H_i \trianglelefteq G, H_i/H_{i+1} \leq Z(G/H_{i+1})\} \Leftarrow [H_i, G] \leq H_{i+1}$).

Proposizione 7.3. Sia G un gruppo nilpotente, ed $M \leq G$ un sottogruppo massimale di G. Allora

- $M \trianglelefteq G$;
- $|G : M| = p$, con p primo[3].

Dimostrazione. Facciamo seguire il risultato da due Lemmi di facile dimostrazione:

Lemma 7.1 : Se $K \trianglelefteq G$ ha indice primo in G, allora è massimale[4].

Lemma 7.2 : Se G è nilpotente, e $H \lneq G$, allora $H \lneq N_G(H)$.

Il primo è facile (basta ragionare con l'indice di K in G). Il secondo: se G ha una catena di sottogruppi

$$G = H_0 \geq H_1 \geq \cdots \geq H_r = 1 \tag{85}$$

tale che $[H_i, G] \leq H_{i+1}$, certamente $H \gneq H_0 = G$, e $H \geq H_r = 1$. Dunque esiste un minimo indice i tale che $H \not\geq H_i$ e $H \geq H_{i+1}$. Ora, $[H_i, H] \leq [H_i, G] \leq H_{i+1} \leq H$, da cui $H_i \leq N_G(H)$, e però $H_i \not\leq H$, dunque deve essere un sottogruppo proprio (esiste $h \in H \setminus H_i$ che normalizza comunque H). Da questo ricaviamo che[5]

- Se G è nilpotente, ed M massimale, allora M è un sottogruppo proprio del suo normalizzatore: per massimalità però deve essere $N_G(M) = G \iff M \trianglelefteq G$.
- Inoltre $G/M \neq \langle 1 \rangle$, e G/M non ha sottogruppi non banali, ed è finito. Dunque ha ordine primo. □

Quanto dimostrato nella nota sotto (gli indici di gruppi massimali non devono per forza essere primi) si generalizza come segue:

Esempio 7.2 : Per ogni $n > 1$ esistono G, H, con $H \leq G$ massimale e $|G : H| = n$.

Consideriamo $G = S_n$ e $H = \text{Stab}_G(n)$; è chiaro che $H \cong S_{n-1}$ e $|G : H| = \frac{n!}{(n-1)!} = n$. Resta da mostrare la massimalità: procediamo così.

[3] Può essere che $H \leq G$ sia massimale, senza che $|G : H|$ sia primo: $G = A_4 \leq S_4$, e $H = \langle (123) \rangle$ è massimale in A_4 ma ha indice 4.

[4] *Non vale il viceversa*: si prenda $H = \langle (123) \rangle \leq S_4$, è massimale in A_4, perché un eventuale gruppo intermedio $H \lneq K \lneq A_4$ dovrebbe avere ordine 6. Però non ci sono gruppi di ordine 6 in A_4 (questo ha 12 elementi, e contiene come sottogruppo proprio solo il gruppo di Klein, che ne ha 4. Allora H è massimale in A_4, e d'altra parte ha indice 4 in A_4.

[5] Da ciò deduciamo che S_3 non è nilpotente: troviamo un massimale $H \leq G$ che non è normale e coincide col proprio normalizzante. Questo contraddice il secondo Lemma e conclude. Vediamo che $H = \langle (12) \rangle$ ha queste proprietà; anzitutto è massimale perché ha indice primo in S_3, e non è normale perché non contiene tutti gli scambi ($(13)(12)(13) = (23) \notin H$). Quindi per massimalità $H = N_G(H)$.

Supponiamo che $H \lneq T \leq S_n$. In T c'è dunque una permutazione, τ, che non fissa n: $\tau(n) = j \neq n$.

Sia ora $\rho \in S_n$; distinguiamo vari casi

- Se $\rho(n) = n$, allora $\rho \in H$, dunque a fortiori $\rho \in T$.
- Se $\rho(n) = i \neq n$, distinguiamo a sua volta due casi:
  - Se $\rho(n) = i = j = \tau(n)$, allora $\tau^{-1}\rho \in H$, dunque in T; d'altra parte $\tau \in T$, dunque $\tau\tau^{-1}\rho = \rho \in T$.
  - Se $\rho(n) = i \neq j$, consideriamo $\tau^{-1}(ij)\rho$; tale permutazione sta in H, e allo stesso modo ci stanno τ e (ij) (fissa ovviamente n perché non compare nel 2-ciclo). Allora $\rho \in T$ con lo stesso ragionamento di prima.

In ogni caso, $S_n \leq T$, dunque devono essere uguali. □

8 Teorema Fondamentale dell'Algebra.

Rammentiamo due fatti;

- Se $f(X) \in \mathbb{R}[X]$ ha grado dispari, allora ha una radice reale: infatti se $f(z) = 0$ per $z \in \mathbb{C}$, allora $f(\bar{z}) = 0$. Dunque le radici di f si presentano a coppie $\{z, \bar{z}\}$; se però $\deg f$ è dispari deve esserci almeno una coppia che in realtà è un singoletto.
- Se $f(X) \in \mathbb{R}[X]$ ha grado due, allora ha una (e quindi due) radice complessa; il motivo è che il sistema

$$\begin{cases} z = a + ib \\ (u + iv)^2 = a + ib \end{cases} \qquad \begin{cases} u^2 - v^2 = a \\ 2uv = b \end{cases} \tag{86}$$

  ha sempre due soluzioni, eventualmente coincidenti, in (u, v).

Ora, il teorema fondamentale dell'algebra dice che il campo $\mathbb{C}$ è algebricamente chiuso, ossia ogni $f(X) \in \mathbb{C}[X]$ si fattorizza completamente in fattori lineari.

Dimostrazione. Supponiamo per assurdo che $f(X) \in \mathbb{C}[X]$ non abbia zeri complessi. Allora non li ha nemmeno $\bar{f}$. Dunque $g = f\bar{f} \in \mathbb{R}[X]$ non ha zeri complessi.

Sia ora $E = \text{Split}_{\mathbb{C}}(g)$: questo ha grado $|E : \mathbb{R}| = 2^m n$, con n dispari. Sia ora $G = \text{Gal}(E|\mathbb{R})$. Per il teorema di Sylow esiste un sottogruppo $S \trianglelefteq G$ di ordine 2^m. Ora, $|G/S| = n$ è dispari, dunque S corrisponde a $K|\mathbb{R}$, estensione di grado dispari. In tal senso esiste un polinomio $h(X) \in \mathbb{R}[X]$ irriducibile, tale che $K = \text{Split}(h)$: questo è assurdo, perché nessun polinomio di grado dispari è irriducibile su $\mathbb{R}$.

Allora $n = 1$, e $\text{Gal}(E|\mathbb{R}) = 2^m$. Per ipotesi di assurdo, $m > 1$; consideriamo $H_1 = \text{Gal}(E|\mathbb{C})$ e $H_2 \leq H_1$ massimale: $|H_2| = 2^{m-1}$, e $|H_1 : H_2| = 2$. Questo corrisponde a una estensione $\text{Fix}(H_2) = L|\mathbb{C}$ di grado 2, ossia esiste un polinomio di grado 2 irriducibile su $\mathbb{C}$, assurdo. □

9 Costruibilità con riga e compasso.

Diciamo *costruibile con riga e compasso* un numero(complesso) le cui coordinate stanno nel piano determinato a partire da due punti (che identificano una retta, che fa da asse delle ascisse: il compasso permette di costruire una retta ortogonale che fa da asse delle ordinate), che si può ottenere mediante intersezione di rette o circonferenze parimenti costruibili (le rette: come uniche linee per due punti già costruiti; le circonferenze: puntando il compasso in un punto già costruito, di raggio il segmento tra due punti già costruiti). Questo problema è intrinsecamente legato al problema delle estensioni di campi, dato che l'intersezione di luoghi geometrici è il problema algebrico della soluzione di sistemi non lineari di equazioni polinomiali.

- I numeri interi sono costruibili a partire da due punti nel piano e sono giustapposti in una retta.
- La somma, il prodotto e l'inverso di numeri costruibili è costruibile (si usano teoremi classici di geometria euclidea sulle proporzioni).
- $i = \sqrt{-1}$ è costruibile.

Il campo dei numeri costruibili è una estensione di $\mathbb{Q}(i)$, chiusa rispetto al coniugio ($a + ib$ costruibile implica che lo sia $a - ib$, perché $z = a + ib$ è costruibile se e solo se lo sono sia a che b).

Aggiungiamo all'insieme dei numeri costruibili tutti quelli che si ottengono mediante intersezione di rette che passano per punti già costruiti, e intersezioni di una circonferenza di centro un punto costruito e raggio il segmento OA verso un altro punto A costruito.

In questo secondo caso le coordinate dei punti della circonferenza possono non essere nel campo, ma in una sua estensione di grado 2.

Dunque un criterio di costruibilità è il seguente: $z \in \mathbb{C}$ è costruibile se e solo se $\mathbb{Q}(z) \subseteq K$, dove K è alla sommità di una torre di campi $Q = F_0 \leq F_1 \leq \cdots \leq F_r = K$, tale che $F_i = F_{i-1}(\beta_i)$, per β_i tale che $\beta_i^2 \in F_{i-1}$.

Dimostrazione. ($\Leftarrow$). Tutte le radici quadrate di numeri sono costruibili. ($\Rightarrow$). Segue dal ragionamento appena fatto (ovviamente questo è dovuto al fatto che vogliamo usare *coniche*: con curve di grado più elevato si possono costruire più cose). □

Osservazione 19. z costruibile $\iff \mathbb{Q}(z) \subseteq K = F(\beta_1, \ldots, \beta_r) \Rightarrow |\mathbb{Q}(z) : \mathbb{Q}|$ è una potenza di due.

Proposizione 9.1. Si consideri la torre di campi

$$F = F_0 \leq F_1 \leq \cdots \leq F_r \tag{87}$$

dove $F_i = F_{i-1}(b_i)$ e $b_i^{m_i} \in F_{i-1}$, per certi $m_i > 0$. Allora esiste un'altra torre di campi (generalmente un raffinamento, $s \geq r$)

$$F = L_0 \leq L_1 \leq \cdots \leq L_s \tag{88}$$

dello stesso tipo ($L_i = L_{i-1}(\gamma_i)$ e $\gamma_i^{n_i} \in L_{i-1}$, per certi $n_i > 0$), tale che L_s è normale su F, ed $n_i \in \{m_1, \ldots, m_r\}$

Dimostrazione. Sia $g_i = \min_F(b_i)$ e $K_i = \text{Split}_F\left(\prod_{l=1}^{i} g_l\right)$. Allora $K_r = \text{Split}_F(g_1 \ldots g_r)$; K_r è normale su F (ed è di Galois se i b_i sono separabili). Si ha la catena

$$F = K_0 \leq K_1 \leq \cdots \leq K_{i-1} \leq K_i \leq \cdots \leq K_r \tag{89}$$

$K_{i-1} = \text{Split}(g_1 \ldots g_{i-1})$, dunque $K_i = K_{i-1}(\beta_{i_1}, \ldots, \beta_{i_{t_i}})$, dove $b_i = \beta_{i_1}, \ldots, \beta_{i_{t_i}}$ sono gli zeri di $g_i(X)$. Ora,

$$K_{i-1} \leq K_{i-1}(\beta_{i_1}) \leq \cdots \leq K_{i-1}(\beta_{i_1}, \ldots, \beta_{i_{t_i}}) = K_i \tag{90}$$

è una torre di campi che raffina la precedente, $\beta_{i_1} = b_i$, $b_i^{m_i} \in F_{i-1} \leq K_{i-1}$ perché F_{i-1} si ottiene da F aggiungendo $b_1, \ldots, b_{i-1}$ e K_{i-1} li contiene.

Ora nella corrispondenza

$$\begin{array}{ccc} K_r & \xrightarrow{\phi} & K_r \\ | & & | \\ F(\beta_{i_2}) & \xrightarrow{\sigma} & F(b_i) \\ | & & | \\ F & \longrightarrow & F \end{array} \tag{91}$$

definiamo $\sigma\colon F(\beta_{i_2}) \to F(b_i)$ come la mappa che manda $\beta_{i_2} \mapsto b_i$; il polinomio che sto spezzando su K_r viene mandato in sè da σ, dunque esiste $\varphi\colon K_r \to K_r$ che estende quest'ultimo omomorfismo. Cosa fa tale φ su K_{i-1}? Potendo solo permutare le radici lo manda in sè stesso, e manda β_{i_2} in b_i. Dato che $\varphi(\beta_{i_2})^{m_i} = b_i^{m_i} \in K_{i-1}$, β_{i_2} sta in $\varphi^{-1}(K_{i-1}) = K_{i-1}$; lo stesso accade per le altre β_{i_k}, con lo stesso esponente m_i, e ripetendo questo ragionamento per ogni $1 \leq i \leq r$ la tesi segue (e implicitamente si è anche determinato un procedimento in cui s è una funzione esplicita di r e dei gradi di certi polinomi). □

Proposizione 9.2. $z \in \mathbb{C}$ è costruibile $\iff$ $E = \text{Split}(\min_{\mathbb{Q}}(z))$ ha grado 2^r su $\mathbb{Q}$ per qualche $r \geq 1$.

Dimostrazione. Se z è costruibile, $\mathbb{Q}(z) \subseteq F_r$ dove F_r è l'ultimo di una torre di campi $\mathbb{Q} = F_0 \leq F_1 \leq \cdots \leq F_r$ tale che $F_i = F_{i-1}(b_i)$, e $b_i^2 \in F_{i-1}$; per il risultato precedente ne esiste però anche una $\mathbb{Q} = L_0 \leq L_1 \leq \cdots \leq L_r$ tale che $L_r|\mathbb{Q}$ è di Galois (perché normale, grazie alla Proposizione precedente, e separabile, perché estendiamo campi perfetti) e $L_i = L_{i-1}(c_i)$, con $c_i^2 \in L_{i-1}$. Dunque L_r contiene tutte le radici di $\min_{\mathbb{Q}}(z)$. Dunque $E = \mathbb{Q}(\text{radici di } \min_{\mathbb{Q}}(z)) \subseteq L_r$ (contiene tutte le radici di tutti i polinomi minimi che ci sono serviti per costruire la torre). A questo punto $|L_r : \mathbb{Q}|$ è una potenza di 2, e d'altra parte per la formula dei gradi deve esserlo anche $|E : \mathbb{Q}|$.

Viceversa, se $|E : \mathbb{Q}| = 2^r$ è charo che $E|\mathbb{Q}$ è di Galois (è campo di spezzamento di un polinomio, ovviamente separabile su $\mathbb{Q}$). Dunque $|\operatorname{Gal}(E|\mathbb{Q})| = 2^r$ è un 2-gruppo; allora esiste una catena di sottogruppi

$$1 = G_0 \leq G_1 \leq \cdots \leq G_r = G \tag{92}$$

tale che $G_i \trianglelefteq G$ e $G_{i+1}/G_i \cong C_p$ (ciclico) per ogni $i = 0, \ldots, r$. Questa catena corrisponde, mediante l'aggiunzione di Galois, ad una catena di campi intermedi da $\mathbb{Q}$ (corrispondente a G) ad E (corrispondente ad $\langle 1 \rangle$), ognuno di grado due sul precedente:

$$\mathbb{Q} \leq F_{r-1} \leq \cdots \leq F_0 = E \tag{93}$$

dove $F_i = F_{i-1}(b_i)$, $b_i^2 \in F_{i-1}$, b_i^2 =discriminante di un polinomio in $F_{i-1}[X]$. Allora $\mathbb{Q}(z) \subseteq E$, campo che si ottiene mediante una torre di estensioni tale che…, dunque z è costruibile. □

Esempio 9.1 : Un controesempio: il fatto che $\operatorname{Split}_{\mathbb{Q}}(\min_{\mathbb{Q}}(z))$ abbia grado una potenza di due su $\mathbb{Q}$ non implica la costruibilità. Sia $E|\mathbb{Q}$ di Galois su $\mathbb{Q}$ e tale che $G = \operatorname{Gal}(E|\mathbb{Q}) \cong S_4$ (va provato che effettivamente *esiste* un tale E: è un'istanza del problema di Galois inverso). Allora $|E : \mathbb{Q}| = |S_4| = 4! = 24$; consideriamo l'azione naturale di G su $\{1, 2, 3, 4\}$, e il sottogruppo $S_3 \cong \operatorname{Stab}(4) \leq S_4$. Quest'ultimo è massimale in S_4 e corrisponde a $\operatorname{Fix}(S_3) = M \geq \mathbb{Q}$ estensione di grado 4. Ora, se $M = \mathbb{Q}(z)$ per qualche $z \in \mathbb{C}$ (cioè se M è semplice: questo va provato, e segue dal successivo *Teorema dell'elemento primitivo*), $|\mathbb{Q}(z) : \mathbb{Q}| = 4 = 2^2$.

Proviamo adesso che z non è costruibile.

E è separabile, dunque $E \leq \operatorname{Split}_{\mathbb{Q}}(\min(z)) = K$. $K \leq M = \operatorname{Fix}(S_3)$, dunque per aggiunzione $N = \operatorname{Gal}(E|K) \leq S_3$, ed $N \trianglelefteq G$ (corrisponde ad una estensione di Galois su $\mathbb{Q}$). Dunque $N \trianglelefteq G$ e $N \leq S_3 \cong \operatorname{Stab}(4)$; se usiamo la notazione H^σ per indicare $\sigma^{-1} H \sigma$ e osserviamo che $\operatorname{Stab}(4)^\sigma = \operatorname{Stab}(\sigma(4))$, abbiamo che $N^\sigma \leq \operatorname{Stab}(4)^\sigma$ per ogni $\sigma \in S_4$, dunque per normalità $N^\sigma = N \leq \bigcap_{k=1}^4 \operatorname{Stab}(k) = \langle 1 \rangle$; dunque $N = 1$, $K = E$. Ma $|E : \mathbb{Q}| = 24$ *non* è una potenza di due, dunque z non è costruibile.

Per quanto riguarda le due cose da precisare, della prima (esiste un'estensione di $\mathbb{Q}$ che ha gruppo di Galois S_4) sembra non preoccuparsi nessuno.

Per quanto riguarda la seconda vale il

Teorema 9.1 [DELL'ELEMENTO PRIMITIVO]**:** Sia $E = F(\alpha_1, \ldots, \alpha_n)$ dove tutti gli α_i *tranne al più uno* sono separabili, e tutti sono algebrici.

Allora $E \cong F(\gamma)$, per qualche γ algebrico su F.

Osservazione 20. Prima di dimostrare il risultato osserviamo che l'ipotesi in corsivo non è rimovibile. Sia $E = \mathbb{F}_p(u, v)$ con u, v algebricamente indipendenti su $\mathbb{F}_p$; allora possiamo considerare la torre di campi

$$F = \mathbb{F}_p(u^p, v^p) \leq F(u) \leq E \tag{94}$$

E si ottiene da F aggiungendo due elementi algebrici su F, dato che char $F = p$, u è radice di $X^p - u^p$, e v di $X^p - v^p$ (e i due polinomi sono irriducibili perché $u \notin F$ è l'unica radice). Dunque

$$|E : F(u)| = p = |F(u) : F| \tag{95}$$

$$|E : F| = |E : F(u)||F(u) : F| = p^2 \tag{96}$$

Nel suo campo di spezzamento, inoltre, $X^p - u^p = (X - u)^p$, dunque $E|F$ *non* è separabile. Ora, può essere $E = F(\gamma)$?

Supponiamo di sì: $\gamma = \frac{f(u,v)}{g(u,v)}$, per qualche $f, g \in \mathbb{F}_p[u, v]$ e $g \neq 0$. Si osservi anzitutto che $\gamma^p = \frac{f(u,v)^p}{g(u,v)^p} = \frac{f(u^p,v^p)}{g(u^p,v^p)} \in F$, dunque γ è radice di $X^p - \gamma^p$, dunque $|F(\gamma) : F| \leq p$. Si danno due casi ora:

- $\gamma \in F$, dunque $E = F$, assurdo.
- $\gamma \notin F$, dunque $|F(\gamma) : F| = p = |E : F| = p^2$, assurdo.

La morale è che in caratteristica p non sempre le estensioni algebriche sono semplici.

Osservazione 21. Posponiamo la dimostrazione ad altre due osservazioni preliminari:

- Se $K|F$ sono campi, ed $f, g \in F[X]$ vengono riguardati in $K[X]$ allora $\gcd(f, g)$ in $F[X]$ = $\gcd(f, g)$ in $K[X]$ (può sembrare banale ma sarà utile).
- Se F è un campo finito, $|E : F| < \infty$ implica che anche E è un campo finito. Ora però $E^\times$ è un gruppo ciclico, e la tesi del Teorema dell'elemento primitivo è vera per ogni γ generatore di $E^\times$. Dunque possiamo limitarci a provarlo per F campo infinito.

Dimostrazione. Ci limitiamo a provare che dati α, β F-alegbrici e β separabile, allora esiste γ F-algebrico tale che $F(\alpha, \beta) = F(\gamma)$; la tesi segue per induzione.

Sia $\Omega = \text{Split}_F(fg)$ dove $f = \min_F(\alpha), g = \min_F(\beta)$. Siano poi $\alpha = \alpha_1, \ldots, \alpha_r$ le radici di f, $\beta = \beta_1, \ldots, \beta_s$ le radici di g. Operiamo la

sostituzione $f(X) \mapsto f(v - uX)$ in modo che il polinomio così ottenuto abbia $\beta = \beta_1$ come *unica* radice in comune con g. Per farlo abbiamo 2 gradi di liberà nel definire u, v. Anzitutto deve essere $v = \alpha_1 + u\beta_1$, e $v \neq \alpha_i + u\beta_j$ per $j = 2, \ldots, s$, $i = 1, \ldots, r$. Ciò si traduce in $\alpha + u\beta = u\beta_j \neq \alpha_i$ per $j = 2, \ldots, s$, $i = 1, \ldots, r$, ossia

$$u \neq \tfrac{\alpha_i - \alpha}{\beta - \beta_j} \tag{97}$$

per $j = 2, \ldots, s$, $i = 1, \ldots, r$. Ci sono solo un numero finito di tali valori proibiti, dunque (supponendo, come possiamo fare, F infinito) esiste $c \in F$ diverso da tutti gli $\frac{\alpha_i - \alpha}{\beta - \beta_j}$. Ora, consideriamo $\gamma = \alpha + c\beta$: il polinomio $f(\gamma - cX)$ ha le proprietà richieste perché $f(\gamma - c\beta_1) = f(\alpha) = 0$, e non è zero per ogni altra β_j. Ora, è facile osservare che $F(\gamma) \subseteq F(\alpha, \beta)$. D'altra parte $\gcd(f(\gamma - cX), g(X)) = X - \beta$, per costruzione, e tale gcd coincide con quello in $F(\gamma)[X]$. Dunque $\beta \in F(\gamma)$ e $\alpha = \gamma - c\beta$ anche. Da questo si conclude. □

Osservazione 22. Se $\operatorname{char} F = 0$, il teorema appena dimostrato prende la forma

> Ogni estensione di grado finito di F è algebrica semplice.

10 Gruppo di Galois di un polinomio.

Sia $f(X) \in F[X]$ un polinomio separabile di grado positivo, ed $E = \operatorname{Split}_F(f(X))$. Ora, $E \cong F(\alpha_1, \ldots, \alpha_n)$, dove le α_i sono le radici di $f(X)$. È facile osservare che ogni $\sigma \in \operatorname{Gal}(E|F)$ agisce per permutazione sull'insieme $Z = \{\alpha_1, \ldots, \alpha_n\} \cong \{1, \ldots, n\}$ degli zeri di $f(X)$.

Dunque abbiamo un omomorfismo di gruppi $\theta\colon \operatorname{Gal}(E|F) \to S_n$, iniettivo perché le σ sono univocamente determinate dalla loro azione su Z), che dunque identifica $\operatorname{Gal}(E|F)$ ad un sottogruppo $H \leq S_n$ (ciò da cui segue $|\operatorname{Gal}(E|F)| < \infty$ per ogni estensione finita).

Definizione 10.1 : Il *gruppo di Galois* di $f(X) \in F[X]$ è l'immagine di $\operatorname{Gal}(\operatorname{Split}_F(f)|F)$ mediante $\theta\colon \sigma \mapsto \sigma|_Z$. Si denota con $\operatorname{Gal}_F(f)$.

Osservazione 23. Si osservi che

- $\operatorname{Gal}_F(f) \cong \operatorname{Gal}(E|F)$;
- $\operatorname{Gal}_F(f)$ è per definizione, il sottogruppo di S_n fatto dalle permutazioni delle radici che inducono F-automorfismi.

Esempio 10.1 : $\operatorname{Gal}_F(f)$ se $\operatorname{char} F \neq 2$, ed $f(X) = X^4 + aX^2 + b$ è biquadratico. Le radici di $f(X)$ sono $\{\pm u, \pm v\}$, dunque $\operatorname{Gal}_F(f) \leq S_4$;

questo segue dal fatto che per ogni $\sigma \in \mathrm{Gal}_F(f)$

$$\begin{cases} \sigma_1(u) = \pm u & \Rightarrow \sigma_1(-u) = \mp u \\ \sigma_2(v) = \pm v & \Rightarrow \sigma_2(-v) = \mp v \\ \sigma_3(u) = \pm v & \Rightarrow \sigma_3(-u) = \mp v \end{cases} \tag{98}$$

D'altra parte esistono altre permutazioni in S_4 (per esempio quella che manda $u \mapsto -v$, $-v \mapsto u$ e fissa il resto). Allora $\mathrm{Gal}_F(f)$ è un sottogruppo di D_8 (può avere al più otto elementi ottenuti combinando id, σ_i).

Il *criterio di Galois* per la risolubilità attraverso radicali di un polinomio è il seguente:

> Se $\mathrm{char}\, F = 0$, ed $f(X) \in F[X]$ di grado positivo n, f è *risolubile per radicali* se e solo se $\mathrm{Gal}_F(f)$ è un sottogruppo risolubile di S_n.

Definizione 10.2 : Diciamo che $f(X) \in F[X]$ è risolubile per radicali su F se esiste una torre di campi finita $F = F_0 \leq F_1 \leq \cdots \leq F_r$ tale che

- $F_i = F_{i-1}(b_i)$, per b_i tali che $b_i^{m_i} \in F_{i-1}$, $m_i \in \mathbb{Z}_>$;
- $\mathrm{Split}_F(f) \leq F_r$.

Osservazione 24. Se $\deg f \leq 4$ allora ogni $f(X)$ è risolubile per radicali, perché $\mathrm{Gal}_F(f) \leq S_4$ è sottogruppo di un gruppo risolubile, dunque è risolubile. Nulla si può dire per $n \geq 5$, perché non si sa se i $\mathrm{Gal}(E|F)$ si possono tutti realizzare come gruppi di permutazioni S_n.

Dimostrazione. Trattiamo l'implicazione $(\Rightarrow)$.

Se esiste la torre di campi in oggetto, si può supporre che $F_r|F$ sia di Galois (la torre si può sostituire con una analoga dove F_r è normale, la separabilità segue dal fatto che $\mathrm{char}\, F = 0$). Sia ora $n = \mathrm{lcm}\{m_1, \ldots, m_r\}$, e $\Omega = F_r(\zeta)$, dove ζ è una radice n-esima primitiva dell'unità. $\Omega|F$ è di Galois, perché se $g(X)$ è il polinomio tale che $F_r = \mathrm{Split}_F(g(X))$, si ha $\Omega = \mathrm{Split}_F(g(X)(X^n - 1))$. Allora $\mathrm{Gal}(E|F) \cong \frac{\mathrm{Gal}(\Omega|F)}{\mathrm{Gal}(\Omega|E)}$: nel diagramma

$$\begin{array}{ccc} \Omega & \longrightarrow & 1 \\ | & & | \\ E & \longrightarrow & \mathrm{Gal}(\Omega|E) \\ | & & | \triangle \\ F & \longrightarrow & \mathrm{Gal}(\Omega|F) \end{array} \tag{99}$$

Ora, quozienti di gruppi risolubili sono risolubili, dunque basta mostrare che $\mathrm{Gal}(\Omega|F)$ è risolubile. Siano adesso

$$K_0 = F(\zeta) \tag{100}$$
$$K_1 = K_0(b_1), \dots, K_i = K_{i-1}(b_i) \tag{101}$$
$$(K_1 \cong F(b_i)), \dots, (K_i \cong F_i(\zeta)) \tag{102}$$

questa è una torre di campi da $F(\zeta)$ a Ω tale che $b_i^{m_i} \in F_{i-1} \subseteq K_{i-1}$; ogni campo è di Galois sull'antecedente, dato che $F(\zeta)|F$ è di Galois (e $\mathrm{Gal}(F(\zeta)|F)$ è abeliano) e K_{i-1} contiene sia $b_i^{m_i}$ che tutte le radici m_i-esime di 1, e K_i è perciò il campo di spezzamento di $X^{m_i} - b_i^{m_i}$ su K_{i-1}.

La corrispondenza di Galois porge perciò una catena

$$\mathrm{Gal}(\Omega|F) \geq H_0 \geq H_1 \geq \cdots \geq H_r = 1 \tag{103}$$

tale che $H_0 \trianglelefteq \mathrm{Gal}(\Omega|F)$, perché $F(\zeta)|F$ è di Galois, e $H_i \trianglelefteq H_{i-1}$ (perché $K_i|K_{i-1}$ è di Galois). Ora, il quoziente H_{i-1}/H_i è ciclico, dunque abeliano, e $\mathrm{Gal}(F(\zeta)|F) \cong \mathrm{Gal}(\Omega|F)/H_0$ anche. Dunque $\mathrm{Gal}(\Omega|F)$ è risolubile.

Consideriamo l'implicazione inversa.

Sia $G = \mathrm{Gal}(E|F) \cong \mathrm{Gal}_F(f)$ risolubile, $|G| = n = |E : F|$. Sia ζ una radice n-esima primitiva di 1, e consideriamo $\Omega = E(\zeta)$, $F' = F(\zeta)$: $\Omega \cong \mathrm{Split}_{F'}(f)$. Sia ora $\sigma \in \mathrm{Gal}(\Omega|F') \leq \mathrm{Gal}(\Omega|F)$, e allora $\sigma(E) = E$ (perché $E|F$ è un'estensione intermedia e di Galois). Dunque $\sigma|_E \in \mathrm{Aut}(E)$, e ogni tale automorfismo fissa F (perché ne fissa un sovracampo). Consideriamo allora la mappa di restrizione

$$\mathrm{Gal}(\Omega|F') \to \mathrm{Gal}(E|F). \tag{104}$$

Questo è iniettivo (se $\sigma|_E = \mathrm{id}_E$, σ era già id_Ω).

Ora $\mathrm{Gal}(\Omega|F')$ si identifica ad un sottogruppo di un gruppo risolubile, ed è perciò esso stesso risolubile. Il suo ordine deve dividere n (Lagrange). Ora, deve esistere una catena

$$\mathrm{Gal}(\Omega|F') = H_0 \geq H_1 \geq \cdots \geq H_r = 1 \tag{105}$$

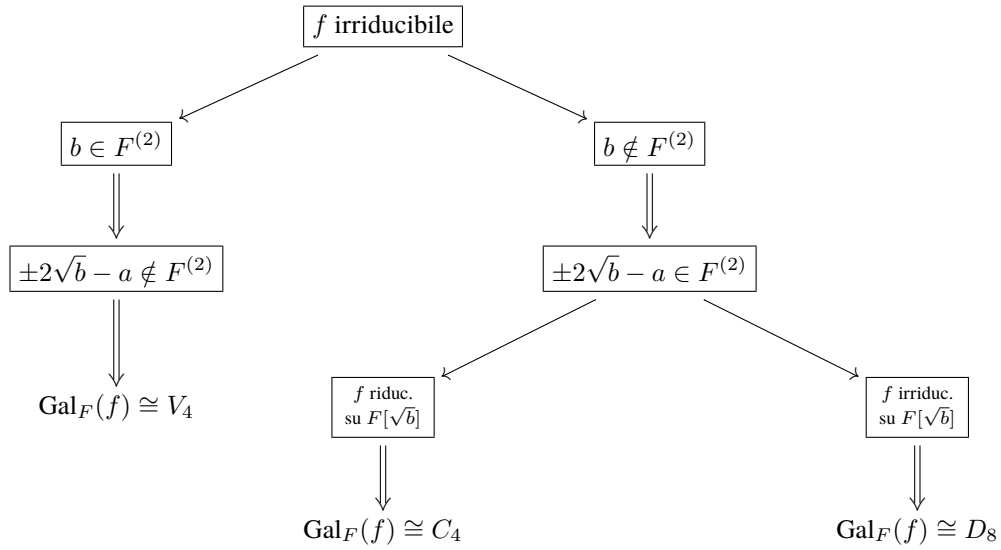
con ogni sottogruppo normale nel precedente e quozienti tutti ciclici (dato che $\mathrm{Gal}(\Omega|F')$ è finito e risolubile). A questa catena corrisponde una torre di campi, mediante l'aggiunzione di Galois, della forma $\Omega \geq K_1 \geq \cdots \geq F'$ dove ogni estensione è di Galois sulla precedente, e $\mathrm{Gal}(K_i/K_{i-1})$ ciclico di ordine m_i che divide n. $K_i (\leq F')$ contiene perciò le radici n-esime di 1, e dunque $K_i \cong K_{i-1}(b_i)$ dove $b_i^{m_i} \in K_{i-1}$[6]; allora Ω si ottiene da F aggiungendo radici, e questo campo contiene E: f è quindi risolubile per radicali. □

[6] Questo fatto segue dal Satz 90 di Hilbert, dimostrato a pagina 38. Per non spezzare la dimostrazione a metà l'ho messo comunque qui

Esempio 10.2 : Consideriamo il polinomio biquadratico $f(X) = X^4 + aX^2 + b$, pensato a coefficienti in un campo di caratteristica zero o dispari. Ciò che ci proponiamo di dimostrare è quanto raccolto nel diagramma seguente

$$f \text{ riduc.} \iff f(X) = (X^2 - u^2)(X^2 - v^2) \tag{106}$$

$$\iff (a^2 - 4b \in F^{(2)}) \vee (b, \pm 2\sqrt{b} - a \in F^{(2)}) \tag{107}$$



Andiamo con ordine: anzitutto è evidente che (data la parità della funzione polinomiale f) $f(u) = 0 \iff f(-u) = 0$. Col ché se f è riducibile ed u è una radice di f, $X^2 - u^2 \mid f(X)$, dunque f ammette un fattore di grado due, e ovviamente anche il viceversa è vero (se f ammette un fattore di grado due è riducibile).

Supponiamo quindi $f(X) = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta)$. Aprendo i prodotti otteniamo il sistema (non lineare)

$$\begin{cases} \gamma + \alpha = 0 \\ \beta\delta = b \\ \delta + \beta + \alpha\gamma = a \\ \alpha\delta + \beta\gamma = 0 \end{cases} \tag{108}$$

da cui si ricava che deve essere $\gamma = -\alpha$ e $\alpha(\delta - \beta) = 0$; ora,

- se $\alpha = \gamma = 0$ si ha $f(X) = (X^2 + \beta)(X^2 + \delta)$; questo accade precisamente quando il discriminante di $f(t) = f(X^2) = t^2 + at + b$, $\Delta = a^2 - 4b$, è un quadrato in F (infatti $\Delta = (\delta - \beta)^2$.
- se $\alpha \neq 0$ e $\beta = \delta$ allora $b = \beta^2$ è un quadrato in F, e dalla terza equazione anche $\pm 2\sqrt{b} - a = \alpha^2$ lo è.

Questo esaurisce i primi due punti.

Supponiamo da ora in poi $f(X)$ *irriducibile* su F.

- Se b è un quadrato in F non lo è $\pm 2\sqrt{b} - a$, e poiché $b = (uv)^2$, ne segue che uv deve stare in F. Alla luce di questo ogni $\sigma \in \mathrm{Gal}_F(f)$ deve mandare uv in sè; vogliamo provare che questo implica che $\mathrm{Gal}_F(f) \cong V_4$.

  - $\sigma\colon u \mapsto u$, allora $uv = \sigma(uv) = \sigma(u)\sigma(v) = u\sigma(v)$, e da ciò $\sigma(v) = v$;
  - $\sigma\colon u \mapsto -u$, allora $uv = \sigma(uv) = \sigma(u)\sigma(v) = -u\sigma(v)$, e da ciò $\sigma(v) = -v$;
  - $\sigma\colon u \mapsto v$, allora $uv = \sigma(uv) = \sigma(u)\sigma(v) = v\sigma(v)$, e da ciò $\sigma(v) = u$;
  - $\sigma\colon u \mapsto -v$, allora $uv = \sigma(uv) = \sigma(u)\sigma(v) = -v\sigma(v)$, e da ciò $\sigma(v) = -u$.

  Non vi sono altre possibilità per $\sigma \in \mathrm{Gal}_F(f)$. Segue la tesi.

- Supponiamo adesso che b *non* sia un quadrato in F. Osserviamo che sotto tali ipotesi $\pm 2\sqrt{b} - a$ non è un quadrato in $F[\sqrt{b}]$[7]. Chiaramente $b = \left(\sqrt{b}\right)^2$ è un quadrato in $F[\sqrt{b}]$.

  Dividiamo due sottocasi

  - Se $f(X)$ è riducibile su $F' = F[\sqrt{b}]$, allora $a^2 - 4b$ è un quadrato in F', dunque

    $$a^2 - 4b = (\alpha + \beta\sqrt{b}) = \alpha^2 + 2\alpha\beta + \beta^2 b \qquad (109)$$

    dunque deve essere $\alpha\beta = 0$; se $\alpha = 0$, $b(a^2 - 4b) = (\beta b)^2$ è un quadrato in F; il caso $\beta = 0$ porta a un assurdo. In $F'[X]$ $f(X)$ si fattorizza come $(X^2 - u^2)(X^2 - v^2)$; col che $u^2, v^2, uv = \sqrt{b} \in F'$; allora $E = F'(u)$ ha grado 2 su F', e per la formula dei gradi $|E : F| = 4$.

    A questo punto esiste certamente $\varphi_0\colon F' \to F'\colon \sqrt{b} \mapsto -\sqrt{b}$,che si estende ad una $\sigma\colon E \to E$. Tale σ deve mandare $X^2 - u^2$ in $X^2 - v^2$ (perché deve mandare $u^2 = x + \sqrt{b}y$ in $x - \sqrt{b}y \neq u^2$, e quella è l'unica possibilità se deve andare in un altro divisore del polinomio di partenza). Ora, gli unici casi possibili sono $\sigma_\pm(u) = \pm v$: entrambi questi elementi sono generatori di $\mathrm{Gal}_F(f)$ che hanno periodo 4, ergo $\mathrm{Gal}_F(f)$ è il ciclico.

[7] Infatti se lo fosse, $(s + \sqrt{b}t)^2 = \pm 2\sqrt{b} - a$, dopo qualche conto sarebbe $s^4 + as^2 + b = 0$, assurdo per l'irriducibilità di $f(X)$ su F.

– Se $f(X)$ non è riducibile su $F' = F[\sqrt{b}]$, allora $|E : F'| = 4$, perché $\min_{F'}(u) = f(X)$ per qualsiasi radice di f in E. Dunque $|E : F| = 8$, quindi $\mathrm{Gal}_F(f) \cong D_8$ (sappiamo che deve essere un sottogruppo di D_8)

Questo conclude la discussione.

Intermezzo: Questioni di costruibilità. Un n-agono regolare è costruibile se e solo se risulta costruibile ζ, una radice n-esima primitiva dell'unità, ovvero se e solo se $\mathrm{Split}_{\mathbb{Q}}(\zeta)$ ha grado 2^r su $\mathbb{Q}$. Questo accade se e solo se $|\mathbb{Q}(\zeta) : \mathbb{Q}| = 2^r$, ovvero se e solo se $\deg \Phi_n(X) = \phi(n) = 2^r$.

Il problema della costruibilità di un n-agono risulta quindi collegato intimamente a proprietà aritmetiche dell'intero n; in particolare se $n = \prod p_i^{m_i}$ allora $\phi(n) = \prod (p_i - 1) p_i^{m_i - 1}$ è una potenza di due se e solo se tutti i fattori primi dispari hanno esponente 1, e ogni $p_i - 1$ è una potenza di 2, ossia $p_i = 2^{k_i} + 1$ per ogni $i = 1, \ldots, t$; questi primi si dicono *primi di Fermat*: è noto che k_i deve essere a sua volta una potenza di due[8]. Dunque un n-agono regolare è costruibile se e solo se i primi dispari che compaiono nella sua fattorizzazione sono primi di Fermat distinti, ossia

$$n = 2^k p_1 \ldots p_t \tag{110}$$

ove $p_i = 2^{2^{w_i}} + 1$ (si ricordi che *non* tutti i numeri di questa forma sono primi: si prenda $2^{2^5} + 1 = 6700417 \cdot 641$).

Esempio 10.3 : Troviamo un polinomio di grado p primo che ha per gruppo di Galois S_p. Per $p = 3$ si è già visto che va bene $X^3 - 2$; per $p \geq 5$ procediamo come segue.

Costruiamo un polinomio di grado $p \geq 5$ che ha esattamente $p-2$ radici reali e 2 complesse coniugate: prendiamo $g(X) = (X^2 + m) \prod_{i=1}^{p-2} (X - a_i)$, dove $m, a_i \in 2\mathbb{Z}$, tutti positivi e diversi tra loro. Questo polinomio non è irriducibile, quindi non è quello che cerchiamo. Ha però radici semplici, il che equivale a dire che se $g'(\alpha) = 0$, $g(\alpha) \neq 0$. Sia allora

$$\epsilon = \min\{|g(x)| \mid g'(x) = 0\} \tag{111}$$

(il minimo è fatto su un insieme finito di razionali). Dato che se se $g'(\alpha) = 0$, $g(\alpha) \neq 0$ possiamo pensare che nella striscia di semiampiezza ϵ non cadano zeri di g. Prendiamo ora $h(X) = g(X) - \frac{2}{n}$, dove n è dispari e determinato dalla condizione $\frac{2}{n} < \epsilon$: "spostando" il polinomio di una quota minore di ϵ non perdiamo nè aggiungiamo zeri reali, quindi anche h ne ha $p - 2$ reali e 2 complesse coniugate.

Ora $f(X) = nh(X) = ng(X) - 2$ ha $p - 2$ radici reali, 2 complesse coniugate, e coefficienti interi. Se $f(X) = nX^p + \ldots$, tutti gli altri coefficienti tranne il termine noto sono divisibili per 4; 4 divide b_0 (il termine

[8] Altrimenti se $k = dr$ con d dispari, $2^k + 1$ si fattorizza come $(2^r + 1) \sum_{j=0}^{d-1} 2^{rj}$.

noto di $g(X)$), quindi $nb_0 - 2$ non è divisibile per 4. Per il criterio di Eisenstein $f(X)$ è irriducibile su $\mathbb{Z}$; il lemma di Gauss implica che lo sia anche su $\mathbb{Q}$.

Resta da provare che $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_p$. Sia $G \leq S_p$; mostriamo che se G contiene un p-ciclo e uno scambio, allora $G = S_p$.

Sia $\sigma \in G$ il p-ciclo, consideriamo $H = \langle\sigma\rangle \leq G$, questo è un sottogruppo fatto da p-cicli; in particolare si può pensare che contenga $(12\dots p)$[9]. A questo punto lo scambio si può supporre essere (12); si osservi ora che $\sigma^i(12)\sigma^{-i} = (\sigma^i(1)\sigma^i(2)) = (i{+}1, i{+}2)$, per ogni $i \geq 1$. Dunque G contiene $(12), (23), \dots, (p-1, p)$. Ora, è facile vedere che $(1j) = (2j)(12)(2j)$, dunque G contiene anche $(13), (14), \dots, (1p), (24), (25), \dots$

Da ultimo si osservi che $(ij) = (1j)(1i)(1j)$, dunque G contiene tutti gli scambi; ma ora è ben noto che $\langle\text{scambi}\rangle \cong S_p$.

Ora, se $E = \mathrm{Split}_{\mathbb{Q}}(f)$, e α è una radice di f in E, $p = \deg f(X) = |\mathbb{Q}(\alpha) : \mathbb{Q}| \mid |E : \mathbb{Q}| = |\mathrm{Gal}(E|\mathbb{Q})| = \mathrm{Gal}_{\mathbb{Q}}(f)$. Inoltre è evidente che $E \cong \mathbb{Q}(\alpha_1, \dots, \alpha_{p-2}, z, \bar{z})$. Se prendiamo il coniugio su $\mathbb{C}$ otteniamo un automorfismo di E che fissa tutte le α_i e scambia $z \mapsto \bar{z}$; questo è lo scambio in S_p.

Poi, siccome $p \mid |\mathrm{Gal}_{\mathbb{Q}}(f)|$, per il teorema di Sylow $\mathrm{Gal}_{\mathbb{Q}}(f)$ contiene un sottogruppo di ordine p (infatti p divide *esattamente* $p!$, e per il teorema di Cauchy contiene anche un elemento di ordine p, ossia un p-ciclo: si conclude.

Un esempio numerico conclude davvero: sia $g(X) = (X^2 + 2)(X - 4)(X - 6)(X - 8)$. Allora $\epsilon \simeq 81$ e va bene $n = 1$; $f(X) = g(X) - 2$ è irriducibile su $\mathbb{Q}$ e ha per gruppo di Galois S_5, che non è risolubile.

Esempio 10.4 : Osserviamo che se n non è primo, esistono sottogruppi di S_n che contengono un ciclo e una trasposizione ma che non coincidono con S_n: si prenda $n = 6$, (12) e il 6-ciclo (123456).

11 Un po' di rappresentazione.

11.1 Teoria di base: caratteri, cocicli e coomologia.

Teorema 11.1 [INDIPENDENZA DEI CARATTERI DI DEDEKIND]**:** Sia G un gruppo, F un campo, $\chi_1 \dots, \chi_m \colon G \to F^\times$ omomorfismi *distinti*. Allora $\chi_1 \dots, \chi_m$ sono linearmente indipendenti come vettori di $F^G = \hom(G, F)$.

Osservazione 25. La struttura di spazio vettoriale su F^G è quella ovvia data puntualmente. Osserviamo che nessuna delle χ_i è una funzione suriettiva. Da ultimo, non è essenziale che G sia un gruppo: il teorema vale anche nel caso di F^M per un qualsiasi monoide M.

[9] A meno di riordinare σ, si può pensare che cominci da 1: $\sigma = (1\sigma(1)\dots)$. Ovviamente esiste k tale che $\sigma^k(1) = 2$, e questo è ancora un p-ciclo (*solo perché p è primo!*); quindi in $\langle\sigma\rangle$ c'è una permutazione $(12\sigma^k(2)\dots)$; si ripete il ragionamento fino a trovare $(123\dots p)$.

Dimostrazione. Ragioniamo per induzione: la base è ovvia $\chi = \chi_1$ non è la funzione costantemente zero perché, per esempio $\chi(1_G) = 1_F$.

Per $m > 1$, supponiamo che $\sum c_i\chi_i = 0$, cioè $\sum c_i\chi_i(x) = 0$ per ogni x. Possiamo supporre, dato che le χ_i sono distinte, che esista $g \in G$ tale che $\chi_1(g) - \chi_2(g)neq0$. Allora $\sum c_i\chi_i(gx) = \sum c_i\chi_i(g)\chi_i(x) = 0$ e d'altra parte $\chi_1(g)\sum c_i\chi_i(x) = 0$; sottraendo queste ultime due quantità otteniamo

$$\sum_{i=2}^{m} a_i\chi_i(x) = 0 \tag{112}$$

per ogni $x \in G$, dove $a_i = c_i(\chi_1(g) - \chi_2(g))$. Ne segue che per ipotesi induttiva $a_i = 0$, in particolare $a_2 = c_2 s = 0$, con $s \neq 0$. Questo implica che $c_2 = 0$, dunque

$$\sum_{i\neq2} c_i\chi_i(x) = 0 \tag{113}$$

da cui si conclude, ancora per ipotesi induttiva. □

Ricordiamo ora che un G-*modulo* consiste nel dato di (equivalentemente)

- Un gruppo abeliano denotato additivamente e una funzione $\cdot\colon G \times M \to M$ tale che
  - $g_1 \cdot (g_2 \cdot m) = (g_1 g_2) \cdot m$, per ogni $g_1, g_2 \in G, m \in M$;
  - $1 \cdot m = m$ per ogni $m \in M$;
  - $g \cdot (m + n) = g \cdot m + g \cdot n$, per ogni $g \in G$, $m, n \in M$.
- Un gruppo abeliano M denotato additivamente e un omomorfismo di monoidi $G \to \mathrm{End}(M)$ (la cui immagine è un sottomonoide di $\mathrm{Aut}(M)$).
- Un $\mathbb{Z}[G]$-modulo M, dove $\mathbb{Z}[G]$ è l'*anello gruppale* di G.

L'idea è la stessa della teoria della rappresentazione.

Osservazione 26. Sia $E|F$ una estensione di campi. Se E è di Galois su F, allora sia $(E, +)$ che $(E^\times, \cdot)$ sono $\mathrm{Gal}(E|F)$-moduli.

Definizione 11.1 : Sia M un G-modulo. Una *derivazione*, o *omomorfismo crociato*, o *1-cociclo* è una funzionee $f\colon G \to M$ tale che $f(\sigma\tau) = f(\sigma) + \sigma \cdot f(\tau)$.

Osservazione 27. Le derivazioni formano un gruppo abeliano (e se M è un R-modulo, un R-modulo) con le ovvie definizioni puntuali, denotato $\mathrm{Der}(G, M)$.

Osservazione 28. Se $f \in \mathrm{Der}(G, M)$, allora $f(1) = 0$: infatti $f(1) = f(1) + 1 \cdot f(1) = 2f(1)$.

Fissiamo $a \in M$ e definiamo una derivazione $f\colon G \to M$ ponendo $f_a\colon G \to M\colon \sigma \mapsto \sigma(a) - a$. La verifica che f_a è una derivazione è immediata: l'insieme delle derivazioni della forma f_a per $a \in M$ forma un sottogruppo di $\mathrm{Der}(G, M)$, che si chiama sottogruppo delle *derivazioni interne*, od *omomorfismi crociati principali*, od *1-cobordi*, denotato $\mathrm{Der}_I(G, M)$.

Il quoziente

$$\frac{\mathrm{Der}(G,M)}{\mathrm{Der}_I(G,M)} =: H^1(G, M) \tag{114}$$

prende il nome di primo gruppo di coomologia di G in M.

Osservazione 29. Sia G un gruppo ciclico finito, di ordine n, ed $\eta \in G$ un suo generatore.

Sia $f\colon G \to M$ una derivazione e sia $f(\eta) = a \in M$. Se conosciamo $f(\eta)$ possiamo determinare f: infatti è facile notare che $f(\eta^2) = a + \eta \cdot a$, e in generale $f(\eta^i) = a + \eta \cdot a + \ldots \eta^{i-1} \cdot a$; in particolare, $0 = f(1) = f(\eta^n) = a + \eta \cdot a + \cdots + \eta^{n-1} \cdot a$; dunque $\sum \eta^k \cdot a = 0$ (leggasi: a non si può scegliere in modo qualunque).

Viceversa, se $a \in M$ soddisfa $\sum \eta^k \cdot a = 0$ allora esiste $f \in \mathrm{Der}(G, M)$ tale che $f(\eta) = a$.

Va controllato che questa è effettivamente una derivazione, ossia che $f(\eta^1\eta^j) = f(\eta^i) + \eta^i \cdot f(\eta^j)$; se $i + j \leq n$ questo segue dal fatto che

$$\begin{aligned} f(\eta^i\eta^j) &= f(\eta^{i+j}) && (115)\\ &= a + \eta \cdot a + \cdots + \eta^{i-1}a + \eta^i(a + \cdots + \eta^{j-1} \cdot a) && (116)\\ &= f(\eta^i) + \eta^i \cdot f(\eta^j) && (117) \end{aligned}$$

e se $i + j > n$, sia $\ell = \lfloor \frac{i+j}{n} \rfloor$. Allora

$$\begin{aligned} f(\eta^i\eta^j) &= f(\eta^{i+j-n\ell}) && (118)\\ &= a + \eta \cdot a + \cdots + \eta^{i+j-n\ell-1} \cdot a + \\ &+ \eta^{i+j-n\ell}(a + \cdots + \eta^{n\ell-1} \cdot a) && (119)\\ &= a + \eta \cdot a + \cdots + \eta^{i+j-n\ell-1} \cdot a && (120)\\ &= \eta^{n\ell} \cdot (a + \eta \cdot a + \cdots + \eta^{i+j-n-1} \cdot a) && (121)\\ &= a + \eta \cdot a + \cdots + \eta^{i+j-1} \cdot a && (122)\\ &= f(\eta^i) + \eta^i \cdot f(\eta^j) && (123) \end{aligned}$$

Da ultimo è evidente che se h, k sono congrui modulo n, ossia se $h = pn+k$ per $p \in \mathbb{Z}$, allora $f(\eta^h) = f(\eta^k)$, dunque f è ben definita.

Ci chiediamo ora per quali scelte di $a = f(\eta)$ la derivazione ottenuta è interna.

Deve essere $f)b(\sigma) = \sigma \cdot b - b$, per ogni $\sigma \in G$. Allora

> f è una derivazione interna se e solo se $a = f(\eta) = \eta \cdot b - b$ per qualche $b \in M$.

11.2 Nöther e Hilbert.

Teorema 11.2 [NÖTHER]**:** Sia $E|F$ di Galois, e riguardiamo $M = E^\times$ come $G = \text{Gal}(E|F)$-modulo. Allora $\text{Der}(G, M) = \text{Der}_I(G, M)$, ossia $H^1(G, M) \cong 0$.

Dimostrazione. Sia $f\colon G \to E^\times$ una derivazione; essa è interna se e solo se $f(\sigma) = \sigma(\gamma)\gamma^{-1}$, per qualche $\gamma \in E^\times$.

Consideriamo $\sum_{\tau\in G} f(\tau)\tau\colon E \to E$; mostriamo che questa non è la mappa zero. Anzitutto, se $u \neq 0$ tutti i $\tau(u)$ sono diversi da zero (sono automorfismi di E). Dunque $\{\tau\colon E^\times \to E^\times\}$ al variare di $\tau \in \text{Gal}(E|F)$ è un insieme finito di automorfismi, che per Dedekind sono linearmente indipendenti su E; se $\sum_{\tau\in G} f(\tau)\tau$ è zero, tutti gli $f(\tau)$ sono zero, e così lo è f. In caso contrario esiste almeno un $\alpha \in E$ tale che $\beta = \sum_{\tau\in G} f(\tau)\tau(\alpha) \neq 0$.

Calcoliamo ora $\sigma(\beta)$:

$$\sigma(\beta) = \sigma\left(\sum f(\tau)\tau(\alpha)\right) \tag{124}$$

$$= \sum_{\tau\in G} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau(\alpha) \tag{125}$$

$$= f(\sigma)^{-1} \sum_{\rho\in G} f(\rho)\rho(\alpha) \tag{126}$$

$$= f(\sigma)^{-1}\beta \tag{127}$$

Ora, se $\sigma(\beta) = f(\sigma)^{-1}\beta$, si ha $f(\sigma) = \sigma(\beta)^{-1}\beta = \sigma(\beta^{-1})\beta$ e ponendo $\gamma = \beta^{-1}$ si conclude. □

Definizione 11.2 : Sia $E|F$ di Galois, $G = \text{Gal}(E|F)$. Sia $a \in E$, definiamo la *norma* di a come

$$N(a) = \textstyle\prod_{\sigma\in G} \sigma(a) \tag{128}$$

Osservazione 30. Su $\mathbb{C}|\mathbb{R}$, $N(z) = z\bar{z} = |z|^2$.

Si osservi anche che $N(a) = 0 \iff a = 0$, e che $N(ab) = N(a)N(b)$; ci chiediamo chi sono gli elementi $z \in E$ tali che $N(z) = 1$.

Supponiamo G ciclico con n elementi. Per ogni $b \in E^\times$ si ha, allora, $N\left(\frac{\eta(b)}{b}\right) = \frac{N(\eta(b))}{N(b)} = \frac{N(b)}{N(b)} = 1$, e d'altra parte è vero il viceversa.

Teorema 11.3 [SATZ 90]**:** Sia $\text{Gal}(E|F) = \langle\eta\rangle$ per campi $E|F$; allora $N(z) = 1 \iff z = \eta(b)/b$ per qualche $b \neq 0$.

Dimostrazione. Un verso è stato appena fatto. Se $1 = N(a) = \prod_{k=0}^{n-1} \eta^k(a)$, ricordando quanto è stato detto prima in notazione additiva, sappiamo che gli $a \in E$ tali che $f(\eta) = a$ per qualche $f \in \text{Der}(G, M)$ sono tutti e soli quelli tali che $a + \eta \cdot a + \cdots + \eta^{n-1} \cdot a = 0$. Da ciò sappiamo che esiste

una $f\colon \mathrm{Gal}(E|F) \to E^\times$ tale che $f(\eta) = a$, e in questa situazione ogni derivazione è interna: dunque $f = f_b\colon \sigma \mapsto \sigma(b)/b$. Quindi $a = f_b(\eta) = \eta(b)/b$. □

Proposizione 11.1. Sia E un'estensione di Galois di F di grado n, ed F contenga n radici n-esime dell'unità. Se $\mathrm{Gal}(E|F)$ è ciclico, allora $E = F(b)$, dove $b^n \in F$.

Dimostrazione. Sia ζ una radice n-esima primitiva di 1. Allora $1 = \zeta^n = N(\zeta)$, infatti $N(\zeta) = \prod \sigma(\zeta)$, ma $\sigma|_F = \mathrm{id}$, dunque $\prod \sigma(\zeta) = \prod \zeta = \zeta^n$. Per il Satz 90 di Hilbert allora, se $\mathrm{Gal}(E|F) \cong C_n$ $\zeta = \eta(b)/b$ per qualche $b \in E^\times$.

Dunque $\eta(b) = b\zeta$, e allora $\eta(b^n) = \eta(b)^n = b^n\zeta^n = b^n$, dunque $\eta^i(b^n) = b^n$ per ogni $i \geq 1$, dunque $b^n \in \mathrm{Fix}(\mathrm{Gal}(E|F)) = F$.

Ora, $\eta^2(b) = b\zeta^2$, e per induzione $\eta^i(b) = b\zeta^i$, dunque $\eta^i(b) = b \iff n \mid i \iff \eta^i = \mathrm{id}_E$, quindi $\mathrm{Gal}(E|F(b)) = \langle 1\rangle$, da cui $E \cong F(b)$. □

Transitività e irriducibilità. Ricordiamo che se G agisce su un insieme X, l'*orbita* di $x \in X$ è l'insieme $Gx = \{gx \mid g \in G\}$. In caso ci sia una sola orbita, l'azione si dice *transitiva*. In caso $G = S_n$ per qualche n, un sottogruppo $H \leq S_n$ si dice *transitivo* se l'azione naturale di H su S_n è transitiva (non tutti i gruppi sono transitivi: si prenda $\{(2), (34), (12)(34), \mathrm{id}\} \cong V_4 \leq S_4$).

Dato che $\mathrm{Gal}_F(f) \leq S_n$ è naturale chiedersi se questo sia un gruppo transitivo rispetto all'azione sull'insieme Z delle radici di $f(X)$.

Cerchiamo dunque di determinare le orbite di elementi di Z sotto l'azione di $\mathrm{Gal}_F(f)$. Se $f = \prod g_i$ è la sua decomposizione in irriducibili su F, allora le orbite di $\mathrm{Gal}_F(f)$ sono gli insiemi degli zeri dei fattori; in particolare f è irriducibile se e solo se $\mathrm{Gal}_F(f)$ è transitivo.

Come si vede che questo è vero? Da una parte, è immediato che se β è uno zero di g_i, allora $\sigma(\beta)$ resta uno zero di g_i; d'altro canto, se β' è un altro zero di g_i, c'è un F-omomorfismo $F(\beta) \to F(\beta')$ che manda β in β', e che si estende ad un F-automorfismo di E. Dunque, se β', β sono zeri di g_i esiste una $\sigma \in \mathrm{Gal}(E|F)$ che manda β in β'. Allora $\mathrm{Gal}(E|F)\beta = Z(\min_F(\beta))$.

Proposizione 11.2. Se $G \leq S_n$ è transitivo, allora $n \mid |G|$.

Dimostrazione. L'orbita di α ha $|G : \mathrm{Fix}(\alpha)|$ elementi se $\mathrm{Fix}(\alpha)$ è lo stabilizzatore di α in G. Ma $|G\alpha| = n$, perché G era transitivo. Dunque $n \mid |G| = |G : \mathrm{Fix}(\alpha)| \cdot |\mathrm{Fix}(\alpha)|$. □

12 Polinomi Simmetrici.

Sia F un campo, e $F[X_1, \ldots, X_n]$ l'anello dei polinomi in n indeterminate a coefficienti in F. È chiaro che il gruppo simmetrico, che agisce natu-

ralmente sull'insieme $\{1, \ldots, n\}$ identificato a $\{X_1, \ldots, X_n\}$, induce una azione (espressa come rappresentazione permutazionale) $S_n \to \mathrm{Aut}(F[\underline{X}])$, che agisce sui polinomi mandando $f(\underline{X}) = f(X_1, \ldots, X_n)$ in $f(X_{\sigma 1}, \ldots, X_{\sigma n})$; ognuna di queste mappe è chiaramente un automorfismo, e la rappresentazione così determinata è fedele, permettendo di individuare in $\mathrm{Aut}(F[\underline{X}])$ un sottogruppo isomorfo a S_n.

L'azione così determinata si trasferisce direttamente al campo dei quozienti per funtorialità (come del resto passava la precedente azione si S_n su $\{1, \ldots, n\}$), dando così $S_n \lesssim \mathrm{Aut}(F(\underline{X}))$; il Lemma di Artin ora implica che $|F(\underline{X}) : \mathrm{Fix}(S_n)| = |S_n| = n!$, e dunque che l'estensione è di Galois ($\mathrm{Gal}(F(\underline{X})|\,\mathrm{Fix}(S_n)) \geq S_n$, ma se $|\,\mathrm{Gal}(F(\underline{X})|\,\mathrm{Fix}(S_n))| = n!$ sono uguali.

Dunque abbiamo ottenuto un risultato rimarchevole:

> S_n è il gruppo di Galois di una estensione di campi (ma non possiamo fissare quali).

Definizione 12.1 [Polinomi Simmetrici]**:** Il campo $\mathrm{Fix}(S_n) \leq F(\underline{X})$ (risp., l'anello $\mathrm{Fix}(S_n) \leq F[\underline{X}]$, con identico significato dei simboli) contiene i *polinomi simmetrici* nelle indeterminate $X_1, \ldots, X_n$. Definiamo i *polinomi simmetrici elementari* come

$$\begin{aligned}
p_0(X_1, X_2, \ldots, X_n) &= 1, \\
p_1(X_1, X_2, \ldots, X_n) &= \textstyle\sum_{1 \leq j \leq n} X_j, \\
p_2(X_1, X_2, \ldots, X_n) &= \textstyle\sum_{1 \leq j < k \leq n} X_j X_k, \\
p_3(X_1, X_2, \ldots, X_n) &= \textstyle\sum_{1 \leq j < k < l \leq n} X_j X_k X_l, \\
&\vdots \\
p_n(X_1, X_2, \ldots, X_n) &= X_1 X_2 \cdots X_n
\end{aligned}$$

(ovviamente tutti loro sono simmetrici).

Ciò che rende essenziali i polinomi simmetrici elementari è che essi generano l'intero sottoanello (e quindi sottocampo) $\mathrm{Fix}(S_n)$. Vediamo prima il caso del campo.

Teorema 12.1 : $F(X_1, \ldots, X_n)$ è un'estensione di Galois di $F(p_1, \ldots, p_n) \cong \{\text{quozienti di polinomi simmetrici}\}$.

Dimostrazione. Va provato solo l'isomorfismo: da un lato, se tutti i p_i stanno in $\mathrm{Fix}(S_n)$ è evidente che $F(p_1, \ldots, p_n) \leq \mathrm{Fix}(S_n)$. Vorremmo provare, per concludere, che $|\,\mathrm{Fix}(S_n) : F(p_1, \ldots, p_n)| = 1$.

Sia allora $h(X) = \prod_{i=1}^{n} (X - t_i)$. Quelle che prendono il nome di *formule di Vieta* affermano che

$$h(X) = X^n - p_1(\underline{t}) X^{n-1} + \cdots + (-1)^n p_n \tag{129}$$

cioè che i coefficienti di un polinomio di grado n, espresso come prodotto dei suoi fattori lineari, sono (a meno di un segno) i polinomi simmetrici valutati nelle n radici di h; con ciò $h(X) \in F(p_1, \ldots, p_n)[X]$; supponiamo ora che le t_i siano a due a due algebricamente indipendenti: allora $F(t_1, \ldots, t_n) \cong F(X_1, \ldots, X_n)$, e $F(X_1, \ldots, X_n)$ è campo di spezzamento per $h(X)$ su $F(p_1, \ldots, p_n)$. Dunque il grado di $F(X_1, \ldots, X_n)$ su $F(p_1, \ldots, p_n)$ può essere al più $n!$ (perché tale grado deve dividere $n!$), e questo fa concludere che nella torre

$$\begin{array}{c} F(X_1, \ldots, X_n) \\ | \\ \mathrm{Fix}(S_n) \\ | \\ F(p_1, \ldots, p_n) \end{array} \tag{130}$$

c'è in realtà un isomorfismo $\mathrm{Fix}(S_n) \cong F(p_1, \ldots, p_n)$. □

Osservazione 31. Sia G un qualunque gruppo finito. Il teorema di Cayley assicura che $G \hookrightarrow S_n$ per qualche n, dunque c'è una corrispondenza

$$\begin{array}{ccc} F(X_1, \ldots, X_n) & & \langle 1 \rangle \\ | & & | \\ K = \mathrm{Fix}(G) & \longleftrightarrow & G \\ | & & | \\ F(p_1, \ldots, p_n) & & S_n \end{array} \tag{131}$$

ed $F(X_1, \ldots, X_n)|K$ è di Galois con gruppo di Galois G: allora

> Ogni gruppo finito è isomorfo al gruppo di Galois di una estensione $F(X_1, \ldots, X_n)|K$ (ma non possiamo scegliere quale sia il campo di base).

La parte difficile del problema di Galois inverso è quindi: *fissato un gruppo finito G, esiste un'estensione E di un campo prescritto F che ha gruppo di Galois G?*

Teorema 12.2 : In $F[\underline{X}] = F[X_1, \ldots, X_n]$ valgono le seguenti:

- I polinomi simmetrici elementari generano l'intero sottoanello $\mathrm{Fix}(S_n)$ dei polinomi simmetrici.
- I polinomi simmetrici elementari sono algebricamente indipendenti su F, dunque esiste un F-isomorfismo $F[T_1, \ldots, T_n] \to F[p_1, \ldots, p_n]$ che manda $t_i \mapsto p_i$.

Osservazione 32. Osserviamo che il primo punto implica quanto già dimostrato per $F(p_1, \dots, p_n)$. Fissiamo poi la terminologia usata:

$$\overbrace{c \cdot \underbrace{X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}}_{\text{termine}}}^{\text{monomio}} \tag{132}$$

Ordiniamo l'insieme dei termini secondo la relazione $\underline{X^i} \leq \underline{X^j}$ se e solo se o si ha $\sum i_r \leq \sum j_s$, oppure, se le due somme (dette *grado totale* del termine) sono uguali, per il primo indice k con $i_k \neq j_k$ si ha $i_k \leq j_k$.

Questo ordinamento è totale, ed è una congruenza (ossia $s \leq t \Rightarrow su \leq tu$). Diciamo *termine direttivo* di $f(\underline{X})$, $\delta(f)$, il termine massimo (nell'ordinamento introdotto) con coefficiente diverso da zero.

Dimostrazione. Si osservi che p_i ha termine direttivo $X_1 \dots X_i$; dal fatto che l'ordine sui termini è una congruenza segue che il termine direttivo di $f(X)g(X)$ è il prodotto dei rispettivi termini direttivi[10].

Il polinomio $p_1^{d_1} \dots p_n^{d_n}$ ha allora termine direttivo

$$X_1^{d_1}(X_1X_2)^{d_2} \cdots (X_1 \cdots X_n)^{d_n} = X_1^{\sum_{i=1}^n d_i} \cdots X_k^{\sum_{i=k}^n d_i} \cdots X_n^{d_n} \tag{133}$$

Osservazione 33. Detto $\underline{X^d}$ un termine di questo tipo, $\underline{d} \neq \underline{e} \Rightarrow \underline{X^d} \neq \underline{X^e}$: infatti, se i termini fossero uguali, sarebbe $e_n = d_n \Rightarrow e_{n-1} = d_{n-1} \Rightarrow \cdots \Rightarrow e_1 = d_1$.

Osservazione 34. Se $f(X)$ è un polinomio *simmetrico* di termine direttivo $\delta(f) = \underline{X^k} = X_1^{k_1} \cdots X_n^{k_n}$ non è possibile che $i < j$ e $k_i < k_j$. Infatti se f è simmetrico deve essere in particolare fissato dalla permutazione che manda i in j, dunque $X_1^{k_1} \cdots X_i^{k_j} \cdots X_j^{k_i} \cdot X_n^{k_n}$ deve appartenere ancora a f; col che, deve essere $\delta(f) \geq X_1^{k_1} \cdots X_i^{k_j} \cdots X_j^{k_i} \cdots X_n^{k_n}$, e dunque non può essere $k_i < k_j$.

In conclusione il termine direttivo di f è tale che $k_1 \geq k_2 \geq \cdots \geq k_n$.

Ora, dato un polinomio simmetrico f, esiste un $p_1^{d_1} \cdots p_n^{d_n}$ che ha lo stesso termine direttivo? Sì: deve succedere che $\sum_{i=1}^n d_i = k_1$, e in generale $\sum_{i=r}^n d_i = k_r$, $d_n = k_n$. Questo sistema si risolve dall'ultima equazione in modo ricorsivo, dunque esiste un prodotto di polinomi simmetrici elementari che ha lo stesso termine direttivo di f.

Appare chiaro ora come $f - p_1^{d_1} \cdots p_n^{d_n}$ sia ancora simmetrico, con termine direttivo minore del termine direttivo di f; applicando ricorsivamente la stessa procedura si arriva, in un numero finito di passi, a determinare un polinomio nelle p_i che coincide con $f(\underline{X})$.

[10] La dimostrazione è semplice: ovviamente $\delta(f), \delta(g)$ hanno coefficiente diverso da zero, dunque lo ha $\delta(f)\delta(g)$; scelto poi un termine di $f(X)$ diverso da $\delta(f)$, si ha $u < \delta(f)$, e per congruenza $uv \leq u\delta(g) < \delta(f)\delta(g)$; idem a ruoli invertiti, $uv \leq \delta(f)v < \delta(f)\delta(g)$. Dunque $\delta(f)\delta(g) = \delta(fg)$, ottenendosi tutti i termini di fg come prodotti uv di termini di f e di g.

Per il secondo punto del Teorema, supponiamo che $\sum c_{\underline{d}} \underline{p}^{\underline{d}} = 0$ (notazioni cailottiane), con qualche coefficiente non nullo. Allora, se prendiamo due prodotti $\underline{p}^{\underline{d}}, \underline{p}^{\underline{e}}$ con $\underline{d} \neq \underline{e}$, i rispettivi termini direttivi sono diversi: ma a questo punto basta considerare la n-upla $\underline{r} = (r_1, \ldots, r_n)$ tale che $\underline{p}^{\underline{r}}$, con coefficiente $c_{\underline{r}} \neq 0$ e che abbia termine direttivo massimo. Questo non ha modo di essere cancellato da altri termini, perchè nessun altro $\underline{p}^{\underline{d}}$ può avere termine direttivo uguale. Questo è assurdo perché si era supposto $\sum c_{\underline{d}} \underline{p}^{\underline{d}} = 0$. □

Esempio 12.1 : Sia F un campo di caratteristica diversa da 2, ed $f(X) \in F[X]$. Come ormai è ben noto, ogni $\sigma \in \text{Gal}(\text{Split}_F(f)|F)$ permuta le radici di $f(X)$, $\{\alpha_1, \ldots, \alpha_n\}$. Ora, definiamo

$$\Delta = \prod_{i<j}(\alpha_i - \alpha_j); \tag{134}$$

è facile notare che per ogni σ si ha $\sigma(\Delta) = \pm\Delta$, a seconda che σ sia pari o dispari. Allora

$$\sigma(\Delta) = \Delta \iff \sigma \in \text{Gal}_F(f) \cap A_n \tag{135}$$

(facendo agire il gruppo alterno nel modo ovvio per permutazione).

Ora, $D = \Delta^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2$ è tenuto fermo da ogni $\sigma \in \text{Gal}(E|F)$, dunque deve stare in F. Come determinarlo? Consideriamo l'espressione che lo definisce, che si può riguardare come un polinomio simmetrico nelle α_i (è precisamente $\prod_{i<j}(X_i - X_j)^2$ valutato nelle α_i). Si ha

$$\prod_{i<j}(X_i - X_j)^2 = g(p_1(\underline{X}), p_2(\underline{X}), \ldots, p_n(\underline{X})) \tag{136}$$

dato che ogni polinomio simmetrico si scrive come un polinomio nei simmetrici elementari, e allora

$$D = g(p_1(\underline{\alpha}), p_2(\underline{\alpha}), \ldots, p_n(\underline{\alpha})) = g(a_1, \ldots, a_n) \tag{137}$$

dove gli a_i sono, a meno del segno, esattamente i coefficienti di $f(X)$.

L'elemento D si dice *discriminante* del polinomio $f(X)$: si osservi che $F(\Delta) = \text{Fix}(\text{Gal}_F(f) \cap A_n)$; alla luce di tutto quanto appena detto è chiaro che

$f(X)$ ha radici multiple $\iff D = 0$.

Facciamo degli esempi:

- *Polinomi di secondo grado*: il generico polinomio di secondo grado è $X^2 + bX + c$, le cui radici si trovano con la solita formula da scuola media
$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2} \tag{138}$$
Ora, $x_2 - x_2 = \sqrt{b^2 - 4c} = \Delta$, e dunque $D = b^2 - 4c$. D'altra parte, per altra via,
$$D = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = (-b)^2 - 4c = b^2 - 4c. \tag{139}$$

- *Polinomi di terzo grado*: Il generico polinomio di terzo grado, $X^3 + uX^2 + vX + w$, si può riportare, mediante la sostituzione $X \mapsto X - \frac{u}{3}$ alla forma $X^3 + aX + b$[11].

  Per procedere, scopriamo una espressione alternativa per $D = \prod(\alpha_i - \alpha_j)^2$. Nel suo campo di spezzamento un polinomio monico di grado n si scrive $(X - \alpha_1) \cdots (X - \alpha_n)$; se ora lo deriviamo formalmente otteniamo che $f'(\alpha_j) = \prod_{i \neq j}(\alpha_j - \alpha_i)$. Se allora consideriamo $\prod_{j=1}^{n} f'(\alpha_j)$ notiamo che ogni suo fattore è della forma $\alpha_r - \alpha_s$, per $r \neq s$. Lo stesso termine $(\alpha_r - \alpha_s)$ si trova due volte in quel prodotto, una volta in $f'(\alpha_r)$, e una volta in $f'(\alpha_s)$ con segno opposto. Quindi con un ragionamento combinatorio elementare,

  $$\prod_{j=1}^{n} f'(\alpha_j) = (-1)^{\binom{n}{2}} \prod_{r<s}(\alpha_r - \alpha_s)^2 = (-1)^{\binom{n}{2}} D \tag{140}$$

  Nel caso di un polinomio di terzo grado, usando questa formula, si ha

  $$D = (-1) \prod_{j=1}^{3} (3\alpha_j^2 + a) \tag{141}$$

  $$= \cdots$$

  $$= -(27b^2 + 4a^3) \tag{142}$$

Ci chiediamo ora come caratterizzare $\mathrm{Gal}_F(f)$ se f ha grado 3. Dobbiamo distinguere vari casi.

- $f(X)$ è prodotto di fattori lineari in $F[X]$. Allora $\mathrm{Gal}_F(f) = \langle 1 \rangle$ ed $E = \mathrm{Split}_F(f) = F$.
- $f(X)$ è prodotto di un fattore lineare e di un irriducibile di grado 2. Allora $\mathrm{Gal}_F(f) \cong C_2$.
- $f(X)$ è irriducibile in $F[X]$: allora $\mathrm{Gal}_F(f) \leq S_3$ è un sottogruppo transitivo, dunque il suo ordine è multiplo di 3. Ci sono due casi: $\mathrm{Gal}_F(f) \cong S_3$ oppure $\mathrm{Gal}_F(f) \cong A_3$.

  Nel secondo caso, $\mathrm{Gal}_F(f) \cap A_3 = A_3 = \mathrm{Gal}_F(f)$, e allora $F(\Delta) = \mathrm{Fix}(A_3) = F$, cioè $\Delta \in F$, cioè D è un quadrato in F.

  Per esclusione, $\mathrm{Gal}_F(f) \cong S_3$ se e solo se D *non* è un quadrato in F.

  Nel caso di un polinomio di grado 3, abbiamo che $-(27b^2 + 4a^3)$ è un quadrato in F se e solo se $\mathrm{Gal}_F(f) \cong S_3$, e non lo è se e solo se $\mathrm{Gal}_F(f) \cong A_3$.

[11] Esplicitamente, vogliamo trovare una sostituzione affine $X \mapsto X + \alpha$ tale da uccidere il termine di secondo grado: per farlo, un semplice conto mostra che va scelto $\alpha = -u/3$; ora resta da vedere che questa sostituzione è lecita. Le radici del nuovo polinomio sono controllate, perché se β_i era radice del polinomio di partenza, $\beta_i - \alpha$ è radice del nuovo. Il campo di spezzamento poi resta immutato dalla traslazione ($\alpha \in F$), e così resta invariato anche il gruppo di Galois.

L'ultimo caso "scolastico" è quello dei polinomi di grado 4 a coefficienti in F (di caratteristica diversa da $2, 3$). Il generico polinomio di grado 4 ha la forma

$$X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \tag{143}$$

Esauriamo alcuni casi banali:

- Se $f(X)$ si spezza come prodotto di fattori lineari $\mathrm{Gal}_F(f) = \langle 1 \rangle$ e $E = \mathrm{Split}_F(f) \cong F$.

- Se $f(X)$ è prodotto di due fattori lineari e un irriducibile di secondo grado, $\mathrm{Gal}_F(f) \cong C_2$.

- Se $f(X)$ è prodotto di un fattore lineare e di uno di terzo grado, ci si riconduce al caso precedente e a seconda che il discriminante della parte di terzo grado sia o no un quadrato in F, $\mathrm{Gal}_F(f)$ è isomorfo a S_3 oppure ad A_3.

- Se $f(X)$ è prodotto di due fattori di grado 2, $\mathrm{Gal}_F(f) \cong C_2 \times C_2 = V_4$.

Resta il caso in cui $f(X)$ è irriducibile su F. In questo caso, se $\alpha_1, \ldots, \alpha_4$ sono le radici di $f(X)$ nel suo campo di spezzamento, $G = \mathrm{Gal}_F(f)$ è un sottogruppo di S_4 che le permuta transitivamente. Vi sono due sottogruppi notevoli in S_4: il gruppo di Klein V_4 e l'alterno (che contiene Klein). Sappiamo che il gruppo $G \cap A_4$ corrisponde, mediante l'equivalenza aggiunta $\mathrm{Fix}(-)$, al campo $F(\Delta)$; a cosa corrisponde il gruppo $G \cap V_4$?

Consideriamo gli elementi di E

$$\gamma_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4 \tag{144}$$
$$\gamma_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 \tag{145}$$
$$\gamma_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3 \tag{146}$$

Ciascuna delle γ_i sta in E, e sono tutte a due a due distinte. G agisce sull'insieme $\{\gamma_1, \gamma_2, \gamma_3\}$ permutandolo: allora per certo $F(\gamma_1, \gamma_2, \gamma_3) \leq \mathrm{Fix}(G \cap V_4)$ (in effetti il piano è dimostrare che sono uguali: questo segue dal fatto che se $E|F(\underline{\gamma})$ è di Galois, l'inclusione inversa è data dalla relazione $\mathrm{Gal}(E|F(\underline{\gamma})) \supseteq \mathrm{Gal}(E|\,\mathrm{Fix}(G \cap V)) = G \cap V$), e il polinomio $(X - \gamma_1)(X - \gamma_2)(X - \gamma_3)$ è tenuto fisso da tutto G, e deve dunque appartenere a $F[X]$; questo si chiama *risolvente cubica* di $f(X)$.

Nel diagramma

$$\begin{array}{ccc} E & & 1 \\ | & & | \\ F(\underline{\gamma}) & \longleftarrow & G \cap V_4 \\ | & & | \\ F(\Delta) & \longleftarrow & G \cap A_4 \\ | & & | \\ F & & G \end{array} \tag{147}$$

osserviamo che $F(\Delta)|F$ e $F(\underline{\gamma})|F$ sono di Galois (la prima ha grado 2 ed $F(\Delta) \cong \text{Split}_F(X^2 - D)$ e la seconda è il campo di spezzamento per la risolvente cubica $r_f(X)$, che per quanto visto ha zeri semplici). Ora, si osservi che

$$\tfrac{G}{G\cap V_4} \cong \tfrac{\text{Gal}(E|F)}{\text{Gal}(E|F\left(\underline{\gamma}\right))} \cong \text{Gal}(F(\underline{\gamma})|F) \cong \text{Gal}_F(r_f(X)) \tag{148}$$

Questo gruppo è noto, perché $r_f(X)$ ha grado 3 e abbiamo classificato completamente le cubiche.

I gruppi transitivi di S_4, possibili candidati per $\text{Gal}_F(f)$, sono quattro: S_4, A_4, D_8 (il diedrale), V_4 e il ciclico C_4.

La casistica si può riassumere quindi nella tabella seguente

G	$G \cap V_4$	$G/(G \cap V) \cong \text{Gal}_F(g)$
S_4	V_4	S_3
A_4	V_4	C_3
V_4	V_4	1
C_4	C_2	C_2
D_8	C_2	C_2

(149)

L'idea è che conoscendo $\text{Gal}_F(g)$ si conosce $\text{Gal}_F(f) = G$, a parte due casi. Se $\text{Gal}_F(g) \cong C_2$ infatti può essere sia $\text{Gal}_F(f) \cong C_4$ che $\text{Gal}_F(f) \cong D_8$; a questo punto studiare la struttura di $G \cap V$, o se si preferisce, un argomento di cardinalità, è l'unico modo di uscire dall'empasse: se $G \cap V_4 \cong V_4$, esso è transitivo (sull'insieme delle α_i), dunque è il Gal di un polinomio irriducibile su $F\left(\underline{\gamma}\right)[X]$.

Se invece $G \cap V_4 \cong C_2$, esso *non* è transitivo sull'insieme delle α_i, quindi $f(X)$ è riducibile su $F\left(\underline{\gamma}\right)[X]$.

L'argomento di cardinalità è parimenti semplice: se $G\cap V_4$ ha 4 elementi, G ne ha 8, e se ne ha 2, G ne ha 4.

Esempio 12.2 : Consideriamo il polinomio $X^4 - 4X + 2$, irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein. La sua risolvente cubica[12] è $X^3 - 8X + 16$, che ha gruppo di Galois S_3 (infatti $D = -4864$ che non è un quadrato su $\mathbb{Q}$). Allora $\mathrm{Gal}_F(f) \cong S_4$.

13 Chiusure algebriche.

Sarebbe bello se ogni campo avesse una *chiusura algebrica*:

Definizione 13.1 : Sia F un campo. un'estensione $\Omega|F$ è una *chiusura algebrica* di F se ne è una estensione algebrica, ed è algebricamente chiuso.

Esempio 13.1 : $\mathbb{C}|\mathbb{R}$ è algebricamente chiuso e di grado 2. Di converso, $\mathbb{C}$ non è una chiusura algebrica (per esempio) di $\mathbb{Q}$, perché contiene trascendenti.

Proposizione 13.1. Se $F \leq K$, e K è algebricamente chiuso, allora K contiene una chiusura algebrica di F.

Dimostrazione. Sia $A = \{a \in K \mid a\ F\text{-algebrico}\}$. A è un sottocampo di K, ed è per costruzione un'estensione algebrica di F. È algebricamente chiuso: se $f(X) \in A[X]$ di grado maggiore di zero, tutti gli zeri di f sono elementi di K algebrici su A, e dunque su F[13]. Dunque, A è algebricamente chiuso, perché contiene tutti gli zeri di polinomi a coefficienti in A. □

Ne segue che, per esempio, l'insieme dei numeri complessi $\mathbb{Q}$-algebrici è una chiusura algebrica di $\mathbb{Q}$.

13.1 Ordini e Cardinalità.

Ricordiamo che un insieme $\varnothing \neq X$ su cui sia posta una relazione riflessiva, antisimmetrica e transitiva si dice *ordinato*. È ordinato *totalmente* se ogni coppia di elementi è confrontabile. Una *catena* in un insieme ordinato X è un sottoinsieme di X totalmente ordinato.

Diciamo che $m \in (X, \leq)$ è un *maggiorante* per $Y \subseteq X$ se $y \leq m$ per ogni $y \in Y$. Un insieme ordinato e non vuoto si dice *induttivo* se ogni sua catena ammette un maggiorante; un elemento $t \in (X, \leq)$ si dice *massimale* se non esiste nessun $x \in X$ tale che $t < x$.

Lemma 13.1 [Lemma di Zorn]**:** (una delle tante istanze dell'assioma di scelta). Se $X \neq \varnothing$ è ordinato e induttivo, allora ammette un elemento massimale.

[12] Si può ragionare in generale: se $f(X) = X^4 + qX^2 + rX + s$, la sua risolvente cubica è $g(X) = X^3 - 2qX^2 + (q^2 - 4s)X + r^2$; nel caso non sia ridotto, e $f(X) = X^4 + bX^3 + cX^2 + dX + e$, invece $g(X) = X^3 - cX^2 + (bd + 4r)X - b^2e + 4ce - d^2$

[13] Se $E = \mathrm{Split}_A(f)$, $|E : A| = \deg f$; allora $|E : F| = \deg f |A : F| < \infty$.

Esempio 13.2 : Se $X = \mathbb{Z}_>$ è ordinato dalla relazione di divisibilità inversa, ossia $a \leq b \iff b \mid a$, allora 1 è massimale.

Esempio 13.3 : $X = \mathbb{Z}_\geq$ è ordinato dalla relazione di divisibilità inversa, i primi sono elementi massimali. Analogamente se si considera come X il reticolo degli ideali di $\mathbb{Z}$.

In effetti questo è un fatto generale.

Esempio 13.4 : Sia A un anello unitario. Consideriamo una catena $\{I_\lambda\}$ di ideali *propri* di A; allora $\bigcup I_\lambda$ è un ideale proprio di A, perché $1 \in \bigcap I_\lambda^c$, e le operazioni si fanno nel modo ovvio. Dunque $\bigcup I_\lambda$ è un maggiorante della catena: l'insieme degli ideali propri di A è induttivo, e per Zorn ammette elementi massimali.

Esistono gruppi senza sottogruppi massimali non banali: per esempio $(\mathbb{Z}/p\mathbb{Z}, +)$, oppure $(\mathbb{Q}, +)$ (questo è più difficile: se per assurdo esiste $M \leq \mathbb{Q}$ massimale, allora $\mathbb{Q}/M$ è semplice abeliano, quindi ciclico finito di ordine primo: allora $\mathbb{Q}/M \cong \mathbb{Z}_p$; d'altra parte $\mathbb{Q}$ è divisibile, quindi iniettivo in $\mathbf{Ab}$. Allora la sequenza $0 \to M \to \mathbb{Q} \to \mathbb{Z}/p\mathbb{Z} \to 0$ è esatta e spezza: questo è assurdo, perché è noto che $\mathbb{Q}$ non ha sottogruppi di indice finito.)

Dal Lemma di Zorn segue anche che ogni spazio vettoriale ammette una base:

Teorema 13.1 : Sia V uno spazio vettoriale sul campo K, $\mathcal{F} \subseteq V$ un sottoinsieme di vettori linearmente indipendenti (ossia, comunque venga scelto un insieme finito di vettori di $\mathcal{F}$, questo è linearmente indipendente), e $\mathcal{G} \subseteq V$ un insieme di generatori.

Allora è possibile completare $\mathcal{F}$ ad una base di V, aggiungendo elementi di $\mathcal{G}$, ossia esiste un insieme X di vettori di V tale che $\mathcal{F} \subseteq X \subseteq \mathcal{F} \cup \mathcal{G}$.

Dimostrazione. Consideriamo

$$\mathcal{X} = \big\{X \subseteq V \mid \mathcal{F} \subseteq X \subseteq \mathcal{F} \cup \mathcal{G},\ X \text{ insiem indipendente}\big\} \tag{150}$$

$\mathcal{X} \neq \varnothing$, perché contiene $\mathcal{F}$, e ordinato dall'inclusione è un insieme induttivo. Se infatti $C \subseteq \mathcal{X}$ è una catena, e definiamo $\bar{X} = \bigcup_{X \in C} X$, è evidente che $\mathcal{F} \subseteq \bar{X} \subseteq \mathcal{F} \cup \mathcal{G}$. Resta da provare che è un insieme indipendente. Se $y_1, \dots, y_n \in \bar{X}$, e supponiamo che $\sum c_i y_i = 0$, allora esiste X_k che contiene tutti gli y_i; questo però implica che essi sono indipendenti, dato che $X_k \in \mathcal{X}$. Dunque per il Lemma di Zorn $\mathcal{X}$ ha un elemento massimale B.

Mostriamo che è una base: basta vedere che è un insieme di generatori. Sia $v \in V$ e consideriamo $B \cup \{v\}$; ci sono due casi: o $v \in B$, e allora $v \in \langle B \rangle$, oppure no, e allora $B \cup \{v\}$ non può essere indipendente (violerebbe la massimalità di B). Allora, in ogni caso, si ha $v \in \langle v \rangle$, dunque $\langle B \rangle \supseteq \langle G \rangle = V$. □

13.2 Numeri Cardinali.

Raccogliamo per comodità di lettura le nozioni di base riguardo l'aritmetica dei numeri cardinali.

Definizione 13.2 : Un insieme non vuoto si dice *induttivo* se $\forall x(x \in X \Rightarrow x \cup \{x\} \in X)$.

Assioma. Esiste un insieme induttivo.

Si osservi che l'intersezione di una famiglia arbitraria di insiemi induttivi (in un opportuno universo) è induttiva.

Definizione 13.3 : Definiamo ω l'intersezione di tutti gli insiemi induttivi.

ω è il modello di Peano dei numeri naturali; la somma di numeri naturali risulta nell'unione di elementi dell'insieme, la funzione successore consta di $n \mapsto n \cup \{n\}$.

Un insieme X si dice *finito* se esistono $n \in \omega$ e una biiezione $X \to n$. Si dice *infinito* in caso contrario.

Accettando l'assioma della scelta, una definizione equivalente di insieme infinito è la seguente

Definizione 13.4 : Un insieme X si dice *infinito nel senso di Dedekind* se può essere messo in biiezione con un suo sottoinsieme proprio, e *finito* in caso contrario. La scelta è necessaria per mostrare che ogni D-finito è finito.

Osservazione 35. ω è Dedekind infinito ed è il minimo insieme infinito, nel senso precisato dalla seguente

Proposizione 13.2. Sia X un insieme infinito. Allora esiste una iniezione $\omega \to X$.

Dimostrazione. Definiamo $f\colon \omega \to X$ induttivamente: $f(0)$ è scelto ad arbitrio; $f(1)$ è scelto nel complementare di $\{f(0)\}$, ed $f(n)$ nel complementare di $I_f = \{f(0), \ldots, f(n-1)\}$. Ad ogni passo, $X \setminus I_f$ non può essere vuoto, altrimenti X sarebbe finito. La funzione f è chiaramente iniettiva. □

Diciamo che X *ha cardinalità minore* di Y se esiste una funzione iniettiva $X \to Y$, e scriviamo $|X| \leq |Y|$. Questo ordina totalmente la classe degli insiemi, e in tal senso $|\omega|$ è il minimo cardinale infinito. Lo si indica con $\aleph_0$.

La classe dei *numeri cardinali* può essere dotata di opportune operazioni di somma e prodotto:

- $|X| + |Y| := |X \cup Y|$;
- $|X| \cdot |Y| := |X \times Y|$.

Vale poi il Teorema di Cantor-Scröder-Bernstein, che assicura che la relazione suddetta è antisimmetrica: $|X| \leq |Y|, |Y| \leq |X|$ implica che $|X| = |Y|$, ossia che esiste una biiezione tra i due.

Proposizione 13.3. Sia F un campo. L'anello dei polinomi $F[X]$ ha cardinalità $|F|$ se F è infinito, e $\aleph_0$ se F è finito.

Dimostrazione. Se F è infinito, ovviamente i polinomi di grado zero sono $|F|$, e i polinomi lineari sono $|F \times F| = |F|$; allo stesso modo i polinomi di grado $\leq n$ sono $|F^n| = |F|$, dunque per induzione si conclude che esiste una biiezione $\lambda_k \colon F[X]_{\leq k} \to F$; la funzione $F[X] \to \mathbb{N} \times F \colon f(X) \mapsto (k, \lambda_k(f))$ è iniettiva. Dunque

$$|F| \leq |F[X]| \leq \aleph_0 |F| = |F| \tag{151}$$

da cui si conclude, per Cantor-Schröder-Bernstein.

Se F è finito, si tratta di stabilire una biiezione tra un prodotto numerabile di insiemi finiti (tali sono gli insiemi $F[X]_{\leq k}$) e $\aleph_0$; questo è classico. Si tratta in effetti di notare due cose: da una parte esiste una funzione iniettiva $F[X] \to \mathbb{N} \times \mathbb{N} \colon f \mapsto (\deg f, \lambda_k(f))$, dove $\lambda_k \colon F[X]_{\leq k} \hookrightarrow \mathbb{N}$, e dunque $|F[X]| \leq \aleph_0$, e dall'altra ovviamente $F[X]$ contiene almeno $\aleph_0$ elementi (la base $\{1, X, X^2, \dots\}$). □

Questo risultato ha come corollario il fatto che se $E|F$ è algebrica, quando F è infinito si ha $|E| = |F|$, e quando F è finito $|E| \leq \aleph_0$.

Dunque devono esistere dei numeri reali $\mathbb{Q}$ trascendenti, perché $|\mathbb{R}| = 2^{\aleph_0} \gneq \aleph_0 = |\mathbb{Q}|$, e devono anzi essere "quasi tutti" trascendenti, nel senso che i numeri $\mathbb{Q}$-algebrici sono un insieme di cardinalità $\aleph_0$, e $|\mathbb{R} \setminus A| = 2^{\aleph_0}$.

Osservazione 36. Poichè su un campo finito ci sono polinomi irriducibili di ogni grado, la chiusura algebrica di un campo finito è infinita (quando esiste: ma tra poco dimostriamo che esiste), e numerabile. In effetti ogni campo algebricamente chiuso deve essere infinito: se per assurdo fosse finito, diciamo con n elementi, il polinomio $\prod_{i=1}^{n}(X - a_i) + 1$ non avrebbe zeri.

Teorema 13.2 : Sia F un campo, allora esiste una chiusura algebrica per F.

Dimostrazione. Consideriamo l'insieme F; esiste certamente un monomorfismo verso qualche insieme X (per esempio $\mathcal{P}(F)$). Consideriamo ora l'insieme

$$\mathcal{K} = \big\{K \mid F \leq K \subseteq X\big\} \tag{152}$$

dei sovracampi di F che sono sottoinsiemi di X. Sia poi

$$\mathcal{X} = \big\{(E, +, \cdot) \mid E \subseteq X, E|F \text{ estensione alg.}\big\} \tag{153}$$

$\mathcal{X}$ non è vuoto (contiene F), è ordinato (dall'inclusione) e induttivo, perché è sufficiente definire $E = \bigcup E_i$ come maggiorante di una catena $\{E_i\}$ (le

operazioni sono definite notando che per ogni $a, b \in E$ esiste un j sufficientemente grande tale che $a, b \in (E_j, +_j, \cdot_j)$, dunque essi si sommano e moltiplicano rispetto a $+_j, \cdot_j$; **l'essere algebrica…**).

Il Lemma di Zorn porge quindi un elemento massimale $\Omega \in \mathfrak{X}$. Ora, Ω è un'estensione algebrica, e se per assurdo $f(X) \in \Omega[X]$ non avesse radici in Ω, esisterebbe una estensione $K = \Omega(a)$, in cui $f(a) = 0$; ora $\Omega \subsetneq K$, e a seconda che Ω sia o no finito, $|K| \leq \aleph_0$ oppure $|K| = |\Omega|$. Quindi in ambo i casi $|\Omega| \leq |K|$, ciò che implica $|K \setminus \Omega| \leq |X \setminus \Omega|$. Dunque esiste una funzione iniettiva $\phi\colon K \setminus \Omega \hookrightarrow X \setminus \Omega$[14]. Definiamo ora

$$\psi\colon K \to X\colon k \mapsto \begin{cases} k & k \in \Omega \\ \phi(k) & k \notin \Omega \end{cases} \tag{154}$$

Tale funzione è iniettiva: definiamo $L = \operatorname{im}\psi$ e le operazioni $\psi(k) +_L \psi(h) = \psi(k +_K h)$ (analogamente col prodotto), che rendono ψ un omomorfismo. Le operazioni di L ristrette a Ω devono dare le vecchie somma e prodotto, ossia L è estensione di Ω; ogni algebrico su L deve poi essere algebrico su Ω, dunque su F. D'altra parte L sarebbe una estensione algebrica di F strettamente più grande di Ω, e questo è assurdo. □

14 Generalizzazioni varie.

14.1 Teoria di Galois infinita.

Una estensione algebrica, normale e separabile di F, $\Omega|F$, si dice *estensione di Galois* di F.

In tali ipotesi, Ω è il campo di spezzamento di una famiglia di polinomi di $F[X]$ separabili.

Teorema 14.1 : Sia $\Omega|F$ di Galois, ed E un campo intermedio. Ogni F-omomorfismo $f\colon E \to \Omega$ si estende ad un F-endomorfismo di Ω.

Dimostrazione. Segue dal Lemma di Zorn; sia $\mathcal{K}$ l'insieme di tutte le coppie (K, φ) tali che $E \leq K \leq \Omega$ e φ estende f. Ordinato per inclusione questo insieme è induttivo (il massimale di una catena è l'unione di tutti i campi della catena). Allora ammette un massimale, diciamo $(\bar{K}, \bar{\varphi})$; se ora $\bar{K} \subsetneq \Omega$ viene violata la massimalità. □

Sia $\Omega|F$ estensione algebrica e di Galois, e sia $G = \operatorname{Aut}(\Omega|F)$. Sia poi $S \subseteq \Omega$ un insieme finito, e $\operatorname{Stab}(S) = \{\sigma \in G \mid \sigma(s) = s,\ \forall s \in S\}$. Dunque $\sigma|_{F(S)} = \mathrm{id}$, dove $F(S)$ è il minimo sovracampo di F che contiene $F \cup S$: $F(S)$ è un'estensione finita di F contenuta in Ω, perché S è finito e fatto di elementi algebrici su F.

[14] Se esistono funzioni iniettive $i\colon A \to B$ e $j\colon B \to C$, e in particolare $j\colon B \to C$ e $j \circ i\colon A \to C$, allora $j \circ (B \setminus i(A)) = j(B) \setminus j \circ i(A) \subseteq C \setminus i \circ j(A)$, e $j \circ i|_{B \setminus i(A)}\colon B \setminus i(A) \to C \setminus j \circ i(A)$ è una funzione iniettiva tra gli insiemi voluti.

Dunque $\text{Stab}(S) = \text{Aut}(\Omega|F(S)) \leq G$.

Definiamo poi come $GS = \bar{S}$ l'orbita di $S \subseteq \Omega$ per l'azione naturale di G. GS è ancora un sottoinsieme finito di Ω.

Dimostrazione. Ogni elemento $s \in S$ è algebrico su F, e ogni $\sigma \in G$ ne fissa il polinomio minimo, ovvero può al massimo permutarne le radici, mandando s in un'altra radice di $\min_F(s)$, ovvero in un altro elemento di un insieme finito. Gli elementi di S essendo un numero finito, si conclude. □

Consideriamo ora $\text{Stab}(GS) = \{\sigma \in G \mid \sigma(u) = u \ \forall u \in GS\}$. Questo è un sottogruppo di G, normale in G; in effetti $\text{Stab}(GS)$ è precisamente il nucleo del morfismo $\theta\colon G \to \text{Aut}(F(GS)|F)\colon \tau \mapsto \tau|_{F(GS)}$.

Inoltre, $|G : \text{Stab}(GS)| = |G/\text{Stab}(GS)| \leq |\text{Aut}(F(GS)|F)|$ (l'uguaglianza vale perché ogni elemento di $\text{Aut}(F(GS)|F)$ "viene" dalla restrizione di un F-automorfismo di Ω, dunque la mappa θ è suriettiva).

Si osservi anche che $F(GS)|F$ è finita, e che dunque $|G : \text{Stab}(GS)|$ è finito: riassumendo abbiamo provato che

- $|G : \text{Stab}(GS)| < \infty$;
- $\text{Stab}(S) \geq \text{Stab}(GS)$, dove $\text{Stab}(GS) \trianglelefteq G$, e $|G/\text{Stab}(S)| < \infty$;
- $\bigcap_{S \in \mathcal{P}_f(\Omega)} \text{Stab}(S) = \{\text{id}\}$ e $\bigcap_{\substack{S \in \mathcal{P}_f(\Omega) \\ G(\bar{S}) = \bar{S}}} \text{Stab}(GS) = \{1\}$.

14.2 Topologia di Krull.

Le famiglie di sottoinsiemi

$$\{\text{Stab}(S) \mid S \subseteq \Omega \text{ finito}\} \tag{155}$$

$$\{\text{Stab}(GS) \mid S \subseteq \Omega \text{ finito}, \ G\bar{S} = \bar{S}\} \tag{156}$$

sono basi di intorni $\mathcal{U}$, $\mathcal{V}$ di una topologia su G[15]. Con la topologia generata da questa base (che consiste degli elementi di base $U \in \mathcal{U}$, più loro traslati, più unioni del tipo $\bigcup_{\substack{\sigma \in G \\ U \in \mathcal{U}}} \sigma U$), $\text{Aut}(\Omega|F)$ diventa un gruppo topologico.

Dimostrazione. Siano $\sigma, \tau \in G$, allora se $\sigma\tau$ sta nell'intorno di base $U = \text{Stab}(\bar{S})$, consideriamo l'intorno $\sigma U \times \tau U$: allora

$$\sigma U \tau U = \sigma\tau(\tau^{-1}U\tau)U = \sigma\tau U$$

[15] Va controllato che $U_S = \text{Stab}(S)$ al variare di S nelle parti finite di Ω ricopre $G = \text{Aut}(\Omega|F)$, ma questo è banale perché $U_{\{1\}} = G$, e poi che comunque dati due U_S, U_T, per ogni $\sigma \in U_S \cap U)T$ esiste un $R \subseteq \Omega$, finito, tale che $U_S \cap U)T \supseteq U_R \ni \sigma$; questo è ovvio quando si sia osservato che $U_S \cap U_T = U_{S \cup T}$.

Osservazione 37. La topologia così ottenuta su G è di Hausdorff, e rende G uno spazio totalmente disconnesso e compatto. Infatti se $\sigma \neq \tau$ $\sigma\tau^{-1} \neq \mathrm{id}$. Poiché $\bigcap \mathrm{Stab}(S) = \{\mathrm{id}\}$, esiste un S tale che $\sigma\tau^{-1} \notin U = \mathrm{Stab}(S)$. Dunque $\sigma U \neq \tau U$; dato che due classi laterali o coincidono o hanno intersezione vuota (è una proprietà generale delle classi di equivalenza!) si conclude che $\sigma U \cap \tau U = \varnothing$. Resta da provare che lo spazio così ottenuto è compatto e totalmente sconnesso. Dato che è noto che

$$\mathrm{Aut}(\Omega|F) \cong \varprojlim_{\substack{S\subseteq\Omega \\ \text{finito}}} \mathrm{Gal}(F(S)|F); \tag{157}$$

questo si traduce nel provare che $\mathrm{Aut}(\Omega|F)$ è chiuso; la tesi segue dal fatto che è un sottospazio chiuso di un Hausdorff compatto: il teorema di Tychonov e proprietà topologiche elementari dicono che **CHaus** ammette prodotti, e dunque $\prod \mathrm{Gal}(F(S)|F)$ è un Hausdorff compatto. Ora però $\varprojlim_{S\subseteq\Omega} \mathrm{Gal}(F(S)|F)$ si caratterizza come l'equalizzatore di una coppia di frecce[16] tra (prodotti di) Hausdorff compatti, e deve quindi essere chiuso (l'equalizzatore è controimmagine della diagonale, che in un Hausdorff è chiusa). □

[16]Precisamente, se per brevità diciamo $\Gamma(-) = \mathrm{Gal}(F(-)|F)$, è l'equalizzatore di

$$\prod_{S\in\mathcal{P}_f(\Omega)} \Gamma(S) \underset{\beta}{\overset{\alpha}{\rightrightarrows}} \prod_{S\subseteq T} \Gamma(T)$$

dove $\alpha = (\Gamma(\subseteq) \circ \pi_{\Gamma(S)})_{S\in\mathcal{P}_f(\Omega)}$ e $\beta = (\pi_{\Gamma(T)})_{T\in\mathcal{P}_f(\Omega)}$.