1 Richiami di Teoria di Galois

Ricordiamo alcuni concetti e risultati dal corso di Algebra II (vedi [AII]).
Siano E, F campi tali che $F \subseteq E$; allora si dice che E è una *estensione* (o un *ampliamento*) di F, e si scrive $F \leq E$; si dice anche che $E|F$ è una estensione di campi. Più in generale, definiamo $E|F$ una estensione di campi se esiste un omomorfismo iniettivo $\iota : F \to E$ (in tal caso $\iota(F)$ è un sottocampo di E isomorfo a F). Data una estensione $E|F$ e un campo K tale che $F \leq K \leq E$, K si dice un *campo intermedio* dell'estensione $E|F$.
Se E è una estensione di F, allora E è in particolare un F-spazio vettoriale; il *grado* dell'estensione $E|F$ è la dimensione $[E : F] = \dim_F(E)$. $E|F$ si dice estensione *finita* se il grado $[E : F]$ è finito. Formula dei Gradi: per ogni campo intermedio L dell'estensione finita $E|F$, vale $[E : F] = [E : L][L : F]$.
Sia $E|F$ una estensione di campi. Un elemento $a \in E$ si dice *algebrico su* F se esiste un polinomio $0 \neq f(x) \in F[x]$ tale che $f(a) = 0$. Una estensione $E|F$ si dice *algebrica* se ogni elemento $a \in E$ è algebrico su F.
Sia $E|F$ una estensione di campi. Ricordiamo i seguenti risultati:
(1) Ogni estensione finita è algebrica ([AII, Prop. 6.9]);
(2) se $b \in E$ è algebrico su F, allora l'estensione $F[b]|F$ è algebrica ([AII, Cor. 6.10]);
(3) $E|F$ è finita se e solo se $E = F[b_1, b_2, \ldots, b_m]$ con $b_1, b_2, \ldots, b_m \in E$ algebrici su F;
(4) l'insieme $\{a \in E \mid a \text{ è algebrico su } F\}$ è un campo([AII, Teor. 6.12]); ;
(5) dato un campo intermedio K dell'estensione $E|F$, si ha: $E|F$ è algebrica se e solo se $E|K$ e $K|F$ sono algebriche.
Dato $a \in E$, a algebrico su F, l'omomorfismo di sostituzione $\varphi_a : F[x] \to E$ tale che $\varphi(f(x)) = f(a)$, per $f(x) \in F[x]$ ha nucleo $I = \ker(\varphi_a)$ non nullo e, dato che $F[x]$ è un PID, esiste un unico generatore monico $\min_F(a)$, il *polinomio minimo* di a su F, di I. Dato che F è un dominio di integrità, segue che $\min_F(a)$ è irriducibile in $F[x]$.
Sia a un elemento di E, estensione di F, con a algebrico su F e sia $p(x) = \min_F(a) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$, $n = \deg(p(x))$. Allora $F(a)$ (il sottocampo di E generato da a su F) è isomorfo all'anello quoziente $F[x]/(p(x))$; quindi $F(x) = F[a]$ (sottoanello generato da a su F). Inoltre, vediamo che ogni elemento di $F[a]$ si rappresenta in modo unico nella forma $\sum_{i=0}^{n-1} b_i a^i$ con $b_0, b_1, \ldots, b_{n-1} \in F$.
Dato un omomorfismo di campi $\phi : F \to L$, per il Principio di Sostituzione ([AI, Teorema 8.3]) esiste un unico omomorfismo (che per semplicità denotiamo con lo stesso simbolo) $\phi : F[x] \to L[x]$ che estende il precedente.

Proposizione 1.1. *Siano F, L campi e sia dato un omomorfismo $\phi : F \to L$. Siano $F(a)$ e $L(b)$ estensioni algebriche semplici e supponiamo che $\phi(\min_F(a)) = \min_F(b)$. Allora esiste un unico isomorfismo $\hat{\phi} : F[a] \to L[b]$, che estende ϕ e tale che $\hat{\phi}(a) = b$.*

DIMOSTRAZIONE. Si veda [AII, Lemma 6.17]. ∎

Sia $f(x)$ un polinomio non nullo a coefficienti in un campo F. Diciamo che f *si spezza su F (o in $F[x]$)* se ogni fattore irriducibile di f in $F[x]$ ha grado 1. (Osserviamo quindi che i polinomi costanti $\neq 0$ si spezzano su qualunque campo che li contiene, in quanto non hanno fattori irriducibili).
Ricordiamo che un campo E tale che $F \leq E$ si dice un *campo di spezzamento per f su F* se f si spezza su E, ma non si spezza su alcun campo intermedio proprio K, $F \leq K < E$. Osserviamo che la definizione di campo di spezzamento dipende non solo dal polinomio f ma anche dal campo F considerato. Dato $f \in F[x]$, $f \neq 0$, esiste un campo di spezzamento per f su F ([AII, Teor. 6.16]), ed è univocamente determinato a meno di F-isomorfismo ([AII, Teor. 6.18]).
Una estensione algebrica di campi $E|F$ si dice *normale* se, per ogni $a \in E$, E contiene un campo di spezzamento per il polinomio minimo di a su F. Ricordiamo che una estensione $E|F$ è normale e finita se e solo se E è il campo di spezzamento su F di un polinomio $f(x) \in F[x]$ ([AII, Teor. 6.21]).

Esercizio 1.1. Sia $E|F$ una estensione finita. Si provi che esiste una estensione F di E tale che $L|F$ è finita e normale.

Esercizio 1.2. Sia $E|F$ una estensione finita. Si provi che $E|F$ è normale se e solo se per ogni estensione L di E ed ogni F-omomorfismo $\phi : E \to L$, vale $\phi(E) = E$.

Un polinomio $f \in F[x]$ di grado n si dice *a radici distinte* se f ha n radici in una estensione E di F su cui f si spezza (si noti che questo non dipende dalla scelta di E).
Un polinomio non nullo $f \in F[x]$ si dice *separabile su F* se ogni suo fattore irriducible in $F[x]$ ha radici distinte. Osserviamo: (i) la definizione data di separabilità dipende non solo dal polinomio f ma anche dal campo F scelto; (ii) se $F \leq E$ è una estensione di campi e $f \in F[x]$ è un polinomio separabile su F, allora f è anche separabile su E (infatti ogni fattore irriducibile g_0 di f in $E[x]$ divide un opportuno fattore irriducibile g_1 di f in $F[x]$, e quindi ha radici distinte).
Data una estensione $E|F$ e un elemento $a \in E$, a algebrico su F, si dice che a è *separabile su F* se il polinomio minimo $\min_F(a)$ è separabile su F (ovvero, essendo irriducibile su F, ha radici distinte). Una estensione algebrica $E|F$ si dice *separabile* se ogni elemento $a \in E$ è separabile su F. Osserviamo che se $F \leq L \leq E$ e $E|F$ è separabile, allora $E|L$ e $L|F$ sono separabili (vale anche l'implicazione inversa: si veda il Corollario 1.4).
Una estensione $E|F$ si dice *di Galois* se $E|F$ è finita, normale e separabile.

Teorema 1.2. *Sia $E|F$ una estensione finita. Allora sono equivalenti:*

(a) *$E|F$ è una estensione di Galois;*

(b) *E è un campo di spezzamento su F per un polinomio $f(x) \in F[x]$, $f(x)$ separabile su F.*

DIMOSTRAZIONE. (a) $\Rightarrow$ (b): $E = F[a_1, a_2, \ldots, a_k]$ con $a_1, a_2, \ldots, a_k \in E$ elementi algebrici su F; sia, per $i = 1, 2, \ldots, k$, $f_i = \min_F(a_i)$. Osserviamo che $f = f_1 f_2 \cdots f_k$ è un polinomio separabile e che E è un campo di spezzamento per f su F.

(b) $\Rightarrow$ (a): segue da [AII, Teorema 7.12].. ∎

Una estensione algebrica $E|F$ si dice *puramente inseparabile* se, per ogni $a \in E$, a è separabile su F solo se $a \in F$.
Banalmente, per ogni campo F l'estensione $F|F$ è puramente inseparabile (e anche separabile!).

Teorema 1.3. *Sia $E|F$ una estensione algebrica e sia*

$$L = \{a \in E \mid a \ \text{ è separabile su } \ F\} .$$

Allora

(a) *L è un campo; $L|F$ è la massima estensione intermedia separabile di $E|F$.*

(b) *$E|L$ è puramente inseparabile.*

DIMOSTRAZIONE. Siano $a, b \in L$ e sia $f = \min_F(a)\min_F(b) \in F[x]$. Osserviamo che f è separabile su F. Sia K un campo di spezzamento per f su $F[a, b]$. Allora K è anche campo di spezzamento per f su F e quindi per il Teorema 1.2 $K|F$ é una estensione di Galois. In particolare, $K|F$ è separabile e quindi, dato che $F \leq F[a, b] \leq K$, anche $F[a, b]|F$ è separabile. Dunque $a - b \in L$ e (se $b \neq 0$) $ab^{-1} \in L$. Pertanto L è un sottocampo di E. Chiaramente, $L|F$ è separabile e per ogni K campo intermedio di $E|F$ tale che $K|F$ è separabile, vale $K \leq L$.

Proviamo ora che $E|L$ è puramente inseparabile. Se $\mathrm{char}(F) = 0$, allora $L = E$ e non c'è niente da dimostrare. Supponiamo quindi che sia $\mathrm{char}(F) = p$ primo.
Proviamo intanto che per ogni $a \in E$ esiste un $n \in \mathbb{N}$ tale che $a^{p^n} \in L$. Sia $g(x) = \min_F(a)$; osserviamo che, essendo $g(x) \in F[x]$ monico e irriducibile, esiste $h(x) \in F[x]$ monico, irriducibile e separabile su F tale che $g(x) = h(x^{p^n})$, per un opportuno $n \in \mathbb{N}$: infatti, se $(g, g') = 1$ prendiamo $h = g$; altrimenti, $g' = 0$ e quindi $g(x) = g_1(x^p)$, con $g_1 \in F[x]$ monico e irriducibile (una fattorizzazione propria $g_1 = h_1 k_1$ in $F[x]$ darebbe $g(x) = h_1(x^p)k_1(x^p)$ fattorizzazione propria in $F[x]$); dato che $\deg(g_1) < \deg(g)$, si conclude per induzione. Dato che $h(a^{p^n}) = g(a) = 0$ e $h \in F[x]$ è monico e irriducibile, $h = \min_F(a^{p^n})$. Ma h è separabile su F e quindi a^{p^n} è separabile su F, ovvero $a^{p^n} \in L$.

Supponiamo ora che $a \in E$ sia separabile su L. Sia $q(x) = \min_L(a)$. Per quanto provato nel paragrafo precedente, esiste un $n \in \mathbb{N}$ tale che $a^{p^n} \in L$. Dunque $q(x)$ divide il polinomio $p(x) = x^{p^n} - a^{p^n}$ in $L[x]$. Ma allora $q(x)$ divide $p(x) = (x-a)^{p^n}$ in $E[x]$ e da questo segue $q(x) = (x-a)^k$ in $E[x]$, con k intero positivo. Ma $q(x)$ ha radici distinte in E (poiché è irriducibile e separabile su L); segue $q(x) = x - a$ e quindi $a \in L$. Dunque $E|L$ è puramente inseparabile. ∎

Corollario 1.4. *Sia $E|F$ una estensione algebrica e K un campo intermedio: $F \leq K \leq E$. Se $E|K$ e $K|F$ sono separabili, allora $E|F$ è separabile.*

Dimostrazione. Sia $L = \{a \in E \mid a \text{ è separabile su } F\}$; osserviamo che $K \subseteq L$. Per il Teorema 1.3, L è un campo e $E|L$ è puramente inseparabile. Ma $E|K$ è separabile e $K \leq L \leq E$, quindi $E|L$ è separabile. Segue $E = L$ e dunque $E|F$ è separabile. ∎

Esercizio 1.3. Sia $E|F$ una estensione algebrica, con $\text{char}(F) = p$ primo. Provare che sono equivalenti:

(a) $E|F$ è puramente inseparabile;

(b) per ogni $a \in E$ esiste un intero $n \in N$ tale che $a^{p^n} \in F$.

Esercizio 1.4. Sia $E|F$ una estensione finita, con $\text{char}(F) = p$ primo. Si provi che se $E|F$ è puramente inseparabile, allora $[E : F]$ è una potenza di p.

Esercizio 1.5. Sia $E|F$ una estensione finita inseparabile. Si provi che $\text{char}(F)$ divide $[E : F]$.

Definizione. (1) Un campo E si dice *algebricamente chiuso* se ogni polinomio $0 \neq f(x) \in E[x]$ si spezza su E.
(2) Sia E una estensione di un campo F. E si dice una *chiusura algebrica di F* se

(a) E è algebrico su F;

(a) ogni $0 \neq f(x) \in F[x]$ si spezza su E.

Osserviamo che un campo E è algebricamente chiuso se e solo se è la chiusura algebrica di sé stesso.

Lemma 1.5. *Sia $E|F$ una estensione algebrica. Sono equivalenti:*

(a) *E è algebricamente chiuso;*

(b) *E è una chiusura algebrica di F;*

(c) *se $L|E$ è una estensione tale che L è algebrico su F, allora $L = E$;*

(d) *se $L|E$ è una estensione algebrica, allora $L = E$.*

DIMOSTRAZIONE. (a) $\Rightarrow$ (b): chiaro, dato che $F[x] \leq E[x]$.
(b) $\Rightarrow$ (c): Sia $L|E$ estensione con $L|F$ algebrica. Sia $a \in L$ e $f = \min_F(a)$. Per ipotesi f si spezza in $E[x]$, quindi $x - a \in E[x]$ ovvero $a \in E$. Segue $L = E$.
(c) $\Rightarrow$ (d): segue immediatamente ricordando che se $L|E$ e $E|F$ sono estensioni algebriche, allora $L|F$ è algebrica.
(d) $\Rightarrow$ (a): Sia $0 \neq f \in E[x]$ e sia L un campo di spezzamento per f su E. Allora $L|E$ è algebrica e quindi per (c) $L = E$. ∎

Corollario 1.6. *Sia $E|F$ una estensione di campi con E algebricamente chiuso. Allora*

$$L = \{a \in E \mid a \ \ \textit{algebrico su} \ \ F\}$$

è una chiusura algebrica di F (ed è l'unica contenuta in E).

DIMOSTRAZIONE. Sappiamo che L è un campo. Chiaramente, l'estensione $L|F$ è algebrica. Sia $0 \neq f \in F[x]$. Dato che $f \in E[x]$, per ipotesi E contiene un campo di spezzamento K per f su F. Dato che $K|F$ è una estensione algebrica, abbiamo $K \subseteq L$. Dunque L è una chiusura algebrica di F.
Se $L_0 \leq E$ e L_0 è una chiusura algebrica di F, allora $L_0 \leq L$ (dato che $L|F$ è algebrica). Ma allora $L = L_0$ per (b) $\Rightarrow$ (c) del Lemma 1.5. ∎

Esempio. (1) Per il Teorema Fondamentale dell'Algebra, il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso.
(2) Per il Corollario 1.6, il campo $\mathbb{A}$ dei numeri complessi algebrici su $\mathbb{Q}$ è una chiusura algebrica di $\mathbb{Q}$, ed è quindi algebricamente chiuso.

Corollario 1.7. *Sia E un campo tale che ogni polinomio non costante $f \in E[x]$ ha almeno una radice in E. Allora E è algebricamente chiuso.*

DIMOSTRAZIONE. Sia $0 \neq f \in E[x]$; proviamo che f si spezza su E. Sia g un fattore irriducibile di f in $E[x]$. Dunque $\deg g \geq 1$ e per ipotesi esiste quindi un $a \in E$ radice di g. Per il Teorema di Ruffini, $x - a$ divide g in $E[x]$ e quindi g, essendo irriducibile, è associato a $x - a$; in particolare $\deg g = 1$. Dunque f si spezza su E. ∎

Dimostriamo ora l'esistenza di chiusure algebriche (Teorema 1.8) e la loro unicità a meno di isomorfismo (Corollario 1.10).

Teorema 1.8. *Sia F un campo. Allora esiste E ampliamento di F tale che E è una chiusura algebrica di F.*

DIMOSTRAZIONE. Ad ogni polinomio non costante $f \in F[x]$ associamo una indeterminata x_f, con $x_f \neq x_g$ per $f \neq g$.
Sia $\mathcal{X} = \{x_f \mid f \in F[x], f \text{ non costante}\}$ e sia $A = F[\mathcal{X}]$ l'anello dei polinomi nelle indeterminate $\mathcal{X}$ (ricordiamo che un elemento di A è un polinomio in un numero *finito* di indeterminate). Consideriamo l'ideale $I = \langle f(x_f) \mid f \in F[x], f \text{ non costante}\rangle$ dell'anello A. Proviamo che I è un ideale proprio. Supponiamo, procedendo per assurdo, che $1_A \in I$: allora esistono $g_1, g_2, \ldots, g_n \in A$ tali che

$$g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \cdots g_n f_n(x_{f_n}) = 1 \; . \tag{1}$$

Scriviamo $x_i = x_{f_i}$; osserviamo che, ampliando l'insieme delle indeterminate considerate, possiamo supporre che anche i polinomi $g_1, g_2, \ldots, g_n$ coinvolgano solo indeterminate nell'insieme $\{x_1, x_2, \ldots, x_n, \ldots, x_m\} \subseteq \mathcal{X}$, con m opportuno intero, $m \geq n$. Dunque possiamo riscrivere (1) come

$$\sum_{i=1}^{n} g_i(x_1, x_2, \ldots, x_m) f_i(x_i) = 1 \; . \tag{2}$$

Consideriamo ora un campo di spezzamento L per il polinomio $f_1(x)f_2(x)\cdots f_n(x) \in F[x]$ (in una nuova indeterminata x) su F. Consideriamo, per $1 \leq i \leq n$, a_i una fissata radice di f_i in L e poniamo, per $n+1 \leq i \leq m$, $a_i = 0$. Applicando l'omomorfismo di sostituzione da A a L, definito da $x_i \mapsto a_i$ per $1 \leq i \leq m$, abbiamo allora

$$\sum_{i=1}^{n} g_i(a_1, a_2, \ldots, a_m) f_i(a_i) = 0$$

e quindi, dalla uguaglianza (2) segue $0 = 1$ in L, contraddizione.
Dunque I è un ideale proprio di A. Applicando il Lemma di Zorn all'insieme (ordinato per inclusione) degli ideali propri (ovvero non contententi 1_A) di A che contengono I, si prova che esiste un ideale massimale J di A tale che $I \subseteq J$.
Definiamo $E_1 = A/J$; si noti che E_1 è un campo, estensione di F; identificando (come consueto) F con la sua immagine tramite la proiezione canonica, possiamo supporre $F \leq E_1$. Osserviamo infine che, per ogni polinomio non costante $f \in F[x]$, il campo E_1 contiene una radice del polinomio f: infatti $f(x_f + J) = O_{E_1}$.
Si costruisce così, induttivamente, una sequenza

$$E_0 = F \leq E_1 \leq E_2 \leq \ldots \leq E_n \leq \ldots$$

di estensioni, in modo che, per ogni $i \geq 0$, ogni polinomio non costante $f \in E_i[x]$ abbia almeno una radice in E_{i+1}. Poniamo allora

$$\widehat{E} = \bigcup_{i \geq 0} E_i$$

e definiamo le operazioni di somma e addizione nel modo seguente: dati $a, b \in \widehat{E}$, esiste (visto che la famiglia $\{E_i\}_{i\geq 0}$ è totalmente ordinata per inclusione) un indice n_0 tale che $a, b \in E_{n_0}$; definiamo allora $a + b$ e ab come gli elementi corrispondenti alle operazione nel campo E_{n_0} (si noti che la definizione non dipende dalla scelta di n_0). Rispetto a queste operazioni, $\widehat{E}$ è un campo.
Sia ora $f \in \widehat{E}[x]$ un polinomio non costante; dato che f ha un numero finito di coefficienti, esiste un $n_o \in \mathbb{N}$ tale che $f \in E_{n_0}[x]$; quindi f ha una radice in E_{n_0+1} e quindi in $\widehat{E}$. Per il Corollario 1.7, $\widehat{E}$ è algebricamente chiuso. Posto quindi $E = \{a \in \widehat{E} \mid a \text{ è algebrico su } F\}$, per il Corollario 1.6 E è una chiusura algebrica di F. ∎

Teorema 1.9. *Sia $\phi : F \to F_1$ un isomorfismo di campi e siano E e E_1, rispettivamente, chiusure algebriche di F e F_1. Allora ϕ si estende ad un isomorfismo $\widehat{\phi} : E \to E_1$.*

Dimostrazione. Consideriamo l'insieme

$$\mathcal{P} = \{(K, \theta) \mid F \leq K \leq E,\ \theta : K \to E_1 \ \text{ omomorfismo che estende } \phi\} \ .$$

Su $\mathcal{P}$ definiamo una relazione ponendo, per $(K_1, \theta_1), (K_2, \theta_2) \in \mathcal{P}$ $(K_1, \theta_1) \leq (K_2, \theta_2)$ se $K_1 \leq K_2$ e θ_2 è una estensione di θ_1. Si verifica che $\leq$ è una relazione di ordine su $\mathcal{P}$ e che nell'insieme parzialemente ordinato $(\mathcal{P}, \leq)$ ogni catena ha un maggiorante. Per il Lemma di Zorn esiste quindi un elemento massimale (M, μ) in $\mathcal{P}$.
Dato $f \in F[x]$ un polinomio non nullo, sia $L \leq E$ il campo di spezzamento per f su M in E e $L_1 \leq E_1$ il campo di spezzamento per $\mu(f)$ su $\mu(M)$. Per il Teorema di Unicità dei campi di spezzamento, μ si estende ad un isomorfismo $\widehat{\mu} : L \to L_1$. Dunque $(M, \mu) \leq (L, \widehat{\mu})$ e per la massimalità segue $L = M$. Dunque M è una chiusura algebrica di F. Per il Lemma 1.5, segue $E = L$ e quindi $\mu : E \to \mu(E)$ è un isomorfismo, che estende ϕ. Ma allora $\mu(E)$ è una chiusura algebrica di $\mu(F) = F_1$ e quindi (di nuovo per il Lemma 1.5) concludiamo che $\mu(E) = E_1$ e quindi $\mu : E \to E_1$ è l'isomorfismo cercato.
∎

Corollario 1.10. *Se E e E' sono chiusure algebriche di F, allora E e E' sono campi F-isomorfi.*

2 Complementi

Ricordiamo che una estensione di campi $E|F$ si dice *semplice* se $E = F(a)$ per un opportuno elemento $a \in E$.

Teorema 2.1 (Artin)**.** *Sia $E|F$ una estensione finita.*
$E|F$ è semplice se e solo se il numero dei campi intermedi $F \leq K \leq E$ è finito.

DIMOSTRAZIONE. Supponiamo che l'estensione $E|F$ sia semplice e sia $E = F[\alpha]$ per un opportuno elemento $\alpha \in E$. Poiché $E|F$ è finita, α è algebrico su F; sia $f = \min_F(\alpha)$ il polinomio minimo di α su F.
Dato un campo intermedio K, $F \leq K \leq E$, definiamo $g_K = \min_K(\alpha)$. Osserviamo che g_k divide f nell'anello dei polinomi $K[X]$ e quindi anche in $E[x]$. Dunque abbiamo definito una applicazione γ, tale che $\gamma(K) = g_K$, dall'insieme dei campi intermedi dell'estensione $E|F$ nell'insieme $\mathcal{F}$ dei fattori *monici* del polinomio f in $E[x]$.
Proviamo ora che l'applicazione γ è iniettiva. Sia $g_K = a_0+a_1+\cdots+a_{m-1}x^{m-1}+x^m$, con $a_0, a_1, \ldots, a_{m-1} \in K$ e sia $L = F[a_0, a_1, \ldots, a_{m-1}]$. Mostriamo che $L = K$, osservando che questo è sufficiente per provare l'iniettività di γ, dato che K è univocamente determinato dai coefficienti del polinomio g_K. Osserviamo che da $E = F[\alpha]$ segue $E = K[\alpha]$ e $E = L[\alpha]$. Abbiamo inoltre $g_k \in L[x]$ e, essendo g_k irriducibile in $K[x]$ che contiene $L[x]$, g_k è irriducibile in $L[x]$ e quindi $\min_L(\alpha) = g_k$. Segue

$$[E : K] = \deg g_K = [E : L]$$

e, essendo $L \leq K$, abbiamo $L = K$.
Dato che l'insieme $\mathcal{F}$ è finito, concludiamo quindi che il numero dei campi intermedi dell'estensione $E|F$ è finito.

Viceversa, supponiamo ora che l'estensione $E|F$ abbia un numero finito di campi intermedi. Dividiamo la dimostrazione in due casi. Supponiamo prima che F sia un campo finito. Dato che il grado $[E : F]$ è finito, segue che anche E è un campo finito (precisamente, $|E| = |F|^{[E:F]}$). Ma il gruppo moltiplicativo $E^\times$ degli elementi diversi da zero di E è ciclico([AII, Teeorema 7.6]), ovvero $E^\times = \langle a \rangle$ per un opportuno elemento $a \in E$. Segue quindi $E = F[a]$.
Assumiamo infine che F sia un campo infinito. Dato che $E|F$ è una estensione finita, esistono $a_1, a_2, \ldots, a_n \in E$ tali che sia $E = F[a_1, a_2, \ldots, a_n]$. Procedendo per induzione su $[E : F]$, possiamo supporre che sia $n = 2$, ovvero $E = F[a, b]$ per opportuni $a, b \in E$. Consideriamo ora, per ogni $\lambda \in F$, il corrispondente campo intermedio $K_\lambda = F[a + \lambda b]$. Poiché il numero dei campi intermedi di $E|F$ è finito, mentre $|F|$ è infinita, esistono $\lambda, \mu \in F$, con $\lambda \neq \mu$ e $K_\lambda = K_\mu$. Da $a + \lambda b, a + \mu b \in K_\lambda$ segue $(\lambda - \mu)b \in K_\lambda$ e quindi $b \in K_\lambda$. Pertanto anche $a \in K_\lambda$ e dunque $E = F[a, b] = K_\lambda$, ovvero $a+\lambda b$ è un elemento primitivo dell'estensione $E|F$. ∎

Come conseguenza abbiamo che ogni estensione intermedia di una estensione algebrica semplice è semplice (ciò è vero anche per estensioni trascendenti: Teorema di Lüroth.)

Corollario 2.2. *Sia $E|F$ una estensione di campi tale che $E = F[a]$ con $a \in E$ algebrico su F. Allora per ogni campo K con $F \leq K \leq E$, esiste un elemento $b \in E$ tale che $K = F[b]$.*

Dal Teorema di Artin deduciamo, tramite la corrispondenza di Galois, il seguente interessante risultato: ogni estensione finita separabile è semplice. (Notiamo che $\mathbb{R}|\mathbb{Q}$ è una estensione separabile infinita, e non semplice)
Data una estensione semplice $E|F$ e un elemento $a \in E$ tale che sia $E = F(a)$, l'elemento a si dice un *elemento primitivo* dell'estensione $E|F$). Osserviamo che nel caso di campi finiti il termine 'elemento primitivo' viene usato a volte con il significato, più restrittivo,di generatore del gruppo moltiplicativo del campo.

Teorema 2.3 (dell'Elemento Primitivo)**.** *Sia $E|F$ una estensione finita separabile. Allora $E|F$ è una estensione semplice.*

DIMOSTRAZIONE. Dato che $E|F$ è finita, esistono $a_1, a_2, \ldots, a_m \in E$, algebrici su F, tali che $E = F[a_1, a_2, \ldots, a_m]$. Sia $F = \prod_{i=1}^{m} \min_F(a_i)$ il prodotto dei polinomi minimi degli a_i. Dato che ogni a_i è separabile su F, f è separabile su F. Sia K un campo di spezzamento per f su E. Osserviamo che K è anche campo di spezzamento di f su F e che per il Teorema 1.2 $K|F$ è di Galois. Per la corrispondenza di Galois, l'insieme $\mathcal{K}$ dei campi intermedi dell'estensione $E|F$ è in corrispondenza biunivoca con l'insieme $\mathcal{L}$ dei sottogruppi di $\mathrm{Gal}(K|F)$ che contengono $\mathrm{Gal}(K|E)$. Dunque $|\mathcal{K}| = |\mathcal{L}|$. Ma $|\mathcal{L}|$ è finita, dato che sicuramente il gruppo finito $\mathrm{Gal}(K|F)$ possiede solo un numero finito di sottogruppi. Concludiamo quindi applicando il Teorema di Artin (Teorema 2.1). ∎

Nell'esercizio seguente vediamo un esempio di una estensione finita non semplice.

Esercizio 2.1. Sia $F = \mathbb{Z}_p(x, y)$ il campo delle funzioni razionali nelle due indeterminate x e y sul campo $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Sia E campo di spezzamento su F del polinomio $(t^p - x)(t^p - y) \in F[t]$. Si provi che $E = F[a, b]$, dove $a, b \in E$ sono elementi tali che $a^p = x$ e $b^p = y$. Provare che $[E : F] = p^2$ e che, per ogni $\alpha \in E$, $\alpha^p \in F$. Dedurre che l'estensione $E|F$ non è semplice.

Il prossimo teorema stabilisce l'indipendenza lineare di omomorsimi fra due campi dati. (Ricordiamo che un omomorfismo di campi è necessariamente iniettivo e, per definizione, porta l'unità del primo campo in quella del secondo).

Teorema 2.4 (Dedekind)**.** *Siano E e L campi e sia $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ un insieme finito di omomorfismi e distinti da E in L . Se $a_1, a_2, \ldots, a_n \in L$ sono tali che $\sum_{i=1}^{n} a_1\alpha_i(a) = 0$ per ogni $a \in E$, allora $a_1 = a_2 = \cdots = a_n = 0$.*

DIMOSTRAZIONE. Procediamo per induzione su $n = |A|$. Se $n = 1$, allora $a_1\alpha_1(1) = a_1 1 = a_1 = 0$. Supponiamo quindi $n > 1$ e consideriamo un elemento $b \in E$. Per un qualsiasi $a \in E$ per ipotesi vale

$$\sum_{i=1}^{n} a_i\alpha_i(a) = 0 \tag{3}$$

da cui, moltiplicando per $\alpha_n(b)$ segue

$$\sum_{i=1}^{n} a_i\alpha_i(a)\alpha_n(b) = 0 \tag{4}$$

mentre sostituendo in (3) l'elemento ab al posto di a abbiamo

$$\sum_{i=1}^{n} a_i\alpha_i(ab) = \sum_{i=1}^{n} a_i\alpha_i(a)\alpha_i(b) = 0\ . \tag{5}$$

Deduciamo quindi

$$\sum_{i=1}^{n-1} a_i(\alpha_n(b) - \alpha_i(b))\alpha_i(a) = 0$$

per ogni $a, b \in E$. Dunque, per ipotesi induttiva, segue $a_i(\alpha_n(b) - \alpha_i(b)) = 0$ per ogni $i \in \{1, 2, \ldots, n-1\}$ e per ogni $b \in E$. Dato che gli automorfismi in A sono distinti, per ogni $1 \leq i \leq n-1$ esiste un elemento $b_i \in E$ tale che $\alpha_i(b_i) \neq \alpha_n(b_i)$; pertanto abbiamo $a_i = 0$ per ogni $i \leq n-1$. Ripetendo il ragionamento con α_1 al posto di α_n, otteniamo infine che anche $a_n = 0$. ∎

Dato un campo E, l'insieme E^E di tutte le applicazioni da E in E costituisce un E-spazio vettoriale. Il teorema precedente stabilisce, in particolare, la lineare indipendenza in E^E dell'insieme $\mathrm{Aut}(E)$ degli automorfismi del campo E .

Dimostriamo di seguito il Teorema della Base Normale, un risultato che rafforza (nel caso di estensioni di Galois) il Teorema dell'Elemento Primitivo (Teor. 2.3).
Ricordiamo, preliminarmente, alcuni fatti di Algebra Lineare. Sia F un campo, V un F-spazio vettoriale e $A \in \mathrm{End_F(V)}$ un endomorfismo di V. E' allora definito in maniera naturale un omomorfismo (omomorfismo di valutazione in A) $\phi_A : F[x] \to \mathrm{End_F(V)}$ che associa a ogni polinomio $f(x) \in F[x]$ l'endomorfismo $f(A)$. In tal modo, fissato l'endomorfismo A, V acquista una struttura di $F[x]$-modulo. Il nucleo di ϕ_A è un ideale principale e il suo generatore monico m_A si dice il *polinomio minimo* di A. Il polinomio $p_A = \det(A - xI)$ (dove I è l'omomorfismo identico di V; ricordiamo anche che il determinante di un endomorfismo è ben definito, essendo indipendente dalla scelta di una base di V) si dice *polinomio caratteristico* di V. E' noto che m_A divide f_A (Teorema di Hamilton-Cayley; più ancora: ogni radice di f_A, in una chiusura algebrica di F, è anche radice di m_A).

Teorema 2.5. *Sia V un F-spazio vettoriale di dimensione finita (F campo) e sia $A \in \mathrm{End_F(V)}$. Se il polinomio minimo m_A e il polinomio caratteristic f_A coincidono, allora esiste un $v_0 \in V$ tale che*

$$V = \{f(A)(v_0) \mid f \in F[x]\}$$

(ovvero: $V = \langle v_0 \rangle$ è un $F[x]$-modulo ciclico*).*

DIMOSTRAZIONE. Sia

$$m_A = \prod_{i=1}^{k} p_i^{a_i}$$

una decomposizione del polinomio minimo m_A in fattori irriducibili monici distinti in $F[x]$ (con $a_i \geq 1$ per ogni $i = 1, 2, \ldots, k$). Definiamo, per $j \in \{1, 2, \ldots, k\}$,

$$h_j = \prod_{i \neq j} p_i^{a_i} \qquad \text{e} \qquad g_j = p_j^{a_j - 1} h_j \ .$$

Per ogni dato j, m_a non divide g_j e quindi esiste un vettore $w_j \in V$ tale che $g_j(A)(w_j) = p_j^{a_j-1}(A)(h_j(A)(w_j)) \neq 0$.
Definiamo $v_j = h_j(A)(w_j)$ e $v_0 = v_1 + v_2 + \cdots + v_k$. Osserviamo che $p_j^{a_j-1}(A)(v_j) \neq 0$ e che $p_j^{a_j}(A)(v_j) = m_A(A)(w_j) = 0$, per ogni j. Dunque $g_i(v_j) = 0$ per ogni $i \neq j$. Abbiamo quindi, per $i \in \{1, 2, \ldots, k\}$, $g_i(A)(v_0) = g_i(A)(v_i) \neq 0$, poiché altrimenti da $p_i^{a_i-1} = (g_i, p_i^{a_i})$ seguirebbe $p_i^{a_i-1}(A)(v_i) = 0$, contro quanto sopra osservato.
Pertanto, per ogni divisore proprio g di m_A, si ha $g(A)(v_0) \neq 0$ (dato che g divide almeno uno dei g_j in $F[x]$) e quindi $\{h \in F[x] \mid h(A)(v_0) = 0\} = (m_A)$. Ponendo $W_0 = \{f(A)(v_0) \mid f \in F[x]\}$, segue quindi

$$\dim_F W_0 = \deg(m_A) = \deg(f_A) = \dim_F(V)$$

e dunque $V = W_0 = \langle v_0 \rangle$ è generato da v_0 come $F[x]$-modulo. ∎

Teorema 2.6 (della base normale)**.** *Sia $E|F$ una estensione di Galois e sia $G = \mathrm{Gal}(E|F)$. Allora esiste un elemento $b \in E$ tale che l'insieme*

$$B = \{\alpha(b)\}_{\alpha \in G}$$

sia una base di E come spazio vettoriale su F (B si dice una base normale *di $E|F$).*

DIMOSTRAZIONE. Dividiamo la dimostrazione in due casi. Supponiamo prima che il campo base F sia infinito. È sufficiente provare l'esistenza di un elemento $b \in E$ tale che l'insieme $\{\alpha(b)\}_{\alpha \in G}$ sia linearmente indipendente su F, dato che $[E : F] = \dim_F(E) = |G|$.
Osserviamo che, per una qualunque scelta, al variare di α in G, di elementi $a_\alpha \in F$ vale

$$\sum_{\alpha \in G} a_\alpha \alpha(b) = 0$$

se e solo se, per un qualunque $\beta \in G$

$$\sum_{\alpha \in G} a_\alpha (\beta^{-1}\alpha)(b) = \beta^{-1} \left(\sum_{\alpha \in G} a_\alpha \alpha(b) \right) = 0 \ .$$

Dobbiamo quindi mostrare che, per un opportuno elemento $b \in E$, il determinante della matrice

$$\left((\beta^{-1}\alpha)(b)\right)_{\beta,\alpha\in G}$$

è diverso da zero.
Per il Teorema dell'Elemento Primitivo esiste un elemento $a \in E$ tale che $E = F[a]$. Sia $f(x) = \min_F(a)$ il polinomio minimo di a su F. Allora

$$f(x) = \prod_{\gamma\in G} (x - \gamma(a))$$

poichè il polinomio a secondo membro è mandato in sè da ogni elemento di G, e quindi è un polinomio monico di $F[x]$, ha l'elemento a come radice e dunque è multiplo di $f(x)$, ed ha grado uguale a $\deg(f) = [F[a] : F] = [E : F]$. Dunque tutti gli elementi $\gamma(a)$, al variare di γ in G, sono distinti (si veda anche l'Esercizio 2.3).
Definiamo

$$g(x) = \frac{f(x)}{x - a} = \prod_{1\neq\gamma\in G} (x - \gamma(a))$$

e, per $\beta \in G$ (intendendo con β l'automorfismo indotto su $E[x]$),

$$\beta(g) = \frac{f(x)}{x - \beta(a)} \ .$$

Dunque

$$\beta(g)(a) = 0 \text{ se } \beta \neq 1, \text{ mentre } \beta(g)(a) \neq 0 \text{ se } \beta = 1 \ . \tag{6}$$

Consideriamo ora la matrice a coefficienti in $E[x]$

$$M(x) = \left(\beta^{-1}\alpha(g(x))\right)_{\beta,\alpha\in G} = \left(\frac{f(x)}{x - \beta^{-1}\alpha(a)}\right)_{\beta,\alpha\in G}$$

e denotiamo con $\Delta(x)$ il suo determinante. Applicando (6), abbiamo che $M(a)$ è una matrice diagonale, con coefficienti $g(a) \neq 0$ sulla diagonale. Quindi $\Delta(a) \neq 0$ e pertanto il polinomio $\Delta(x)$ non è il polinomio nullo.
Poiché F è infinito, esiste un elemento $c \in F$ tale che $\Delta(c) \neq 0$. (Si osservi che $c = \beta^{-1}\alpha(c)$ per ogni $\beta, \alpha \in G$, poiché $c \in F$). Dunque la matrice

$$M(c) = \left(\frac{f(c)}{c - \beta^{-1}\alpha(a)}\right)_{\beta,\alpha\in G} = \left(\beta^{-1}\alpha\left(\frac{f(c)}{c - a}\right)\right)_{\beta,\alpha\in G}$$

è non singolare e quindi, per la discussione all'inizio della dimostrazione, ponendo

$$b = \frac{f(c)}{c - a}$$

l'insieme $B = \{\gamma(b)\}_{\gamma \in G}$ è una base normale di $E|F$.

Supponiamo ora che il campo F sia finito; dato che il grado $[E : F]$ è finito, anche il campo E è un campo finito. Dunque il gruppo di Galois $G = \mathrm{Gal}(E|F)$ è ciclico; sia $G = \langle\gamma\rangle$. Consideriamo γ come F-endomorfismo dello spazio vettoriale E e proviamo che il suo polinomio minimo è $x^n - 1$, dove $n = |G|$. Sicuramente il polinomio minimo di γ divide $x^n - 1$, dato che $\gamma^n = 1$. D'altro lato, γ non può essere radice di alcun polinomio in $F[x]$ di grado minore di n, poiché per il Teorema 2.4 le funzioni $1, \gamma, \gamma^2, \ldots, \gamma^{n-1}$ sono linearmente indipendenti su F. Dunque $x^n - 1$ è il polinomio minimo di γ ed esso quindi coincide (essendo $\dim_F(E) = n$) con suo il polinomio caratteristico. Per il Teorema 2.5 ciò implica l'esistenza di un elemento $b \in E$ tale che l'insieme di trasformati $B = \{b, \gamma(b), \gamma^2(b), \ldots, \gamma^{n-1}(b)\}$ costituisca una base dello spazio vettoriale E su F; quindi B è una base normale dell'estensione $E|F$. ∎

Osservazioni.

(i) Sia B una base normale dell'estensione di Galois $E|F$. Allora ogni $\alpha \in \mathrm{Gal}(E|F)$ induce una permutazione π_α di B e l'applicazione $\alpha \mapsto \pi_\alpha$ è un omomorfismo iniettivo di $\mathrm{Gal}(E|F)$ nel gruppo simmetrico $Sym(B)$.

(ii) Sia $E|F$ una estensione di Galois. Se $\{\alpha(b)\}_\alpha$ è una base normale di $E|F$, allora $E = F[b]$, ovvero b è in particolare un elemento primitivo di $E|F$. Infatti, $\prod_{\alpha \in \mathrm{Gal}(E|F)} (x - \alpha(b)) = \min_F(b)$.

(iii) Sia p un numero primo e sia ζ una radice primitiva p-esima dell'unità. Allora $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ è una base normale di $\mathbb{Q}_p|\mathbb{Q}$. (Osserviamo però che gli elementi i e $-i$ sono linearmente dipendenti e quindi non formano una base normale di $\mathbb{Q}_4|\mathbb{Q}$).

Definizione 1. *Siano E, L sottocampi di un campo C. Definiamo il campo* composto *EK come il minimo sottocampo di C che contiene sia E che L.*

Teorema 2.7. *Siano $E|F$ e $L|F$ estensioni di campi, con $E|F$ di Galois e E,L sottocampi di uno stesso campo C. Allora*

(a) *l'estensione $EL|L$ è di Galois.*

(b) $\mathrm{Gal}(EL|L)$ *è isomorfo al sottogruppo* $\mathrm{Gal}(E|E \cap L)$ *di* $\mathrm{Gal}(E|F)$*; in particolare,* $[EL : L]$ *divide* $[E : F]$.

(c) *se anche $L|F$ è di Galois, allora $EL|F$ è di Galois; l'omomorfismo di gruppi $\varphi : \mathrm{Gal}(EL/F) \to \mathrm{Gal}(E|F) \times \mathrm{Gal}(L|F)$, $\alpha \mapsto (\alpha_E, \alpha_L)$ è iniettiva. Se $E \cap L = F$, allora ϕ è un isomorfismo.*

DIMOSTRAZIONE. (a) Per il Teorema 1.2, $E|F$ è campo di spezzamento su F di un opportuno polinomio $f(x) \in F[x]$, f separabile su F. Dunque f è separabile anche su L e, poichè EL è campo di spezzamento per f su L, dal Teorema 1.2 segue che l'estensione $EL|L$ è di Galois.

(b)La restrizione $\rho : \mathrm{Gal}(EL|L) \to \mathrm{Gal}(E|F)$, che associa ad $\alpha \in \mathrm{Gal}(EL|L)$ l'automorfismo $\alpha_E \in \mathrm{Gal}(E|F)$ (osserviamo che $\alpha(E) = E$, perchè α manda in sé l'insieme delle radici di $f(x)$ e fissa il campo $F \leq L$) è un omomorfismo di gruppi. Inoltre, ρ è un omomorfismo iniettivo, perché un automorfismo $\alpha \in \mathrm{Gal}(EL|L)$ che fissa tutti gli elementi di E ha sia L che E nel proprio campo fisso, e quindi è l'automorfismo identico di EL. Sia $H = \rho(\mathrm{Gal}(EL|L))$ l'immagine di ρ; per provare che $H = \mathrm{Gal}(E|E \cap L)$, utilizzando la corrispondenza di Galois basta far vedere che $\mathrm{Fix}(H) = E \cap L$. Se $\alpha \in \mathrm{Gal}(EL|L)$, allora la restrizione $\rho(\alpha)$ fissa $E \cap L$; quindi $E \cap L \subseteq \mathrm{Fix}(H)$. Viceversa, se $a \in \mathrm{Fix}(H)$, allora a è fissato da tutti gli elementi di $\mathrm{Gal}(EL|L)$; quindi, dato che $EL|L$ è di Galois, abbiamo che $a \in L$. Ma $a \in E$ e dunque $a \in E \cap L$. Abbiamo pertanto provato che $\mathrm{Gal}(EL|L)$ è isomorfo a $\mathrm{Gal}(E|E \cap L) \leq \mathrm{Gal}(E|F)$. Dal Teorema di Lagrange segue quindi che $[EL : L] = |\mathrm{Gal}(EL|L)|$ divide $[E : F]| = |\mathrm{Gal}(E|F)|$.

(c) Supponiamo che anche $L|F$ sia di Galois. Allora, dati $f, g \in F[x]$ tali che E è campo di spezzamento per f su F e L è campo di spezzamento per g su F, osserviamo che EL è campo di spezzamento per fg su F. Dato che f e g sono separabili su F, il prodotto fg è separabile su F e quindi $EL|F$ è una estensione di Galois per il Teorema 1.2.
L'applicazione θ che ad un elemento $\alpha \in \mathrm{Gal}(EL|F)$ fa corrispondere la coppia di restrizioni (α_E, α_L) è un omomorfismo da $\mathrm{Gal}(EL|F)$ nel prodotto diretto $\mathrm{Gal}(E|F) \times \mathrm{Gal}(L|F)$. Se $\alpha \in \ker(\theta)$, allora $E, L \leq \mathrm{Fix}(\alpha)$, da cui segue $EL \leq \mathrm{Fix}(\alpha)$ e quindi α è l'identità. Quindi θ è iniettivo. Per concludere, supponiamo $E \cap L = F$ e proviamo che θ è suriettivo. Per il punto (a), per ogni $\alpha_0 \in \mathrm{Gal}(E|F)$, $\beta_0 \in \mathrm{Gal}(L|F)$, esistono $\alpha \in \mathrm{Gal}(EL|L)$ e $\beta \in \mathrm{Gal}(EL|E)$ tali che $\alpha_E = \alpha_0$ e $\beta_L = \beta_0$. Consideriamo $\gamma = \alpha\beta$. Allora $\gamma_E = \alpha_E\beta_E = \alpha_0 id_L = \alpha_0$ e, analogamente, $\gamma_L = \beta_0$. Dunque θ è suriettivo e quindi è un isomorfismo. ∎

Osservazioni. (1) Siano $E = \mathbb{Q}[\sqrt[3]{2}]$ e $L = \mathbb{Q}[\zeta\sqrt[3]{2}]$, dove ζ è una radice primitiva terza dell'unità. Allora $EL = \mathbb{Q}[\zeta, \sqrt[3]{2}]$ e quindi $[EL : L] = 2$ non divide $[E : L]$. Questo mostra che nel Teorema 2.7 (punto (b)) è necessario che $E|F$ sia una estensione di Galois.

(2) Dato un campo F e un polinomio separabile $f \in F[x]$, sia E il campo di spezzamento di f su F e $G = \mathrm{Gal}(E|F)$. Considerando una estensione $L|F$, possiamo vedere f come polinomio a coefficienti in L; il Teorema 2.7 ci dice come cambia il gruppo di Galois di f nell'ampliamento del campo base da F a L: in particolare, il gruppo di Galois di f su L è un sottogruppo del gruppo di Galois di f su F.

Esercizio 2.2. Siano E un campo, G un sottogruppo di $\mathrm{Aut}(E)$ e $F = \mathrm{Fix(G)}$ il campo fisso di G in E. Sia $a \in E$ e $\{a = a_1, a_2, \ldots, a_k\} = \{\alpha(a) \mid \alpha \in G\}$ l'orbita di a rispetto all'azione di G (con $a_i \neq a_j$ per $i \neq j$). Si provi che $\min_F(a) = \prod_{i=1}^{k}(x - a_i)$.

Esercizio 2.3. Sia $E|F$ una estensione di Galois e $G = \mathrm{Gal}\, E|F$. Si provi che $a \in E$ è un elemento primitivo di $E|F$ se e solo se $\alpha(a) \neq \beta(a)$ per ogni $\alpha, \beta \in G$, $\alpha \neq \beta$.

Esercizio 2.4. Siano $E = GF(27)$ e $F = GF(3)$. Si determini

(a) un generatore di $E^\times$ i cui coniugati di Galois non costituiscano una base normale di $E|F$;

(b) una base normale di $E|F$ i cui elementi non siano generatori di $E^\times$.

(È stato provato da Lenstra e Schoof che per ogni estensione di campi finiti $E|F$ esiste una base normale di $E|F$ costituita da generatori di $E^\times$.)

3 Campi ciclotomici

Sia F un campo. Una *radice dell'unità* in F è un elemento di ordine finito nel gruppo moltiplicativo $F^\times$ di F. Precisamente, dato un intero positivo n, se $\zeta \in F$ e $\zeta^n = 1$ (ovvero $o(\zeta)$ divide n), allora ζ si dice una *radice n-esima dell'unità*; se, inoltre, $\zeta^m \neq 1$ per ogni $1 \leq m < n$ (ovvero $o(\zeta) = n$), allora ζ si dice una radice *primitiva* n-esima dell'unità.
Sia F un campo e n un intero positivo. Definiamo

$$U_n(F) = \{a \in F \mid a^n = 1\} .$$

Proposizione 3.1. (i) *$U_n(F)$ è un sottogruppo ciclico di $F^\times$;*

Supponiamo che F contenga un campo di spezzamento per il polinomio $x^n - 1$. Allora:

(ii) *$|U_n(F)|$ divide n; $|U_n(F)| = n$ se e solo se $\mathrm{char}(F)$ non divide n;*

(iii) *se $\mathrm{char}(F)$ non divide n, allora F possiede esattamente $\varphi(n)$ radici primitive n-esime dell'unità (dove φ è la funzione di Eulero).*

Dimostrazione. (i) Chiaramente, $1_F \in U_n(F)$. Se $a, b \in U_n(F)$, allora $(ab^{-1})^n = a^n\,(b^n)^{-1} = 1_F$ e quindi $U_n(F)$ è un sottogruppo del gruppo moltiplicativo $F^\times$. Gli elementi di $U_n(F)$ sono radici del polinomio $x^n - 1$ e quindi $|U_n(F)| \leq n$. $U_n(F)$ è un sottogruppo di ordine finito di $F^\times$ e dunque è ciclico per [AII, Teorema 7.6].

Supponiamo ora che $x^n - 1$ si spezzi su F.

(ii) Sia $U_n(F) = \langle\zeta\rangle$; quindi $|U_n(F)| = o(\zeta)$ e $o(\zeta)$ divide n, dato che $\zeta^n = 1$.
Supponiamo che $p = \mathrm{char}(F)$ divida n; sia $n = pm$. Allora $x^n - 1 = (x^m)^p - 1^p = (x^m - 1)^p$ e quindi ogni $a \in U_n(F)$ verifica $a^m = 1$ con $m < n$; dunque non esistono radici primitive n-esime dell'unità in F.
Viceversa, se $\mathrm{char}(F) \nmid n$, allora il polinomio derivato $(x^n - 1)' = nx^{n-1}$ non ha radici a comune con $x^n - 1$, che quindi ha tutte radici semplici. Dato che $x^n - 1$ si spezza su F, segue $|U_n(F)| = n$.

(iii) Se $\mathrm{char}(F)$ non divide n, allora per i punti (i) e (ii) $U_n(F)$ è un gruppo ciclico di ordine n. I suoi generatori sono le radici primitive n-esime dell'unità, e sono in numero di $\varphi(n)$ (fissata una radice primitiva n-esima ζ, le altre sono tutte e sole le potenze ζ^k con $1 \leq k \leq n$ e $(k, n) = 1$). ∎

Osserviamo che la dimostrazione del punto (ii) della Proposizione precedente prova in effetti che se $p = \mathrm{char}(F)$ e $n = p^a m$ con $(p, m) = 1$, allora $U_n(F) = U_m(F)$.

Proposizione 3.2. *Sia $E|F$ una estensione di campi e $\zeta \in E$ una radice dell'unità. Allora $F[\zeta]|F$ è di Galois e $\mathrm{Gal}(F[\zeta]|F)$ è isomorfo ad un sottogruppo di $\mathrm{Aut}(()\langle\zeta\rangle)$; in particolare, $\mathrm{Gal}(F[\zeta]|F)$ è abeliano.*

Dimostrazione. Sia n l'ordine di ζ nel gruppo moltiplicativo $E^\times$. Dunque $f(x) = x^n - 1 \in F[x]$ è separabile e $F[\zeta]$ è un suo campo campo di spezzamento; pertanto, $F[\zeta]|F$ è di Galois.
L'applicazione $\alpha \mapsto m(\alpha)$, dove $\alpha(x) = x^{m(\alpha)}$, è un isomorfismo da $\mathrm{Aut}(\langle\zeta\rangle)$ nel gruppo moltiplicativo $(\mathbb{Z}_n)^\times$ di $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Inoltre l'applicazione che porta $\alpha \in \mathrm{Gal}(F[\zeta]|F)$ nella sua restrizione a $\langle\zeta\rangle$ è un omomorfismo iniettivo. ∎

Supponiamo, da ora in poi, che sia $F = \mathbb{C}$ il campo complesso, e scriviamo $U_n = U_n(\mathbb{C})$. Ricordiamo che $U_n = \{e^{\frac{2\pi k}{n}i} \mid 1 \leq k \leq n\}$ e che le radici primitive n-esime dell'unità in $\mathbb{C}$ sono gli elementi $e^{\frac{2\pi k}{n}i}$ con k coprimo con n.
Definiamo il *polinomio ciclotomico n-esimo*

$$\Phi_n(x) = \prod_{\substack{\zeta \in U_n \\ o(\zeta) = n}} (x - \zeta) \ .$$

Dunque le radici di $\Phi_n(x)$ sono tutte e sole le radici primitive n-esime dell'unità in $\mathbb{C}$. Proveremo che $\Phi_n(x)$ è un polinomio irriducibile a coefficienti interi.
Premettiamo un risultato sulla fattorizzazione di polinomi a coefficienti interi, conseguenza del Lemma di Gauss.

Lemma 3.3. *Sia $f \in \mathbb{Z}[x]$ un polinomio monico e sia $f = gh$ con $g, h \in \mathbb{Q}[x]$ e g, h monici. Allora $g, h \in \mathbb{Z}[x]$.*

DIMOSTRAZIONE. Sappiamo che ogni polinomio non nullo $q \in \mathbb{Q}[x]$ si scrive in modo unico (a meno del segno) nella forma $q = aq_0$ con $a \in \mathbb{Q}$ e $q_0 \in \mathbb{Z}[x]$ polinomio primitivo (vedi [AI, Lemma 8.13]). Osserviamo che se q è monico, allora $a = 1/d$ con $d \in \mathbb{Z}$. Scriviamo infatti $a = c/d$ con $c, d \in \mathbb{Z}$, $c > 0$ e $(c, d) = 1$. Allora $dq = cq_0$ e, confrontando i coefficienti direttivi, abbiamo che c divide d (in $\mathbb{Z}$) e quindi $c = 1$.
Scriviamo dunque $g = (1/u)g_0$ e $h = (1/v)h_0$ con $u, v \in \mathbb{Z}$ e g_0, h_0 polinomi primitivi a coefficienti interi. Dunque $uvf = g_0h_0$. Per il Lemma di Gauss ([AI, Lemma 8.14]) il polinomio g_0h_0 è primitivo; ma anche f lo è (dato che f è monico). Per l'unicità della rappresentazione menzionata nel paragrafo precedente, abbiamo $uv = 1$ e quindi, a meno di sostituire u e v con i loro opposti, $u = v = 1$ e $g = g_0$, $h = h_0$ sono polinomi a coefficienti interi. ∎

Proposizione 3.4. *Per ogni intero positivo n si ha:*

(i)

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

dove il prodotto è esteso a tutti gli interi positivi d divisori di n.

(ii) *$\Phi_n(x) \in \mathbb{Z}[x]$ è un polinomio monico di grado $\varphi(n)$;*

DIMOSTRAZIONE. Osservando che

$$x^n - 1 = \prod_{\zeta \in U_n} (x - \zeta)$$

il punto (i) segue osservando che (per il Teorema di Lagrange) U_n è unione disgunta dei sottoinsiemi $\{\zeta \in U_n \mid o(\zeta) = d\}$ delle radici primitive d-esime dell'unità, al variare di d nell'insieme dei divisori positivi di n.

È chiaro che $\Phi_n(x)$ è un polinomio monico di grado $\varphi(n)$. Ogni $\alpha \in \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ permuta l'insieme delle radici primitive n-esime dell'unità e quindi $\alpha(\Phi_n(x)) = \Phi_n(x)$. Dunque i coefficienti di $\Phi_n(x)$ appartengono a $Fix(\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) = \mathbb{Q}$. Proviamo, procedendo per induzione su n, che $\Phi_n(x)$ ha coefficienti interi. Chiaramente, $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Per ipotesi induttiva il polinomio

$$h(x) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$$

è un polinomio monico in $\mathbb{Z}[x]$. Dato che la divisione euclidea per un polinomio monico è possibile in $\mathbb{Z}[x]$ ed ha quoziente (e resto) univocamente determinati in $\mathbb{C}[x]$ ([AI, Teorema 8.4]), da $x^n - 1 = h(x)\Phi_n(x)$ segue $\Phi_n(x) \in \mathbb{Z}[x]$. ∎

Teorema 3.5. *I polinomi ciclotomici $\Phi_n(x)$ sono irriducibili in $\mathbb{Q}[x]$, per ogni intero $n \geq 1$.*

DIMOSTRAZIONE. Supponiamo, procedendo per assurdo, che (per un dato n) il polinomio ciclotomico $\Phi_n(x)$ sia riducibile in $\mathbb{Q}[x]$, e quindi per il Lemma 3.3 (oppure per [AI, Proposizione 8.15]) nemmeno in $\mathbb{Z}[x]$. Scriviamo $\Phi_n = fg$ con $f, g \in \mathbb{Z}[x]$ polinomi monici di grado positivo e f irriducibile (in $\mathbb{Z}[x]$ e quindi anche) in $\mathbb{Q}[x]$. L'insieme delle radici primitive n-esime dell'unità si può scrivere quindi come unione di due insiemi disgiunti e non vuoti, A e B, costituiti rispettivamente dalle radici di f e da quelle di g. Consideriamo $\alpha \in A$ e $\beta \in B$; dato che α è un generatore di U_n, esiste un intero k, con $1 \leq k \leq n$ e k coprimo con n, tale che sia $\beta = \alpha^k$. Scegliamo α e β in modo che k sia minimo. Allora, preso un divisore primo p di k (osserviamo che $k \neq 1$), abbiamo $(\alpha^{k/p})^p = \beta$. Per la scelta di k, $\alpha^{k/p} \in A$ e quindi (usando ancora la minimalità di k) $k = p$. Dunque $\beta = \alpha^p$ e pertanto α è radice del polinomio $g(x^p)$. Ma $f = \min_{\mathbb{Q}}(\alpha)$, quindi $f(x)$ divide $g(x^p)$ in $\mathbb{Q}[x]$: $g(x^p) = f(x)h(x)$ con $h(x) \in \mathbb{Q}[x]$ e $h(x)$ monico (osserviamo che sia $f(x)$ che $g(x^p)$ sono monici). Allora, per il Lemma 3.3, $h(x) \in \mathbb{Z}[x]$. Sia ora $F = \mathbb{Z}/p\mathbb{Z}$ e sia $^- : \mathbb{Z}[x] \to F[x]$ la riduzione modulo p. Ricordando che $a^p = a$ per ogni $a \in F$ e che $\mathrm{char}(F) = p$, segue

$$\overline{f(x)h(x)} = \overline{fh(x)} = \overline{g(x^p)} = \overline{g(x)^p} \, .$$

Dunque $\overline{f}$ e $\overline{g}$ hanno un fattore irriducibile in comune in $F[x]$. Poiché $fg = \Phi_n$ divide $x^n - 1$ in $\mathbb{Z}[x]$, abbiamo che $\overline{f}\overline{g}$ divide $\overline{x^n - 1}$ in $F[x]$ e quindi $\overline{x^n - 1} = x^n - \overline{1}$ ha una radice multipla. Ma questo è assurdo, perché (ricordando che p non divide n) il polinomio derivato $(x^n - \overline{1})' = \overline{n}x^{n-1}$ non ha radici a comune con $x^n - \overline{1}$. ∎

Denotiamo con $\mathbb{Q}_n$ il campo di spezzamento (in $\mathbb{C}$) del polinomio $x^n - 1$ su $\mathbb{Q}$. $\mathbb{Q}_n$ si dice l' *n-esimocampo ciclotomico*. Si osservi che $\mathbb{Q}_n = \mathbb{Q}[\zeta]$, dove ζ è una qualunque radice *primitiva* n-esima dell'unità in $\mathbb{C}$ e che l'estensione $\mathbb{Q}_n|\mathbb{Q}$ è di Galois (essendo campo di spezzamento del polinomio $x^n - 1$ separabile su $\mathbb{Q}$).
L'irriducibilità dei polinomi ciclotomici ha come conseguenza il seguente

Corollario 3.6. $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$.

DIMOSTRAZIONE. Basta osservare che $\mathbb{Q}_n = \mathbb{Q}[\zeta]$, dove ζ è una radice primitiva n-esima dell'unità, e che $\min_{\mathbb{Q}}(\zeta) = \Phi_n(x)$ per il Teorema 3.5. ∎

Determiniamo l'intersezione e il campo composto di due campi ciclotomici.

Proposizione 3.7. *Siano a e b due interi positivi. Allora*

(i) $\mathbb{Q}_a \cap \mathbb{Q}_b = \mathbb{Q}_{(a,b)}$;

(ii) $\mathbb{Q}_a\mathbb{Q}_b = \mathbb{Q}_{[a,b]}$.

DIMOSTRAZIONE. Siano $d = (a, b)$ e $m = [a, b]$, rispettivamente il massimo comun divisore e il minimo comune multiplo di a e b.
Osserviamo intanto che, dati due interi positivi x e y, se x divide y allora $\mathbb{Q}_x$ è contenuto in $\mathbb{Q}_y$ (dato che le radici x-esime dell'unità sono anche radici y-esime). Dunque $\mathbb{Q}_d \leq \mathbb{Q}_a \cap \mathbb{Q}_b$ e $\mathbb{Q}_a\mathbb{Q}_b \leq \mathbb{Q}_m$.
Osserviamo inoltre che $U = \langle U_a, U_b \rangle$ è un sottogruppo di U_m di ordine multiplo di a e di b, e quindi $m = [a, b]$ divide $|U|$. Ma U è ciclico (è sottogruppo del gruppo ciclico U_m) e dunque contiene un elemento di ordine m. Concludiamo quindi che $Q_m \leq \mathbb{Q}[U] = \mathbb{Q}_a\mathbb{Q}_b$ e quindi $Q_m = \mathbb{Q}_a\mathbb{Q}_b$.
Per il Teorema 2.7 $[\mathbb{Q}_a : \mathbb{Q}_a \cap \mathbb{Q}_b] = [\mathbb{Q}_a\mathbb{Q}_b : \mathbb{Q}_b] = [\mathbb{Q}_m : \mathbb{Q}_b] = \varphi(m)/\varphi(b)$. Segue $\varphi(a)\varphi(b) = \varphi(m)[\mathbb{Q}_a \cap \mathbb{Q}_b : \mathbb{Q}]$.
Ma $\varphi(a)\varphi(b) = \varphi(m)\varphi(d)$ per l'Esercizio 3.1 e quindi segue $[\mathbb{Q}_a \cap \mathbb{Q}_b : \mathbb{Q}] = \phi(d) = [\mathbb{Q}_d : \mathbb{Q}]$ e dunque $\mathbb{Q}_a \cap \mathbb{Q}_b = \mathbb{Q}_d$. ∎

Procediamo ora a studiare la struttura del gruppo di Galois di una estensione ciclotomica. Proviamo intanto che $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ è isomorfo al gruppo moltiplicativo degli elementi invertibili dell'anello delle classi di resto modulo n; in particolare, quindi, è un gruppo abeliano.
Nel seguito, con un certo abuso di notazione, indichiamo con $A^\times$ il gruppo moltiplicativo degli elementi *invertibili* di un anello A.

Teorema 3.8.

$$\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \simeq \mathrm{Aut}(U_n) \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times .$$

DIMOSTRAZIONE. Ricordiamo intanto che, dato che U_n è un gruppo ciclico di ordine n, il suo gruppo di automorfismi è isomorfo al gruppo moltiplicativo delle unità di $\mathbb{Z}/n\mathbb{Z}$. Scriviamo infatti $U_n = \langle \zeta \rangle$ e consideriamo l'applicazione $\phi : \mathrm{Aut}(U_n) \to \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ definita, per $\alpha \in \mathrm{Aut}(U_n)$, da $\phi(\alpha) = k$ dove $1 \leq k \leq n$ è l'intero positivo tale che $\alpha(\zeta) = \zeta^k$ (dato che l'automorfismo α porta generatori in generatori, k è coprimo con n). Si verifica che ϕ è un isomorfismo di gruppi.
Dato poi $\alpha \in \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$, la restrizione α_{U_n} è un automorfismo del gruppo U_n. L'applicazione $\psi : \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \to \mathrm{Aut}(U_n)$, $\alpha \mapsto \alpha_{U_n}$ è un omomorfismo di gruppi (verificarlo); inoltre ψ è iniettivo poichè $\mathbb{Q}_n = \mathbb{Q}[U_n]$. Infine, dato che $|\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})| = [\mathbb{Q}_n : \mathbb{Q}] = \varphi(n) = |\mathrm{Aut}(U_n)|$, ψ è anche suriettivo, e quindi un isomorfismo. ∎

Il seguente teorema descrive la struttura del gruppo degli automorfismi di un gruppo ciclico.

Teorema 3.9. (a) *Sia C un gruppo ciclico di ordine $n = p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$, con $p_1, p_2, \ldots, p_m$ primi distinti. Allora*

$$\mathrm{Aut}(C) = \mathrm{Aut}(C_1) \times \mathrm{Aut}(C_2) \times \cdots \times \mathrm{Aut}(C_n)$$

dove C_i è il p_i sottogruppo di Sylow di C, per $i = 1, 2, \ldots, n$.

(b) *Sia C ciclico di ordine p^a, con p primo e $a \geq 1$. Allora,*

- **(i)** *se $p \neq 2$, allora $\mathrm{Aut}(C)$ è ciclico di ordine p^{a-1};*
- **(ii)** *se $p = 2$ e $a \geq 3$, allora $\mathrm{Aut}(C) \cong A_1 \times A_2$ con A_1 ciclico di ordine 2 e A_2 ciclico di ordine 2^{a-2}; se $|C| = 2$, allora $\mathrm{Aut}(C) = \{id\}$; se $|C| = 4$, allora $\mathrm{Aut}(C)$ è un gruppo ciclico di ordine 2.*

Premettiamo due risultati:

Lemma 3.10. *Sia G un gruppo finito e siano $N_1, N_2, \ldots, N_m$, $m \geq 2$, sottogruppi normali di G di ordini a due a due coprimi: $(|N_i|, |N_j|) = 1$ per $1 \leq i, j \leq m$, $i \neq j$. Supponiamo inoltre che sia $|G| = |N_1| \cdot |N_2| \cdots |N_m|$. Allora*

(a) $G = N_1 \times N_2 \times \cdots \times N_m$;

(b) $\mathrm{Aut}(G) = \mathrm{Aut}(N_1) \times \mathrm{Aut}(N_2) \times \cdots \times \mathrm{Aut}(N_m)$.

Dimostrazione. (a) Ricordiamo che il prodotto di sottogruppi normali di G è un ancora un sottogruppo normale di G. Proviamo, per induzione su k, che se $N_1, N_2, \ldots, N_k$, $k \geq 2$, sono sottogruppi normali di G di ordini a due a due coprimi, allora

$$|N_1 N_2 \cdots N_k| = |N_1| \cdot |N_2| \cdots |N_k| \,. \qquad (\star)$$

Infatti, se $k = 2$, allora $|N_1 N_2| = |N_1||N_2|/(N_1 \cap N_2) = |N_1||N_2|$ (dato che da $(|N_1|, |N_2|) = 1$ segue $N_1 \cap N_2 = 1$). Se $k \geq 3$, poniamo $H = N_1 N_2 \cdots N_{k-1}$ e ci riconduciamo al caso precedente osservando che $H \trianglelefteq G$ e che $|H| = |N_1| \cdot |N_2| \cdots |N_{k-1}|$ per ipotesi induttiva. Il punto (a) segue poi immediatamente da $(\star)$, ancora per induzione sul numero dei sottogruppi normali.

(b) Proviamo intanto il seguente fatto di carattere generale: se N è un sottogruppo normale di un gruppo finito G e $(|N|, |G/N|) = 1$, allora $\alpha(N) = N$ per ogni $\alpha \in \mathrm{Aut}(G)$ (ovvero N è un sottogruppo *caratteristico* di G). Ponendo infatti $M = \alpha(N)$, abbiamo che $NM \leq G$ e quindi $|NM/N|$ divide $|G/N|$. Ma $|NM/N| = |N/N \cap M|$ (per il secondo teorema di omomorfismo) e quindi $|NM/N|$ divide anche $|N|$. Da $(|N|, |G/N|) = 1$ segue quindi $NM = N$, cioè $M = N$.
Vediamo quindi che tutti i sottogruppi N_i sono caratteristici in G e pertanto, per ogni $\alpha \in \mathrm{Aut}(G)$, la restrizione α_{N_i} è un automorfismo di N_i. Consideriamo l'applicazione

$$\phi : \mathrm{Aut}(G) \to \mathrm{Aut}(N_1) \times \mathrm{Aut}(N_2) \times \cdots \times \mathrm{Aut}(N_m)$$

definita da $\phi(\alpha) = (\alpha_{N_1}, \alpha_{N_2}, \ldots, \alpha_{N_m})$. Si verifica facilmente che ϕ è un omomorfismo iniettivo. Infine, prendendo $\alpha_1 \in \mathrm{Aut}(N_1), \alpha_2 \in \mathrm{Aut}(N_2), \ldots, \alpha_m \in \mathrm{Aut}(N_m)$,

l'applicazione $\alpha : G \to G$ definita, per $g = n_1 n_2 \cdots n_m \in G$, con $n_i \in N_i$, da $\alpha(g) = \alpha_1(n_1)\alpha_2(n_2)\cdots\alpha_m(n_m)$ è un automorfismo di G. Quindi ϕ è suriettiva e dunque un isomorfismo. ∎

Dati un primo p e un intero positivo n, scriviamo $p^a \top n$ se p^a è la massima potenza di p che divide n, ovvero $n = p^a m$ con m intero coprimo con p.

Lemma 3.11. *Sia p un primo, n un intero positivo e sia $p^b \top n-1$. Allora vale $p^{b+1} \top n^p - 1$ se $p \neq 2$ oppure se $p = 2$ e $b \geq 2$.*

Dimostrazione. Poniamo $k = n - 1$; dunque $p^b \top k$. Supponendo $p \neq 2$, osserviamo che

$$n^p = (1+k)^p = 1 + pk + \sum_{i=2}^{p} \binom{p}{i} k^i$$

e che ogni addendo della sommatoria più a destra è divisibile per p^{b+2}. Dunque p^{b+1} divide $n^p - 1$, ma p^{b+2} non lo divide (dato che $p^{b+1} \top pk$); quindi $p^{b+1} \top n^p - 1$.
Supponiamo ora $p = 2$ e $b \geq 2$. Allora $(1+k)^2 = 1 + 2k + k^2$ e concludiamo osservando che 2^{2b} divide k^2 e che $2b > b + 1$ perché $b > 1$. ∎

Dimostrazione. [Dimostrazione del Teorema 3.9] La parte (a) segue subito applicando il Lemma 3.10.

(b) Ricordiamo che se $C = \langle x \rangle$ è un gruppo ciclico di ordine n, l'applicazione $\alpha \mapsto m(\alpha)$, dove $\alpha(x) = x^{m(\alpha)}$, è un isomorfismo da $\mathrm{Aut}(C)$ nel gruppo moltiplicativo $(\mathbb{Z}_n)^\times$ di $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Proviamo allora che se p è un primo dispari allora $(\mathbb{Z}_{p^a})^\times$ è ciclico, e che $(\mathbb{Z}_{2^a})^\times = \langle -\overline{1} \rangle \times \langle \overline{5} \rangle$ per $a \geq 3$ (è chiaro che $(\mathbb{Z}_2)^\times = \{\overline{1}\}$ e che $(\mathbb{Z}_{2^2})^\times = \langle -\overline{1} \rangle$).
Supponiamo intanto $p \neq 2$ e consideriamo l'omomorfismo suriettivo $\psi : (\mathbb{Z}_{p^a})^\times \to (\mathbb{Z}_p)^\times$ definito da $\psi(m + p^a\mathbb{Z}) = m + p\mathbb{Z}$. Allora $C/\ker(\psi)$ è isomorfo al gruppo moltiplicativo $(\mathbb{Z}_p)^\times$ del campo $\mathbb{Z}_p$ ed è quindi ciclico di ordine $p-1$. Osserviamo anche che $|\ker(\psi)| = \left|(\mathbb{Z}_{p^a})^\times\right| / \left|(\mathbb{Z}_p)^\times\right| = \varphi(p^a)/\varphi(p) = p^{a-1}$, quindi $\ker(\psi)$ è un p-sottogruppo di Sylow di $(\mathbb{Z}_{p^a})^\times$. Proviamo che $\ker(\psi) = \langle \overline{1+p} \rangle$. Chiaramente $\overline{1+p} \in \ker(\psi)$ e quindi basta far vedere che l'ordine di $\overline{1+p}$ in $(\mathbb{Z}_{p^a})^\times$ è p^{a-1}; ma ciò segue dall'utilizzo ripetuto del Lemma 3.11 (con $n = 1 + p$). Concludiamo osservando che allora $(\mathbb{Z}_{p^a})^\times = P_1 \times P_2 \times \cdots P_d \times \ker(\psi)$, dove $P_1, P_2, \ldots, P_d$ sono i sottogruppi di Sylow di $(\mathbb{Z}_{p^a})^\times$ corrispondenti ai divisori primi di $p-1$. Dunque $(\mathbb{Z}_{p^a})^\times$ è ciclico in quando prodotto diretto di gruppi ciclici di ordini a due a due coprimi.
Supponiamo ora $p = 2$, $a \geq 3$, e sia $\psi\,(\mathbb{Z}_{2^a})^\times \to (\mathbb{Z}_4)^\times$ definito da $\psi(m + 2^a\mathbb{Z}) = m + 4\mathbb{Z}$. Applicando di nuovo il Lemma 3.11 (con $n = 5$) abbiamo che $\overline{5}$ ha ordine 2^{a-2} in $(\mathbb{Z}_{2^a})^\times$. Dato che ψ è suriettivo, abbiamo $|\ker(\psi)| = |\,(\mathbb{Z}_{2^a})^\times\,|/|\,(\mathbb{Z}_4)^\times\,| = 2^{a-2}$ e quindi, poiché $\overline{5} \in \ker(\psi)$, segue $\ker(\psi) = \langle \overline{5} \rangle$. Infine, $\langle -\overline{1} \rangle \cap \ker(\psi) = 1$ e $|\,(\mathbb{Z}_{2^a})^\times\,| = 2|\ker(\psi)|$. Quindi $(\mathbb{Z}_{2^a})^\times = \langle -\overline{1} \rangle \times \ker(\psi) = \langle -\overline{1} \rangle \times \langle \overline{5} \rangle$. ∎

Esercizio 3.1. Siano a e b interi positivi, $d = (a, b)$ e $m = [a, b]$. Si provi che $\varphi(a)\varphi(b) = \varphi(m)\varphi(d)$. (Sugg.: per la moltipicatività della funzione di Eulero, ci si puo' ricondurre al caso in cui a e b siano potenze dello stesso primo).

Esercizio 3.2. Si scrivano esplicitamente i polinomi ciclotomici $\Phi_n(x)$ per $2 \leq n \leq 10$.

Esercizio 3.3. Si determinino i campi intermedi delle estensioni ciclotomiche $\mathbb{Q}_8|\mathbb{Q}$ e $\mathbb{Q}_{14}|\mathbb{Q}$.

Esercizio 3.4. Sia $n \geq 3$ un intero. Si provi che $\Phi_{2n}(x) = \Phi_n(-x)$.

Esercizio 3.5. Si provi che $\Phi_n(0) = \pm 1$ per ogni intero positivo n

Esercizio 3.6. Si provi che se n è un intero positivo divisibile per il quadrato p^2 di un qualche primo p, allora la somma di tutte le radici primitive n-esime dell'unità in $\mathbb{C}$ è zero.

Esercizio 3.7. Si provi che se n e m sono interi positivi coprimi, allora $\Phi_n(x)$ è irriducibile in $\mathbb{Q}_m[x]$.

Esercizio 3.8. Sia F un campo finito di ordine q (dove $q = p^a$, con p primo), n un intero positivo tale che $(n, q) = 1$ e sia K un campo di spezzamento del polinomio $x^n - 1$ su F. Si provi che $[K : F]$ coincide con l'ordine di q nel gruppo moltiplicativo $\mathbb{Z}_n^\times$. (Suggerimento: si ricordi che il gruppo di Galois $\mathrm{Gal}(K|F)$ è generato dall automorfismo $\alpha : K \to K$, $a \mapsto a^q$.)

Esercizio 3.9. Sia $\zeta = \zeta_n$ una radice primitiva n-esima dell'unità (n intero positivo). Si determinino gli interi n per cui i coniugati di Galois di ζ costituiscono una base normale di $\mathbb{Q}_n|\mathbb{Q}$.

4 Gruppi

Definizione 2. *Sia G un gruppo. Una* serie *di G è una catena di sottogruppi (*termini *della serie)*

$$1 = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{n-1} \leq H_n = G$$

tali che, per $i \in \{0, 1, \ldots, n-1\}$ sia $H_i \trianglelefteq H_{i+1}$, ovvero ognuno dei gruppi della catena è sottogruppo normale del successivo. I gruppi quoziente H_{i+1}/H_i si dicono fattori *della serie. Se tutti i sottogruppi H_i sono distinti, il numero n si dice* lunghezza *della serie. Se inoltre ogni H_i è normale in G, allora la serie si dice* normale.

Esempio. (1) $1 \leq \langle(12)\rangle \leq \langle(12), (34)\rangle \leq A_4 \leq S_4$ è una serie del gruppo simmetrico S_4 (ma non è una serie normale, perché $\langle(12)\rangle$ non è normale in S_4.).

(2) Ogni catena di sottogruppi di un gruppo abeliano è una serie normale. Chiaramente, $1 \leq G$ è una serie normale in un qualsiasi gruppo G.
(Ricordiamo che la normalità non è (in generale) una relazione transitiva; ovvero, da $N \trianglelefteq M \trianglelefteq L$ non segue $N \trianglelefteq L$.)

Una serie $1 = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{n-1} \leq H_n = G$ si dice *raffinabile* se per almeno un $i \in \{0, 1, \ldots, n-1\}$ esite un sottogruppo K di G con $H_i \leq K \trianglelefteq H_{i+1}$ e $H_i \neq K \neq H_{i+1}$. Una serie a termini distinti e non raffinabile di un gruppo G si dice una *serie di composizione* di G. Osserviamo che una serie di G è di composizione se e solo se tutti i suoi fattori sono gruppi semplici.
Definiamo ora una importante classe dei gruppi: quella dei gruppi *risolubili*.

Definizione 3. *Un gruppo G si dice* risolubile *se esiste una serie di G $1 = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{n-1} \leq H_n = G$ tale che H_{i+1}/H_i sia abeliano per ogni $i \in \{0, 1, \ldots, n-1\}$.*

Dunque, un gruppo è risolubile se ha una serie a fattori abeliani. Dato che ogni serie a termini distinti di un gruppo finito si puó raffinare, in un numero finito di passi, fino ad ottenere una serie di composizione, vediamo che i gruppi finiti risolubili sono esattamente quelli che possiedono una serie di composizione con fattori di ordine primo.
Esempio. (1) Il gruppo simmetrico S_3 è risolubile: $1 \leq \langle (1,2,3) \rangle \leq S_3$ è una serie a fattori abeliani (anzi ciclici). Anche il gruppo simmetrico S_4 è risolubile: vedi la serie riportata nell'esempio più sopra.
I gruppi S_n con $n \geq 5$ non sono invece risolubili: i sottogruppi alterni A_n sono infatti semplici per $n \geq 5$ e non abeliani (e quindi non risolubili).

(2) I gruppi abeliani sono chiaramente risolubili. Anche i p-gruppi finiti sono risolubili (si consideri ad esempio la serie centrale ascendente).
La dimostrazione della proposizione seguente è lasciata per esercizio.

Proposizione 4.1. *Sia G un gruppo risolubile.*

(a) *Se H è un sottogruppo di G, allora anche H è risolubile.*

(b) *Sia $N \trianglelefteq G$; allora G è risolubile se e solo se N e G/N sono risolubili.*

5 Estensioni radicali e Teorema di Galois

Consideriamo ora polinomi di tipo particolare, ovvero quelli della forma

$$x^n - b$$

dove n è un intero positivo e $b \neq 0$. (Una equazione del tipo $x^n - b = 0$ viene detta *equazione pura*).

Diremo che una estensione di campi è una *estensione radicale* se $E = F[a]$, dove a è una radice di un polinomio della forma $x^n - b$, con $b \in F$ (ovvero $a^n = b$). In altri termini, una estensione $E|F$ è una estensione radicale se e solo se è semplice ed è generata su F da un elemento $a \in E$ tale che $a^n \in F$ per un opportuno intero positivo n.
Le estensioni $E|F$ di campi finiti e le estensioni ciclotomiche $\mathbb{Q}_n|\mathbb{Q}$ sono esempi di estensioni radicali.
Procediamo alla caratterizzazione delle estensioni radicali, nell'ipotesi che il campo base contenga "abbastanza" radici dell'unità.
Ricordiamo che un elemento ζ di un campo F si dice una radice primitiva n-esima dell'unità se $\zeta^n = 1$ e $\zeta^k \neq 1$ per ogni $1 \leq k < n$, ovvero se n è l'ordine di ζ nel gruppo moltiplicativo $F^\times$.
Ricordiamo che se un campo F contiene una radice primitiva n-esima, allora la caratteristica di F non divide n (ovvero, $\mathrm{char}(F) = 0$ oppure $\mathrm{char}(F) = p$ con $(p, n) = 1$). Infatti se $n = mp$, dove $p = \mathrm{char}(F)$ è un primo, allora $x^n - 1 = (x^m)^p - 1 = (x^m - 1)^p$ e quindi le radici n-esime dell'unità in F sono in realtà radici m-esime dell'unità, con $m < n$.

Teorema 5.1 (Kummer)**.** *Sia n un intero positivo e F un campo che contenga una radice primitiva n-esima dell'unità; Data una estensione $E|F$, sono equivalenti:*

(a) *$E = F[a]$ per un elemento $a \in E$ tale che $a^n \in F$*

(b) *$E|F$ è una estensione di Galois, $G = \mathrm{Gal}(E|F)$ è un gruppo ciclico e $|G|$ divide n.*

Dimostrazione. Supponiamo che $E|F$ sia di Galois e che $G = \mathrm{Gal}(E|F) = \langle\alpha\rangle$ sia ciclico di ordine d, con d divisore di n. Sia $\zeta \in F$ una radice d-esima primitiva dell'unità (F contiene radici primitive d-esime dell'unità perché contiene radici primitive n-esime e $d \mid n$).
Per il Teorema 2.4 esiste almeno un elemento $b \in E$ tale che sia $a = \sum_{i=1}^{d} \zeta^{-i}\alpha^i(b) \neq 0$. Notiamo che

$$\alpha(a) = \sum_{i=1}^{d} \zeta^{-i}\alpha^{i+1}(b) = \zeta \sum_{i=1}^{d} \zeta^{-(i+1)}\alpha^{i+1}(b) = \zeta a \ .$$

Considerando che ζ è fissato da α, si ha quindi $\alpha^i(a) = \zeta^i a$ per ogni $i \in \{1, 2, \ldots, d\}$. Poiché ζ è una radice primitiva n-esima dell'unità, e $a \neq 0$, segue $\alpha^i(a) \neq a$ per ogni $1 \leq i \leq d - 1$. Dunque $\mathrm{Gal}(E|F[a]) = 1$ e quindi $F[a] = E$. Infine, $\alpha(a^n) = \alpha(a)^n = \zeta^n a^n = a^n$, ovvero $a^n \in \mathrm{Inv}(\langle\alpha\rangle) = F$.

Supponiamo viceversa che valga (b), ovvero che sia $E = F[a]$ con $a^n \in F$. Sia $f(x) = x^n - a^n \in F[x]$ e sia $\zeta \in F$ una radice primitiva n-esima dell'unità. Allora, per ogni $1 \leq k \leq n$ gli elementi $\zeta^k a$ sono radici distinte di $f(x)$; quindi $f(x)$ ha $n = deg(f)$ radici

in E. Pertanto $f(x)$ ha radici distinte in E (e quindi $f(x)$ è separabile su F) e $E = F[\alpha]$ è un campo di spezzamento per $f(x)$ su F. Dunque $E|F$ è una estensione di Galois.
Per concludere la dimostrazione, proviamo che $G = \mathrm{Gal}(E|F)$ è isomorfo ad un sottogruppo di $\langle\zeta\rangle$. Osserviamo che, dato che G permuta le radici di $f(x)$, per ogni $\sigma \in G$ vale $\sigma(a) = \delta a$ per un opportuno $\delta \in \langle\zeta\rangle$. Possiamo assumere che sia $a \neq 0$, altrimenti $G = 1$, e definiamo quindi l'applicazione $\omega : G \to \langle\zeta\rangle$ ponendo, per $\sigma \in G$, $\omega(\sigma) = \sigma(a)a^{-1}$. Per $\sigma, \tau \in G$, abbiamo

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

poiché $\langle\zeta\rangle \subseteq F$ (e $\langle\zeta\rangle$ è commutativo). Quindi ω è un omomorfismo di gruppi. Infine, se per $\sigma \in G$ vale $\omega(\sigma) = 1$, allora $\sigma(a) = a$ e quindi σ fissa ogni elemento di $E = F[a]$, ovvero $\sigma = 1$ e ω è pertanto un omomorfismo iniettivo. ∎

Definizione 4. *Una estensione di campi $E|F$ si dice* estensione multiradicale *se esistono campi intermedi F_i con*

$$F = F_0 \leq F_1 \leq \ldots \leq F_k = E$$

con $F_i|F_{i-1}$ estensione radicale per $1 \leq i \leq k$, ovvero esistono elementi $a_i \in F_i$ e interi positivi n_i tali che $F_i = F_{i-1}[a_i]$ e $a_i^{n_i} \in F_{i-1}$ per $1 \leq i \leq k$.

Definizione 5. *Sia F un campo e $f \in F[x]$ un polinomio non nullo. Il polinomio f (oppure l'equazione $f(x) = 0$) si dice* risolubile per radicali su F *se esiste una estensione multiradicale $E|F$ che contiene un campo di spezzamento per f su F.*

Osserviamo che nella definizione precedente non si richiede che il campo di spezzamento di f su F sia esso stesso una estensione multiradicale (Ad esempio: i polinomi irriducibili su $\mathbb{Q}$ di grado 3 che hanno tutte le radici reali, hanno campi di spezzamento che non sono estensioni multiradicali).
Il lemma seguente è impiegato per risolvere il problema tecnico della possibile mancanza delle radici dell'unità necessarie per applicare il Teorema di Kummer (Teorema 5.1).

Lemma 5.2. *Siano, per $1 \leq i \leq k$, F_i campi tali che $F = F_0 \leq F_1 \leq \ldots \leq F_k = L$ e con $F_i|F_{i-1}$ estensione di Galois con gruppo di Galois abeliano. Sia E un campo intermedio dell'estensione $L|F$ e supponiamo che $E|F$ sia un'estensione di Galois. Allora* $\mathrm{Gal}(E|F)$ *è un gruppo risolubile.*

Dimostrazione. Procediamo per induzione sulla lunghezza k della torre di campi. Se $k = 0$, allora $L = F$, quindi $E = F$ e $\mathrm{Gal}(E|F)$ è il gruppo banale. Supponiamo $k \geq 1$ e poniamo $E_1 = EF_1$ (campo composto) e $K = E \cap F_1$. Per il Teorema 2.7, $E_1|F_1$ è di Galois e che $\mathrm{Gal}(E|K) \cong \mathrm{Gal}(E_1|F_1)$. Quindi, applicando l'ipotesi induttiva alla torre di campi da F_1 a L, abbiamo che $\mathrm{Gal}(E_1|F_1)$, e quindi $\mathrm{Gal}(E|K)$, è risolubile.

Osserviamo ora che K è un campo intermedio dell'estensione $F_1|F$ con gruppo di Galois $\mathrm{Gal}(F_1|F)$ abeliano. Per la Corrispondenza di Galois, $K|F$ è una estensione normale, e quindi di Galois, e $\mathrm{Gal}(K|F) \cong \mathrm{Gal}(F_1|F)/\mathrm{Gal}(F_1|K)$. Dunque $\mathrm{Gal}(K|F)$ è risolubile. Abbiamo poi che, vedendo K come campo intermedio di $E|F$, $N = \mathrm{Gal}(K|F)$ è un sottogruppo normale di $G = \mathrm{Gal}(E|F)$ (perchè $K|F$ è una estensione normale), e sia N che $G/N \cong \mathrm{Gal}(E|K)$ sono risolubili. Quindi per il Lemma 4.1, G è risolubile. ∎

Veniamo infine al celebre Teorema di Galois:

Teorema 5.3 (Galois)**.** *Sia F un campo di caratteristica 0, $f \in F[x]$ un polinomio non nullo e E un campo di spezzamento per f su F. Allora f è risolubile per radicali se e solo se il gruppo di Galois $\mathrm{Gal}(E|F)$ è risolubile.*

Dimostrazione. Supponiamo che f sia risolubile per radicali e sia L una estensione multiradicale che contiene un campo di spezzamento E per f su F. Esiste quindi una torre di campi

$$F = F_1 \leq F_2 \leq \ldots \leq F_k = L$$

ed una lista di elementi $a_i \in F_i$ tali che $a_i^{n_i} \in F_{i-1}$, con n_i interi positivi, per $i \in \{2, \ldots, k\}$.
Sia m un multiplo comune degli interi n_i, $2 \leq i \leq k$, e sia M un campo di spezzamento per il polinomio $x^m - 1$ su L. Dato che la caratteristica di M è 0 (e quindi in particolare non divide m), per la Proposizione 3.1 esiste in M una radice primitiva m-esima dell'unità ζ. Definiamo $L_0 = F$ e, per $i = 1, 2, \ldots, k$, $L_i = F_i[\zeta]$. Notiamo che $L_k = M$. Per provare che $\mathrm{Gal}(E|F)$ è risolubile, usando il Lemma 5.2, consideriamo la torre di campi

$$F = L_0 \leq L_1 \leq \ldots \leq L_k = M$$

e mostriamo che i gruppi di Galois $\mathrm{Gal}(L_i|L_{i-1})$ sono tutti abeliani. Osserviamo intanto che $L_1|L_0 = F[\zeta]|F$ e quindi $\mathrm{Gal}(L_1|L_0)$ è abeliano per il Teorema 3.8. Per $2 \leq i \leq k$ abbiamo $L_i = L_{i-1}[a_i]$ e $a_i^{n_i} \in L_{i-1}$. Dato che $F[\zeta] = L_1 \leq L_{i-1}$ e $n_i \mid n$, L_{i-1} contiene radici primitive n_i-esime dell'unità e quindi $\mathrm{Gal}(L_i|L_{i-1})$ è abeliano per il Teorema 5.1. Dal Lemma 5.2 segue quindi che $\mathrm{Gal}(E|F)$ è risolubile.

Assumiamo ora che $\mathrm{Gal}(E|F)$ sia risolubile, dove E è un campo di spezzamento per f su F. Sia $n = [E : F]$ e sia M un campo di spezzamento su E del polinomio $x^n - 1$. Dato che $\mathrm{char}(E) = 0$ non divide n, esiste $\zeta \in M$ radice primitiva n-esima dell'unità. Consideriamo $L = F[\zeta]$ e osserviamo che $M = E[\zeta] = EL$. Per il Teorema 2.7, $\mathrm{Gal}(M|L) \cong \mathrm{Gal}(E|E \cap L)$ e quindi $H = \mathrm{Gal}(M|L)$ è risolubile, perché isomorfo ad un sottogruppo di un gruppo risolubile. Sia

$$1 \leq H_0 \leq H_1 \leq \ldots \leq H_t = H$$

una serie di composizione per H. Dato che H è risolubile (e ogni gruppo semplice abeliano ha ordine primo), è $|H_i/H_{i-1}| = p_i$, con p_i primo, per ogni $1 \leq i \leq t$. Denotiamo, per $1 \leq i \leq t$, con $L_i = \mathrm{Fix}(H_i)$ il campo degli invarianti del sottogruppo H_i. Abbiamo quindi la torre di campi

$$L = L_t \leq L_{t-1} \leq \ldots \leq L_0 = M$$

dove $L_{i-1}|L_i$ è di Galois e $\mathrm{Gal}(L_{i-1}|L_i)$ è un gruppo di ordine primo p_i e quindi ciclico, per ogni $1 \leq i \leq r$. Per il Teorema di Kummer (Teorema 5.1) dunque tutte le estensioni $L_{i-1}|L_i$ sono estensioni radicali (ovvero esiste $a_i \in L_{i-1}$ tale che $a_i^{p_i} \in L_i$). Ma anche $L|F$ è radicale (dato che $L = F[\zeta]$) e quindi M è una estensione multiradicale. Dunque f è risolubile per radicali su F. ∎

Diamo ora alcuni esempi di polinomi non risolubili per radicali su $\mathbb{Q}$. Premettiamo un lemma di teoria dei gruppi.

Lemma 5.4. *Sia p un numero primo e G un sottogruppo transitivo risolubile del gruppo simmetrico S_p. Allora G è contenuto in $\mathrm{N}_{S_p}(P)$, dove P è un opportuno p-sottogruppo di Sylow di S_p, e $p \mid |G| \mid p(p-1)$. Inoltre, ogni elemento di G fissa al più un elemento di $\{1, 2, \ldots, p\}$.*

Dimostrazione. Dato che G è transitivo e risolubile, e dato che $|S_p| = p(p-1)!$ e $(p, (p-1)!) = 1$, G contiene un p-sottogruppo di Sylow P di S_p e per l'Esercizio 5.4 $P \trianglelefteq G$.
Dunque G è un sottogruppo del normalizzante $\mathrm{N}_{S_p}(P)$, che ora andiamo a studiare. Scriviamo $P = \langle \alpha \rangle$. Dunque α un elemento di ordine p e (dalla decomposizione in cicli), abbiamo che α è un p-ciclo.
Viceversa, ogni p-ciclo genera un p-sottogruppo di Sylow di S_p e S_p contiene $p!/p$ p-cicli. Considerando che ogni sottogruppo di Sylow contiene $p-1$ elementi di ordine p e che due p-sottogruppi di Sylow distinti hanno intersezione banale, abbiamo che il numero $n_p(S_p)$ dei p-sottogruppi di Sylow di S_p è $(p-2)!$. Da $n_p(S_p) = [S_p : \mathrm{N}_{S_p}(P)]$ segue quindi $|\mathrm{N}_{S_p}(p)| = p(p-1)$.
Consideriamo ora il campo $F = \mathbb{Z}/p\mathbb{Z}$ e l'insieme di applicazioni

$$A(p) = \{\alpha : F \to F, \alpha(x) = ax + b \mid x, a, b \in F, a \neq 0\} .$$

Si verifica direttamente (esercizio) che $A(p)$ è un gruppo (sottogruppo del gruppo simmetrico $Sym(F)$; $A(p)$ si dice sottogruppo *affine* di $Sym(F)$); $|A(p)| = p(p-1)$. L'insieme (delle traslazioni) $T = \{\alpha \in A(p), \alpha(x) = x + b \mid x, b \in F\}$ è un sottogruppo normale (verificare) di $A(p)$ e $|T| = p$. Identificando (tramite una biiezione fra F e $\{1, 2, \ldots, p\}$) $A(p)$ con un sottogruppo di S_p, vediamo che T è un p-sottogruppo di Sylow di S_p; a meno di coniugio, possiamo quindi supporre $T = P$ e quindi $A(p) = \mathrm{N}_{S_p}(P)$. Pertanto,

$G \leq A(p)$. Concludiamo osservando che, come si verifica direttamente, gli elementi di $A(p)$ hanno al più un punto fisso nella loro azione su $F = \{1, 2, \ldots, p\}$. ∎

Proposizione 5.5. *Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado p primo. Se f è risolubile per radicali, allora ha una sola radice reale in $\mathbb{C}$ oppure tutte le radici di f in $\mathbb{C}$ sono reali.*

Dimostrazione. Possiamo supporre $p \neq 2$. Dato che f è un polinomio di grado dispari, f ha almeno una radice reale a. Supponiamo che esita un'altra radice $b \neq a$ di f tale che $b \in \mathbb{R}$ e sia $K = \mathbb{Q}[\alpha, \beta]$. Sia E il campo di spezzamento di f in $\mathbb{C}$; proviamo che $E = K$, mostrando che $\mathrm{Gal}(E|K) = 1$. Osserviamo che $H = \mathrm{Gal}(E|K)$ è un sottogruppo del gruppo $G = \mathrm{Gal}(E|\mathbb{Q})$. Dato che f è irriducibile in $\mathbb{Q}[x]$, G opera transitivamente (e fedelmente) sull'insieme, di cardinalità p, delle radici di f in $\mathbb{C}$. Poiché G è risolubile, dal Lemma 5.4 abbiamo che l'unico elemento di G che fissa almeno due radici di f è l'identità. Segue quindi $H = 1$ e, per la corrispondenza di Galois, $E = K$. Ma, dato che $\alpha, \beta \in \mathbb{R}$, abbiamo quindi $E \leq \mathbb{R}$ e dunque tutte le radici di f in $\mathbb{C}$ sono reali. ∎

Corollario 5.6. *Per ogni primo $p \geq 5$, il polinomio*

$$f(x) = x^p - 4x + 2$$

non è risolubile per radicali su $\mathbb{Q}$.

Dimostrazione. Per il teorema di Rolle, se f ha n radici reali, allora f' ha almeno $n - 1$ radici reali. Dato che $f'(x) = px^{p-1} - 4$ ha esattamente due radici reali, abbiamo $n \leq 3$. D'altra parte, $f(-2) < 0$, $f(0) > 0$, $f(1) < 0$ e $f(2) < 0$, quindi f ha $n = 3$ radici reali. Dunque f non è risolubile per radicali su $\mathbb{Q}$ per la Proposizione 5.5. ∎

Ricordiamo ora un risultato (presente nelle dispense di Algebra II ([AII, Proposizione 7.14]); ne riportiamo comunque brevemente la dimostrazione) che mostra come il gruppo di Galois di opportuni polinomi di grado p primo sia isomorfo a tutto il gruppo simmetrico S_p.

Proposizione 5.7. *Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado primo p e sia E il campo di spezzamento per f in $\mathbb{C}$. Se $f(x)$ ha esattamente due radici non reali in $\mathbb{C}$, allora* $\mathrm{Gal}(E|\mathbb{Q}) \cong S_p$.

Dimostrazione. Sia $R = \{a \in \mathbb{C} \mid f(a) = 0\}$ l'insieme delle radici di f in $\mathbb{C}$; dato che $\mathbb{Q}$ è un campo perfetto, $|R| = \deg f = p$. Possiamo identificare (tramite un omomorfismo iniettivo, dato che E è generato da R su $\mathbb{Q}$) il gruppo di Galois $\mathrm{Gal}(E|\mathbb{Q})$ con un sottogruppo H di $Sym(R) \cong S_P$
Sia γ il coniugio complesso (quindi un $\mathbb{Q}$-automorfismo di $\mathbb{C}$). Allora $\gamma(E) = E$ e la restrizione $\gamma_E \in \mathrm{Gal}(E|\mathbb{Q})$ scambia i due elementi non reali nell'insieme R delle

radici, e fissa tutti gli altri. Dunque H contiene una trasposizione. Ma, dato che $f(x)$ è irriducibile, H agisce transitivamente su R e quindi p divide $|H|$. Sia $P \leq H$ un sottogruppo di ordine p (esiste per il Teorema di Sylow) e sia $P = \langle \alpha \rangle$. Poichè $\alpha \in S_p$ e $|\alpha| = p$, α è un p-ciclo. Segue quindi (vedi Esercizio 5.5) $H = S_p$. ∎

(Ricordiamo ora che

Teorema 5.8. *Per $n \geq 5$ il gruppo alterno A_n è semplice.*

Quindi S_n non è risolubile per $n \geq 5$.)
Il polinomio $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ ha esattamente due radici non reali (come si verifica facilmente con gli strumenti dell'Analisi). Dunque il suo gruppo di Galois su $\mathbb{Q}$ è isomorfo al gruppo simmetrico S_5 e quindi, per il Teorema di Galois (Teorema 5.3) l'equazione $x^5 - 10x + 2 = 0$ non è risolubile per radicali.
(In altri termini, le soluzioni dell'equazione precedente sono numeri algebrici su $\mathbb{Q}$ che non possono pero' essere espressi, a partire da numeri razionali (o interi), tramite l'applicazione di un numero finito di operazioni aritmetiche ($+$, $-$, , $\times$ o $/$) o estrazioni di radici. Sono, quindi, numeri algebrici su $\mathbb{Q}$ che non appartengono alla "chiusura multiradicale" di $\mathbb{Q}$ in $\mathbb{C}$ (si veda l'Esercizio 5.3).
Osservazione. Per ogni primo p, si possono trovare polinomi irriducibili di grado p in $\mathbb{Q}[x]$, con solo due radici non reali in $\mathbb{C}$. Possiamo supporre $p \geq 5$ (per $p = 2, 3$ è chiaro). Siano $a, b_1, b_2, \ldots, b_{p-2}$ interi pari, con $a > 0$ e $b_1 < b_2 < \cdots < b_{p-2}$. Sia $g(x) = (x^2 + a)(x - b_1)(x - b_2) \cdots (x - b_{p-2})$. Osserviamo che $g(x)$ cambia di segno in ognuno degli intervalli (b_i, b_{i+1}), ha zeri esattamente in $b_1, b_2, \ldots, b_{p-2}$ e $g(x)$ tende a $+\infty$ (risp. a $-\infty$) per $x \to +\infty$ (risp. per $x \to -\infty$). Dunque $g(x)$ ha $(p-3)/2$ massimi relativi nell'intervallo (b_1, b_{p-2}) e tali massimi relativi sono > 2, dato che $|g(d)| > 2$ per ogni intero dispari d.
Definiamo ora $f(x) = g(x) - 2$; dunque $f(x)$ è un polinomio monico, a coefficienti interi, ed è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein (tutti i suoi coefficienti, tranne quello direttivo, sono pari, mentre il termine noto $g(0) - 2$ non è divisibile per 4). Il polinomio $f(x)$ ha $(p-3)/2$ massimi relativi *positivi* nell'intervallo (b_1, b_{p-2}) e $f(b_i) < 0$ per ogni $i \in \{1, \ldots, p-2\}$. Ne segue che $f(x)$ ha almeno $p-3$ radici reali nell'intervallo (b_1, b_{p-2}). Dato che $f(b_{p-2} = -2$ e $\lim_{x \to +\infty} f(x) = +\infty$, $f(x)$ ha anche una radice reale nell'intervallo $(b_{p-2}, +\infty)$. Scrivendo $f(x) = \prod_{i=1}^{p} (x - \gamma_i) = g(x) - 2$ e confrontando i coefficienti dei termini di grado $p-1$ e $p-2$, si ottiene

$$\sum_{i=1}^{p} \gamma_i = \sum_{i=1}^{p-2} b_i \qquad \sum_{1 \leq i < j \leq p} \gamma_i \gamma_j = \sum_{1 \leq i < j \leq p-2} b_i b_j + a$$

e quindi

$$\sum_{i=1}^{p} (\gamma_i)^2 = \left(\sum_{i=1}^{p} \gamma_i \right)^2 - 2 \sum_{1 \leq i < j \leq p} \gamma_i \gamma_j = \sum_{i=1}^{p-2} (b_i)^2 - 2a \, .$$

Scegliendo a sufficientemente grande, possiamo supporre che sia $\sum_{i=1}^{p}(\gamma_i)^2 < 0$ e quindi non tutte le radici γ_i sono reali. Dato che per ogni radice non reale di $f(x)$ anche la coniugata è una radice non reale, e abbiamo già provato che f ha almeno $p-2$ radici reali, concludiamo che $f(x)$ ha esattamente 2 radici non reali.

Esercizio 5.1. Assumendo la notazione e le ipotesi del Teorema 5.1, si provi che $[E:F]$ è il minimo intero positivo d tale che $\alpha^d \in F$.

Esercizio 5.2. Siano E e L sottocampi di un campo C e sia $K = EL$ il campo composto. Si provi che se $E|F$ e $L|F$ sono estensioni multiradicali, allora anche $K|F$ è multiradicale.

Esercizio 5.3. Sia $E|F$ una estensione di campi e sia

$$R = \bigcup_{\substack{F \leq L \leq E \\ L|F \text{ multiradicale}}} L$$

l'unione di tutte le estensioni intermedie multiradicali di $E|F$. Si provi (usando l'Esercizio 5.2) che R è un campo e che se $[E:F]$ è finito allora $R|F$ è una estensione multiradicale. (Possiamo chiamare allora R la *chiusura multiradicale* di F in E).

Esercizio 5.4. Sia G un gruppo che agisce transitivamente e fedelmente su un insieme X, con $|X| = p$, p primo. Si provi che ogni sottogruppo normale di G agisce transitivamente su X. Supponendo poi G risolubile, si provi che G ha esattamente un sottogruppo normale minimale N; inoltre $|N| = p$ e N è un p-sottogruppo di Sylow di G.

Esercizio 5.5. Sia p un numero primo e sia H un sottogruppo del gruppo simmetrico S_p. Si provi che se H contiene una trasposizione e un p-ciclo, allora $H = S_p$.

6 Gruppi abeliani finitamente generati

In questa sezione daremo il teorema di struttura per gruppi abeliani finitamente generati. Vedremo che tali gruppi si scrivono come prodotto diretto di gruppi ciclici finiti di ordine potenza di primo e di gruppi ciclici infiniti. Partiamo considerando gruppi abeliani finiti.

Teorema 6.1 (Teorema di Struttura dei Gruppi Abeliani Finiti)**.** *Ogni gruppo abeliano finito è prodotto diretto di gruppi ciclici di ordine potenza di primo.*

Dimostrazione. Sia G un gruppo abeliano finito. Per il Lemma 3.10, G è prodotto diretto dei suoi sottogruppi di Sylow. Possiamo quindi ricondurci al caso $|G| = p^n$, con p primo.
Sia A un sottogruppo ciclico di G di ordine massimo. Proviamo, per induzione su $|G|$, che allora $G = A \times B$ per un opportuno sottogruppo B di G; da ciò segue, di nuovo per

induzione sull'ordine del gruppo, che G è prodotto diretto di gruppi ciclici. Possiamo supporre che A sia un sottogruppo proprio di G. Scegliamo un elemento $x \in G \setminus A$ di ordine minimo e sia $X = \langle x \rangle$. Allora $x^p \in A$ e $\langle x^p \rangle \neq A$, altrimenti $|X| > |A|$ contro la scelta di A. Dunque $x^p = y^p$ per un opportuno $y \in A$; ponendo $z = xy^{-1}$, si ha $z \notin A$ e $z^p = x^p(y^p)^{-1} = 1$, segue $|x| \leq |z| = p$ e quindi $|x| = p$ e $X \cap A = 1$. Osserviamo che allora $AX/X \cong A$ è un sottogruppo ciclico di ordine massimo di G/X: dato infatti un sottogruppo ciclico $\langle wX \rangle$ di G/X, si ha $|A| \geq |\langle w \rangle| \geq |\langle wX \rangle|$. Applicando l'ipotesi induttiva, esiste quindi un sottogruppo B/X di G/X tale che $G/X = AX/X \times B/X$. Segue $G = AB$ e, da $A \cap B \leq AX \cap B \leq X$, si ha $A \cap B \leq A \cap X = 1$; pertanto $G = A \times B$. ∎

Il numero e gli ordini dei sottogruppi ciclici di ordine primo in una decomposizione in prodotto diretto di un gruppo abeliano, come dal Teorema 6.1, sono univocamente determinati; ciò segue dal seguente esercizio. Ricordiamo che un gruppo finito G si dice un *p-gruppo* se $|G| = p^a$ con p primo e a intero non negativo.

Esercizio 6.1. Sia G un p-gruppo abeliano finito e sia

$$G = A_1 \times A_2 \times \cdots \times A_n = B_1 \times B_2 \times \cdots \times B_m$$

con A_i e B_j gruppi ciclici non banali. Si provi che allora $n = m$ e, a meno di un riordinamento degli indici, $|A_i| = |B_i|$ per ogni $i = 1, 2, \ldots, n$.
(Suggerimento: Sia $G_1 = \{x \in G \mid x^p = 1\}$; si provi che G_1 è un sottogruppo di G e che $|G_1| = p^n = p^m$; si proceda poi per induzione, considerando G/G_1).

Per trattare il caso infinito, dobbiamo premettere alcuni concetti e risultati di teoria dei moduli.

Definizione. (I) Siano A un anello commutativo e U, V, W A-moduli. Una sequenza esatta

$$0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0 \qquad (\star)$$

(dove f e g sono omomorfismi di A-moduli) si *spezza* se esiste un A-sottomodulo W_0 di V tale che $V = f(U) \oplus W_0$.

(II) Sia A un anello commutativo. Un A-modulo W si dice *proiettivo* se ogni sequenza esatta $(\star)$ si spezza.

Osserviamo, in particolare, che se U, V, W sono A-moduli con W proiettivo e $V/U \cong W$, allora esiste un sottomodulo W_0 di V tale che $V = W_0 \oplus U$ (e quindi $W_0 \cong W$).
Diamo ora un criterio che caratterizza le successioni esatte che si spezzano.

Proposizione 6.2. *La successione esatta $(\star)$ si spezza se e solo se esiste un omomorfismo di A-moduli $\overline{g} : W \to V$ tale che $g \circ \overline{g} = id_W$.*

DIMOSTRAZIONE. Supponiamo che la successione esatta $(\star)$ si spezzi, ovvero che esista un A-sottomodulo W_0 di V tale che $V = f(U) \oplus W_0$. Allora la restrizione $g_{W_0} : W_0 \to W$ è un isomorfismo di A-moduli; prendiamo quindi $\overline{g} = (g_{W_0})^{-1}$.

Viceversa, supponendo che esista un omomorfismo $\overline{g} : W \to V$ tale che $g \circ \overline{g} = id_W$, definiamo $W_0 = \overline{g}(W)$. Allora W_0 è un A-sottomoculo di V e $V = W_0 + U_0$, dove $U_0 = \ker(g) = f(U)$: infatti, per $v \in V$, definiamo $w_0 = \overline{g}(g(v)) \in W_0$ e osserviamo che $v = w_0 + (v - w_0)$ e che $g(v - w_0) = g(v) - g(\overline{g}(g(v))) = g(v) - g(v) = 0$. Notiamo infine che $W_0 \cap U_0 = 0$: se $v = \overline{g}(w) \in W_0$ (con $w \in W$), allora da $v \in U_0$ segue $0 = g(v) = g(\overline{g}(w)) = w$ e quindi $v = g(0) = 0$.
Segue $V = W_0 \oplus U_0$. ∎

Ricordiamo che un A modulo V si dice *libero* se è somma diretta di A-moduli regolari, ovvero se $V = \bigoplus_{i \in I} V_i$ con $V_i \cong A_0$ per ogni $i \in I$ e A_0 A-modulo regolare; ciò equivale all'esistenza di una *base* per V, ovvero di un sottoinsieme $B = \{w_i\}_{i \in I}$ di V tale che ogni $v \in V$ si scriva in modo unico come somma finita $v = \sum a_i w_i$ con $a_i \in A$ e $w_i \in B$.

Proposizione 6.3. *Sia A un anello commutativo. Ogni A-modulo libero è proiettivo.*

DIMOSTRAZIONE. Sia W un A-modulo libero e sia $B = \{w_i\}_{i \in I}$ una base di W. Data una successione esatta $(\star)$ (con le notazioni precedenti), consideriamo per ogni $i \in I$ un elemento $v_i \in g^{-1}(w_i)$ della retroimmagine (non vuota) di w_i. Per $w = \sum a_i w_i \in W$, definiamo $\overline{g}(w) = \sum a_i v_i \in V$. Dato che B è una base, $\overline{g} : W \to V$ è ben definito e, come si verifica facilmente, è un omomorfismo di A-moduli e $g \circ \overline{g} = id_W$. Pertanto, per il Lemma 6.2, la generica successione esatta $(\star)$ si spezza e quindi W è proiettivo. ∎

Definizione. Sia A un anello commutativo e V un A-modulo. V si dice *senza torsione* (torsion-free) se per ogni $a \in A$ e $v \in V$ da $a \neq 0 \neq v$ segue $av \neq 0$.

Consideriamo, invece di limitarci al solo anello degli interi, moduli su un generico dominio ad ideali principali. Osserviamo anche di passaggio che, in modo sostanzialmente analogo a quanto fatto qui per gruppi abeliani finitamente generati, si può determinare la struttura di moduli finitamente generati su domini a ideali principali. Abbiamo il seguente risultato (che si applica, in particolare, nel caso dei gruppi abeliani, i quali non sono (tutti e soli gli) $\mathbb{Z}$-moduli).

Teorema 6.4. *Sia A un dominio a ideali principali e sia V un A-modulo finitamente generato e senza torsione. Allora V è un A-modulo libero.*

DIMOSTRAZIONE. Procediamo per induzione sulla minima cardinalità $n = m(V)$ di un insieme di generatori per V. Se $n = 0$, allora V è il modulo nullo e la tesi è banalmente vera.
Supponiamo $n \geq 1$ e sia B un insieme di generatori di V con $|B| = n$. Sia $x \in B$ e sia $U = Ay$ un elemento massimale della famiglia $\mathcal{F} = \{Au \mid u \in V, x \in Au\}$ dei

sottomoduli ciclici di V che contengono x (osserviamo che V è noetheriano, essendo finitamente generato su A e A anello noetheriano).
Proviamo che V/U è senza torsione. Sia $v \in V$ tale che esista un $a \in A$, $a \neq 0$, tale che $av \in U$; proviamo allora che $v \in U$. Ricordando che A è un UFD, possiamo scegliere a con il numero minimo di fattori irriducibili (se tale numero è zero, ovvero a è invertibile in A, allora $v = a^{-1}av \in U$). Da $az \in U = Ay$ segue $az = by$ per un opportuno $b \in A$. Notiamo che a e b sono coprimi in A: se infatti esistesse un irriducibile $p \in A$ che divide sia a che b, diciamo $a = pa_0$, $b = pb_o$ con $a_0, b_0 \in A$, allora $p(a_0z - b_0y) = 0$ e, essendo V senza torsione, questo implica $a_0z = b_0y \in U$, contro la scelta di a (poiché il numero dei fattori irriducibili di a_0 è inferiore a quello di a).
Esistono dunque $c, d \in A$ tali che $1 = ac + bd$. Ricordando che $by = az$, abbiamo dunque $y = acy + bdy = a(cy + dz) \in A(cy + dz)$ e quindi $U = Ay \leq A(cy + dz)$. Per la scelta di U segue quindi $U = A(cy + dz)$, ovvero $cy + dz \in U$, da cui deduciamo $dz \in U$. Ma allora $z = z1 = acz + bdz \in U$, essendo $caz \in U$ e $bdz \in U$.
Pertanto, V/U è senza torsione e, per ipotesi induttiva (dato che $m(V/U) < n$, poiché $\{bU \mid b \in B, b \neq x\}$ genera V/U) segue V/U libero. Per la Proposizione 6.3, quindi $V = U \oplus V_0$ con $V_0 \cong U/V$ libero. Concludiamo osservando che l'applicazione $\phi : A_0 \to U$, tale che $\phi(a) = ay$ per ogni $a \in A_0$, è un isomorfismo di A-moduli (l'iniettività segue dall'ipotesi che V, e quindi U, sia senza torsione). Quindi V è un A-modulo libero. ∎

Come osservato sopra la classe degli $\mathbb{Z}$-moduli coincide con quella dei gruppi abeliani e un gruppo abeliano G è senza torsione esattamente quando l'unico elemento di periodo finito è l'elemento identico (zero) di G. Abbiamo quindi il seguente corollario del Teorema 6.4:

Corollario 6.5. *Sia G un gruppo abeliano finitamente generato e senza torsione. Allora G è somma diretta di un numero finito di gruppi ciclici infiniti.*

Il numero di addendi in una qualsiasi decomposizione in somma diretta come nel Corollario 6.5 è univocamente determinato:

Esercizio 6.2. Sia $G = \bigoplus_{i \in I} C_i = \bigoplus_{i \in J} D_j$ gruppo (additivo) abeliano e D_i, C_j gruppi ciclici infiniti, per ogni $i \in I$, $j \in J$. Si provi che allora $|I| = |J|$. (Sugg.: si può supporre che ogni C_i e D_j sia il gruppo additivo $\mathbb{Z}$; si osservi che, posto $N = pG = \{px \mid x \in G\}$, $V = G/N$ è uno spazio vettoriale su $\mathbb{Z}/p\mathbb{Z}$; si sfrutti poi l'invarianza della dimensione).

Dai risultati precedenti abbiamo infine:

Teorema 6.6 (Teorema Fondamentale dei Gruppi Abeliani Finitamente Generati)**.** *Sia G un gruppo abeliano finitamente generato. Allora G è somma diretta di un numero finito di gruppi ciclici di ordine infinito o potenza di primo.*

Dimostrazione. Sia A un gruppo abeliano finitamente generato. Utilizziamo la notazione additiva. Definiamo $A_0 = \{a \in A \mid |a| \text{ finito}\}$; allora A_0 è un sottogruppo

(sottogruppo di torsione) di A. Si verifica immediatamente che il gruppo quoziente A/A_0 è senza torsione e quindi, per la Proposizione 6.3 e il Teorema 6.4, $A = A_0 \oplus A_1$ con $A_1 \cong A/A_0$ somma diretta di gruppi ciclici infiniti. Osserviamo che, dato che A è uno $\mathbb{Z}$-modulo finitamente generato, A è noetheriano e quindi in particolare A_0 è finitamente generato. Se T è un insieme finito di generatori di A_0 e $m = \max\{|x| \mid x \in T\}$, allora $|A_0| \leq |T|^m$ e quindi A è finito. La tesi segue quindi applicando il Teorema 6.1.
(Osserviamo, per concludere, che il numero degli addendi ciclici infiniti e di quelli di ordine p^n, con p primo e n intero positivo, è univocamente determinato (si vedano gli Esercizi 6.1 e 6.2). ∎

Riferimenti bibliografici

[AI] C. Casolo, Appunti per il corso di Algebra I- a.a. 2013-2014.

[AII] C. Casolo, Appunti per il corso di Algebra II- a.a. 2014-2015.

[I] M. Isaacs, Algebra, a graduate course. Brooks/Cole Publishing Company, 1994.