Questa è una raccolta di approfondimenti scritti durante il corso di Algebra 2 tenuto dal prof. Andrea Lucchini nel primo semestre dell'anno accademico 2013-2014 all'università di Padova, dipartimento di Matematica. Si tratta di cose ben note e le ho scritte soprattutto per suscitare curiosità. Per commenti o domande mi si può scrivere all'indirizzo mgaronzi@math.unipd.it.

Martino Garonzi

1 Un caso particolare del teorema di Burnside

Mostriamo qui che se p, q sono numeri primi e n è un intero positivo allora i gruppi di ordine $p^n q$ non sono semplici. Si tratta di un caso particolare del teorema $p^a q^b$ di Burnside, che dice che *in un gruppo finito semplice non abeliano non ci sono classi di coniugio non banali di cardinalità una potenza di un primo* (questo implica che i gruppi di ordine $p^a q^b$ non sono semplici: basta considerare la classe di coniugio di un elemento centrale di un p-Sylow).

Sia G un gruppo di ordine $p^n q$. Se $p = q$ allora G è un p-gruppo e quindi $Z(G) \neq \{1\}$, per cui G non è semplice. Supponiamo ora $p \neq q$. Se G ha un solo p-Sylow allora esso è normale e G non è semplice. Per il teorema di Sylow possiamo quindi assumere che G abbia q p-Sylow. Se due qualsiasi p-Sylow hanno intersezione banale allora i p-Sylow coprono $q(p^n - 1) + 1 = |G| - (q - 1)$ elementi, quindi in G c'è spazio per al più un q-Sylow; siccome ce n'è almeno uno, esso è normale, quindi G non è semplice.

Supponiamo quindi che esistano due p-Sylow con intersezione non banale. Siano P_1, P_2 due p-Sylow distinti tali che $|P_1 \cap P_2|$ è il massimo possibile, e sia $N_i := N_{P_i}(P_1 \cap P_2)$ per $i = 1, 2$. Mostriamo che $J := \langle N_1, N_2 \rangle$ non è un p-gruppo. Se lo fosse, allora per il teorema di Sylow sarebbe contenuto in un p-Sylow R di G. A meno di scambiare P_1 e P_2 tra di loro possiamo assumere che sia $R \neq P_2$. Allora abbiamo $P_1 \cap P_2 \subseteq N_1 \cap P_2 \subseteq R \cap P_2$ e dalla massimalità di $|P_1 \cap P_2|$ segue che $P_1 \cap P_2 = R \cap P_2$. D'altra parte $R \cap P_2 \supseteq N_2 \supseteq P_1 \cap P_2$ e quindi $P_1 \cap P_2 = N_2 = N_{P_2}(P_1 \cap P_2)$, in altre parole $P_1 \cap P_2$ è auto-normalizzato in P_2, e questo contraddice il fatto seguente.

Lemma 1. *Sia P un p-gruppo finito e sia H un sottogruppo proprio di P. Allora $N_P(H) \neq H$.*

Dimostrazione. Scriviamo $|P| = p^n$ e procediamo per induzione su n. Se $n = 1$ allora $P \cong C_p$ e l'enunciato è chiaramente vero. Supponiamo ora che sia $n > 1$. Sia $H < P$, e sia x un elemento centrale di P diverso da 1 (esiste perché i p-gruppi finiti hanno centro non banale). Se $x \in H$ allora $H/\langle x \rangle < P/\langle x \rangle$ e applicando l'ipotesi induttiva troviamo che $N_{P/\langle x \rangle}(H/\langle x \rangle) = K/\langle x \rangle \neq H/\langle x \rangle$, da cui $N_P(H) = K \neq H$. Supponiamo ora che sia $x \notin H$. Siccome x è centrale normalizza H, cioè $x \in N_P(H)$ e quindi $N_P(H) \neq H$. □

Riepilogando, abbiamo quindi ottenuto che J non è un p-gruppo, quindi il suo ordine è diviso da q. Poiché $|G| = p^n q$, J contiene un q-Sylow di G, sia esso Q. Allora dalla definizione di J segue che Q normalizza $P_1 \cap P_2$. D'altra parte Q agisce per coniugio sui p-Sylow di G transitivamente (infatti $G = QP_1$ e G agisce transitivamente, per il teorema di Sylow) cioè ogni p-Sylow di G ha la forma xP_1x^{-1} con $x \in Q$. Siccome Q normalizza $P_1 \cap P_2$ segue che $P_1 \cap P_2$ è contenuto in tutti i p-Sylow di G, quindi è contenuto nella loro intersezione, che è il cuore normale di P_1, $(P_1)_G$, che è un sottogruppo normale di G. Siccome $\{1\} \neq P_1 \cap P_2 \subseteq (P_1)_G \subseteq P_1 \subset G$ otteniamo allora che G non è semplice.

2 La funzione di Eulero e i gruppi ciclici

Ci proponiamo di caratterizzare i numeri interi positivi n tali che *ogni gruppo di ordine n è ciclico*. Alcuni chiamano tali numeri "numeri ciclici".

Cominciamo con qualche risultato utile di struttura.

2.1 Risultati di struttura

Proposizione 1. *Siano G un gruppo finito e H un suo sottogruppo tale che $\bigcup_{g\in G} gHg^{-1} = G$. Allora $H = G$.*

Dimostrazione. Come è noto dall'equazione delle classi H ha $|G : N_G(H)|$ coniugati in G, dove $N_G(H)$ indica il normalizzante di H in G. Siccome $1 \in gHg^{-1}$ per ogni $g \in G$ l'unione $\bigcup_{g\in G} gHg^{-1}$ non è disgiunta e quindi siccome tutti i coniugati di H hanno ordine $|H|$ e $H \subseteq N_G(H)$, se $H \neq G$ allora

$$|G| < |G : N_G(H)| \cdot |H| = |G| \cdot |H|/|N_G(H)| \leq |G|,$$

contraddizione. □

Osserviamo che questo non vale più se il gruppo G è infinito: per esempio, su $\mathbb{C}$ ogni matrice (e quindi anche ogni matrice invertibile) è "triangolarizzabile", cioè coniugata a una matrice triangolare superiore, e le matrici invertibili triangolari superiori sono un sottogruppo del gruppo delle matrici invertibili.

Proposizione 2. *Siano A, B due gruppi finiti di ordine coprimo. Allora*

$$Aut(A \times B) \cong Aut(A) \times Aut(B).$$

Dimostrazione. Costruiamo un isomorfismo $\varphi : \mathrm{Aut}(A\times B) \to \mathrm{Aut}(A)\times\mathrm{Aut}(B)$. Sia quindi f un automorfismo di $A \times B$. Mostriamo che se $a \in A$ allora $f(a, 1)$ è della forma $(a^*, 1)$ per qualche $a^* \in A$. Sia infatti $f(a, 1) = (a^*, b^*)$. Siccome f è un isomorfismo $(a, 1)$ e (a^*, b^*) hanno lo stesso ordine, che è quindi diviso dall'ordine di b^*. Dal fatto che $|A|$ e $|B|$ sono coprimi otteniamo allora che $b^* = 1$. Similmente $f((1, b))$ ha la forma $(1, b^*)$ con $b^* \in B$. Indichiamo con $\pi_A : A \times B \to A$ e $\pi_B : A \times B \to B$ le proiezioni canoniche, cioè gli omomorfismi definiti da $\pi_A((a, b)) := a$ e $\pi_B((a, b)) := b$. Siano $f_A : A \to A$ e $f_B : B \to B$ definiti come

segue: $f_A(a) := \pi_A(f(a,1)) = a^*$ e $f_B(b) := \pi_B(f(1,b)) = b^*$. È facile vedere che f_A e f_B sono isomorfismi di gruppi. Definiamo allora $\varphi(f) := (f_A, f_B)$. La funzione φ è un omomorfismo di gruppi, infatti

$$\begin{aligned}(f \circ g)_A(a) &= \pi_A(f(g((a,1)))) = \pi_A(f((g_A(a),1))) \\ &= \pi_A((f_A(g_A(a)),1)) = f_A(g_A(a)) = (f_A \circ g_A)(a)\end{aligned}$$

per cui $(f \circ g)_A = f_A \circ g_A$, e analogamente $(f \circ g)_B = f_B \circ g_B$. Siccome $f((a,b)) = (f_A(a), f_B(b))$ l'omomorfismo φ è un isomorfismo. □

Proposizione 3. *Sia G un gruppo finito non abeliano. Se ogni sottogruppo proprio di G è abeliano allora G non è semplice.*

Dimostrazione. Siccome G è non abeliano, è non ciclico, quindi G è l'unione dei suoi sottogruppi massimali, quindi per la Proposizione 1 G ha almeno due sottogruppi massimali non coniugati H, K. Per ipotesi H, K sono abeliani, quindi $H \cap K$ è normale in H e K, per cui il normalizzante in G di $H \cap K$ contiene $\langle H, K\rangle$. Ora siccome H e K sono massimali distinti e $\langle H, K\rangle$ è un sottogruppo di G che contiene entrambi otteniamo che $\langle H, K\rangle = G$ per cui $H \cap K \trianglelefteq G$ e siccome vogliamo dimostrare che G non è semplice possiamo supporre che sia $H \cap K = \{1\}$. Lo stesso argomento dimostra che H e K hanno intersezione banale coi loro coniugati distinti. Ne segue che il numero di elementi che i coniugati di H più i coniugati di K coprono è esattamente (qui supponiamo, a meno di scambiare tra loro H e K, che $|H| \leq |K|$)

$$\begin{aligned}|\bigcup_{g\in G}(gHg^{-1} \cup gKg^{-1})| &= 1 + (|H|-1)|G:H| + (|K|-1)|G:K| \\ &= 1 + 2|G| - |G:H| - |G:K| \\ &\geq 1 + 2|G| - 2|G:H| \\ &\geq 1 + 2|G| - |G| = 1 + |G|,\end{aligned}$$

assurdo. □

2.2 La funzione di Eulero

Ricordiamo che la funzione di Eulero $\varphi : \mathbb{N} \to \mathbb{N}$ (dove si considera $0 \notin \mathbb{N}$) è definita come segue: $\varphi(n)$ è il numero di elementi di $\{1, \ldots, n\}$ coprimi con n. Tale funzione ha le seguenti proprietà (C_n indica il gruppo ciclico di ordine n).

- $\varphi(n) = |\mathrm{Aut}(C_n)|$. Infatti detto g un generatore di C_n, un automorfismo f di C_n è determinato da dove manda g, e siccome $f(g)$ è anch'esso un generatore di C_n (perché f è un isomorfismo) si deve avere $f(g) = g^k$ con k coprimo con n. Quindi ci sono $\varphi(n)$ scelte per un tale f.
- Se p è un primo e m è un intero positivo allora $\varphi(p^m) = p^{m-1}(p-1)$. Infatti i numeri tra 1 e p^m non coprimi con p^m sono i multipli di p, cioè $p, 2p, 3p, \ldots, p^{m-1}p$, sono p^{m-1}, quindi quelli coprimi con p^m sono $p^m - p^{m-1} = p^{m-1}(p-1)$.

- Se a, b sono due interi positivi coprimi allora $\varphi(ab) = \varphi(a)\varphi(b)$. Questo si vede in termini di gruppi ciclici come segue: siccome a e b sono coprimi, per la Proposizione 2 e il teorema cinese del resto

$$\mathrm{Aut}(C_a) \times \mathrm{Aut}(C_b) \cong \mathrm{Aut}(C_a \times C_b) \cong \mathrm{Aut}(C_{ab})$$

  e quindi prendendo gli ordini otteniamo che $\varphi(a)\varphi(b) = \varphi(ab)$.

Ne segue che se $n = \prod_{i=1}^{k} p_i^{a_i}$ è la decomposizione di n come prodotto di potenze di primi p_i a due a due distinti allora $\varphi(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1)$. Osserviamo che da questa formulazione è chiaro che se m divide n allora $\varphi(m)$ divide $\varphi(n)$.

Teorema 1. *Le seguenti affermazioni sono equivalenti.*

1. *n e $\varphi(n)$ sono coprimi.*
2. *Ogni gruppo di ordine n è ciclico.*

Dimostrazione. (1) $\Rightarrow$ (2). Procedo per induzione su n. Sia G un gruppo di ordine n. Per induzione possiamo supporre che tutti i sottogruppi propri e tutti i quozienti propri di G siano ciclici. In particolare per la Proposizione 3 G non è semplice, quindi ammette un sottogruppo normale N con $N \neq \{1\}$ e $N \neq G$. Quindi N è ciclico. L'azione di coniugio di G su N fornisce un omomorfismo $G \to \mathrm{Aut}(N)$ il cui nucleo è il centralizzante $C_G(N) = \{g \in G \ : \ gx = xg \ \forall x \in N\}$. Dal teorema di isomorfismo ne segue un omomorfismo iniettivo $G/C_G(N) \to \mathrm{Aut}(N)$, quindi $|G/C_G(N)| = |G : C_G(N)|$ divide $|\mathrm{Aut}(N)| = \varphi(|N|)$. Ora, siccome $|N|$ divide $|G|$, $\varphi(|N|)$ divide $\varphi(|G|)$ e quindi siccome $|G|$ e $\varphi(|G|)$ sono coprimi, $|G|$ e $|\mathrm{Aut}(N)| = \varphi(|N|)$ sono coprimi, quindi $|G : C_G(N)|$ e $|\mathrm{Aut}(N)|$ sono coprimi, quindi $|G : C_G(N)| = 1$, cioè $G = C_G(N)$, cioè N è contenuto nel centro di G, $Z(G)$, in particolare $Z(G) \neq \{1\}$ e siccome $G/Z(G)$ è ciclico (come tutti i quozienti propri di G) segue (come è noto) che $G = Z(G)$, cioè G è abeliano. Ora siccome n e $\varphi(n)$ sono coprimi n non è diviso da quadrati (si confronti con la formula esibita sopra per il calcolo di $\varphi(n)$), diciamo $n = p_1 \cdots p_k$ con $p_1, \ldots, p_k$ primi distinti, e prendiamo $g_i \in G$ di ordine p_i per ogni $i = 1, \ldots, k$ (esistono per il teorema di Cauchy). Siccome gli ordini di $g_1, \ldots, g_k$ sono a due a due coprimi $g_1 \cdots g_k$ ha ordine $o(g_1 \cdots g_k) = o(g_1) \cdots o(g_k) = p_1 \cdots p_k = |G|$ quindi G è ciclico.

(2) $\Rightarrow$ (1). Per cominciare n non è diviso da quadrati perché se p è un primo e p^2 divide n allora $C_p \times C_p \times C_{n/p^2}$ è un gruppo non ciclico di ordine n. Scriviamo quindi $n = p_1 \cdots p_k$ con $p_1, \ldots, p_k$ primi distinti a due a due. $\varphi(n) = (p_1 - 1) \cdots (p_k - 1)$. Se n e $\varphi(n)$ non fossero coprimi esisterebbero $p_i = p$ e $p_j = q$ primi distinti tali che q divide $p - 1$. Se troviamo un gruppo G non ciclico di ordine pq possiamo dedurre che $G \times C_{n/pq}$ è un gruppo non ciclico di ordine n, contraddizione. Siamo quindi ricondotti a mostrare che se p e q sono due numeri primi e q divide $p - 1$ allora esiste un gruppo non ciclico di ordine pq. Il numero di p-cicli nel gruppo simmetrico S_p è $(p - 1)!$, quindi il

numero di p-Sylow è $(p-1)!/(p-1) = (p-2)!$ (ogni p-Sylow ha ordine p quindi contiene $p-1$ elementi di ordine p). Ne segue che $P := \langle (1 \dots p) \rangle$, che è un p-Sylow di S_p, ha esattamente $|S_p : N_{S_p}(P)| = (p-2)!$ coniugati in S_p, da cui $|N_{S_p}(P)| = p(p-1)$. Ora P è normale in $N_{S_p}(P)$ e per il teorema di Cauchy, siccome q divide $p-1$ che divide $p(p-1) = |N_{S_p}(P)|$, esiste $x \in N_{S_p}(P)$ di ordine q. Sia $G := \langle P, x \rangle$. Siccome x normalizza P si ha $G = P\langle x \rangle$. Siccome $|P| = p$ e $o(x) = q$ sono coprimi si ha $|G| = |P\langle x \rangle| = |P| \cdot |\langle x \rangle| = pq$. Quindi G è un sottogruppo di S_p di ordine pq. Ne segue che G non è ciclico, infatti S_p non ha elementi di ordine pq (un tale elemento avrebbe nella struttura ciclica un p-ciclo e quindi non ci sarebbe spazio per nient'altro). □

3 La formula di inversione di Moebius

3.1 La funzione di Moebius

Sia M l'insieme delle funzioni $\mathbb{N} \to \mathbb{C}$ (qui si considera $0 \notin \mathbb{N}$). Consideriamo l'operazione $*$ in M definita come segue: se $f, g \in M$ allora

$$(f * g)(n) := \sum_{d|n} f(d)g(n/d).$$

La somma è sui divisori di n, inclusi 1 e n. L'operazione $*$ si chiama "*convoluzione di Dirichlet*". Siano

- $\delta : \mathbb{N} \to \mathbb{C}$ la funzione che manda 1 in 1 e ogni $n \neq 1$ in 0,
- $u : \mathbb{N} \to \mathbb{C}$ la funzione che manda tutto in 1: $u(n) = 1 \ \forall n \in \mathbb{N}$,
- $\mu : \mathbb{N} \to \mathbb{C}$ la funzione che manda 1 in 1, n in $(-1)^k$ se n è il prodotto di k primi a due a due distinti e n in 0 se n è diviso da un quadrato diverso da 1. Tale funzione si chiama "*funzione di Moebius classica*".

Ecco la funzione μ per valori piccoli di n.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1

Si ha che $(M, *)$ è un monoide commutativo con elemento neutro δ e che l'inverso di u in M è μ. Che $*$ sia commutativa è molto facile da vedere. Le altre cose enunciate sono mostrate qui di seguito.

1. Mostriamo che δ è un elemento neutro per $*$. Se $f \in M$ si ha $(f * \delta)(n) = \sum_{d|n} f(d)\delta(n/d) = f(n)$, essendo per definizione $\delta(n/d)$ diverso da zero solo per $n = d$, nel qual caso $\delta(n/d) = \delta(1) = 1$. Ne deduciamo che $f * \delta = f$, e ovviamente anche che $\delta * f = f$ essendo $*$ commutativa.

2. Mostriamo che $*$ è associativa. Siano dunque $a, b, c \in M$. Osserviamo che dato $m \in \mathbb{N}$ si ha

$$\{(d,n) \in \mathbb{N} \times \mathbb{N} \ : \ n|m, \ d|m/n\} = \{(d,n) \in \mathbb{N} \times \mathbb{N} \ : \ d|m, \ n|m/d\}.$$

Con questo in mente andiamo a mostrare che $(a*b)*c = a*(b*c)$. Si ha

$$\begin{aligned} ((a*b)*c)(m) &= \sum_{n|m} (a*b)(m/n)c(n) = \sum_{n|m} \left(\sum_{d|m/n} a(d)b(m/dn) \right) c(n) \\ &= \sum_{d|m} a(d) \left(\sum_{n|m/d} b(m/dn)c(n) \right) = \sum_{d|m} a(d)(b*c)(m/d) \\ &= (a*(b*c))(m). \end{aligned}$$

3. Mostriamo che $u*\mu = \delta$. Si ha

$$(u*\mu)(1) = \sum_{d|1} u(d)\mu(1/d) = u(1)\mu(1) = 1.$$

Dato ora $n \in \mathbb{N}$ con $n > 1$, dobbiamo mostrare che $(u*\mu)(n) = 0$, in altre parole che $\sum_{d|n} \mu(d) = 0$. Scriviamo $n = {p_1}^{a_1} \cdots {p_k}^{a_k}$. Siccome $\mu(d) = 0$ ogni volta che d è diviso da quadrati, si ha

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{\{i_1,\ldots,i_h\}} \mu(p_{i_1} \cdots p_{i_h}),$$

dove $\{i_1, \ldots, i_h\}$ varia nella famiglia dei sottoinsiemi non vuoti di $\{1, \ldots, k\}$. Raggruppando tali sottoinsiemi per cardinalità, e ricordando che $\{1, \ldots, k\}$ ha esattamente $\binom{k}{h}$ sottoinsiemi di cardinalità h, otteniamo che

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{h=1}^{k} \sum_{\{i_1,\ldots,i_h\}} \mu(p_{i_1} \cdots p_{i_h}) = \sum_{h=0}^{k} \binom{k}{h} (-1)^h.$$

Ricordando la formula del binomio di Newton, $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$ otteniamo allora che

$$\sum_{h=0}^{k} \binom{k}{h} (-1)^h = \sum_{h=0}^{k} \binom{k}{h} (-1)^h 1^{k-h} = (-1+1)^k = 0^k = 0,$$

come volevamo.

Mostrare per esercizio che $f \in M$ ammette un inverso in M se e solo se $f(1) \neq 0$.

Seguono alcune applicazioni della formula

$$u*\mu = \delta,$$

che è nota come "*formula di inversione di Moebius*".

3.2 La funzione di Eulero

Sia φ la funzione di Eulero, definita come segue: $\varphi(n)$ è il numero di elementi di $\{1, \ldots, n\}$ coprimi con n. Un gruppo ciclico G di ordine n ha esattamente $\varphi(n)$ elementi g tali che $\langle g \rangle = G$. Mostriamo che

$$\varphi(n) = \sum_{d|n} d\mu(n/d).$$

Siccome nel gruppo ciclico C_n ci sono n elementi, e per ogni divisore d di n esiste un unico sottogruppo di C_n di ordine d, C_n ha $\varphi(d)$ elementi di ordine d per ogni divisore d di n e quindi $\sum_{d|n} \varphi(d) = n$, in altre parole $\varphi * u = \mathrm{Id}$, dove Id è la funzione $\mathbb{N} \to \mathbb{C}$ definita da $\mathrm{Id}(n) = n$ per ogni $n \in \mathbb{N}$. Ne segue che

$$\varphi = \varphi * \delta = \varphi * (u * \mu) = (\varphi * u) * \mu = \mathrm{Id} * \mu,$$

che è quello che volevamo dimostrare.

3.3 Radici dell'unità

Sia n un intero positivo e consideriamo il polinomio $X^n - 1$. Esso ammette n zeri in $\mathbb{C}$, i suoi zeri sono

$$\rho_k := e^{2\pi k i/n} = \cos(2\pi k/n) + i \sin(2\pi k/n) \qquad k \in \{1, \ldots, n\}.$$

Allora ovviamente $\rho_k = {\rho_1}^k$ e quindi l'insieme

$$U_n = \{\rho_1, \ldots, \rho_n\}$$

è un gruppo ciclico di ordine n. I suoi generatori, cioè gli elementi $g \in U_n$ tali che $\langle g \rangle = U_n$, sono della forma ${\rho_1}^k$ con $k \in \{1, \ldots, n\}$ e k coprimo con n. Ci poniamo il seguente problema: qual è la *somma* dei generatori di U_n? Sia $F(n)$ tale somma. Allora certamente la somma di tutte le radici n-esime di 1, cioè la somma di tutti gli elementi di U_n, è uguale a $\sum_{d|n} F(d) = (F * u)(n)$. D'altra parte si ha

$$X^n - 1 = (X - \rho_1) \cdots (X - \rho_n)$$

e quindi la somma $\rho_1 + \cdots + \rho_n$ è l'opposto del termine di grado $n-1$ di $X^n - 1$, cioè 1 se $n = 1$ e 0 altrimenti. In altre parole $F * u = \delta$. Ora, abbiamo

$$F = F * \delta = F * (u * \mu) = (F * u) * \mu = \delta * \mu = \mu.$$

Quindi la somma dei generatori di U_n è $\mu(n)$.

I generatori di U_n si chiamano "*radici primitive n-esime*" di 1.

3.4 Polinomi irriducibili su campi finiti

Siano p un primo e n un intero positivo. Mostriamo che il numero di polinomi irriducibili di $\mathbb{F}_p[X]$ di grado n è uguale a $(1/n)\sum_{d|n}\mu(n/d)p^d$. Questo implica in particolare che ne esiste sempre almeno uno.

Sia $N_p(n)$ il numero dei polinomi irriducibili di $\mathbb{F}_p[X]$ di grado n. Il prodotto dei polinomi irriducibili di $\mathbb{F}_p[X]$ di grado che divide n è uguale a $X^{p^n}-X$, dato che ogni elemento del campo finito di p^n elementi, $\mathbb{F}_{p^n}$, è zero di $X^{p^n}-X$ e ha polinomio minimo su $\mathbb{F}_p$ di grado un divisore di n (per la formula dei gradi). Ne segue che, detta $F(n) := nN_p(n)$ si ha $\sum_{d|n}F(n) = p^n$, cioè $F * u = P$, dove $P(n) = p^n$, e quindi

$$F = F * \delta = F * (u * \mu) = (F * u) * \mu = P * \mu,$$

che è quello che volevamo dimostrare.

4 Somme e prodotti di algebrici come zeri di polinomi

Quanto segue è ispirato a un corso di dottorato di Algebra Lineare Applicata tenuto da Harald Wimmer nel 2010 all'università di Padova.

Siano $P(X), Q(X) \in \mathbb{Q}[X]$ e $a, b \in \mathbb{C}$ con $P(a) = 0 = Q(b)$. Siccome i numeri algebrici formano un campo, sappiamo che $a+b$ e ab sono algebrici, cioè sono zeri di polinomi non nulli. E di che polinomi sono zeri?

Nel seguito si espone una costruzione per trovare esplicitamente polinomi $R(X), S(X)$ (*non necessariamente irriducibili*) con $R(a+b) = 0$ e $S(ab) = 0$.

4.1 Matrici compagne

In questa sezione traduciamo il problema in termini matriciali. Sia dato il polinomio monico

$$P(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in \mathbb{Q}[X].$$

Consideriamo la matrice seguente:

$$C(P) := \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}.$$

Essa si dice "matrice compagna" (companion matrix) di $P(X)$. Il motivo è il seguente: il polinomio caratteristico e il polinomio minimo di $C(P)$ sono

entrambi uguali a $P(X)$. In particolare gli zeri di $P(X)$ non sono altro che gli autovalori di $C(P)$.

Il problema è quindi diventato il seguente: date due matrici A, B quadrate, un autovalore λ di A e un autovalore μ di B trovare una matrice che ha $\lambda + \mu$ come autovalore, trovare una matrice che ha $\lambda\mu$ come autovalore.

4.2 Somma e prodotto di Kronecker

Siano date due matrici A, B con A una matrice $m \times n$ e B una matrice $p \times q$. Chiamiamo a_{ij} e b_{ij} le entrate di posto (i, j) di A e B rispettivamente. Il prodotto di Kronecker di A e B è la seguente matrice a blocchi:

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix}.$$

Quindi per esempio

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 1 & 0 & 4 & 2 \\ 1 & 1 & 0 & 2 & 2 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Denotiamo ora con I_k la matrice identità $k \times k$. Supponiamo che $m = n$ e $p = q$. In questo caso la somma di Kronecker di A e B è definita come la matrice $np \times np$

$$A \oplus B := A \otimes I_p + I_n \otimes B.$$

Allora si ha il seguente fatto, che non dimostreremo.

Teorema 2. *Siano A, B due matrici $n \times n$ e $m \times m$ rispettivamente, a coefficienti in $\mathbb{C}$, e siano $\sigma(A) = \{\lambda_1, \dots, \lambda_n\}$ e $\sigma(B) = \{\mu_1, \dots, \mu_m\}$ l'insieme (il multi-insieme) degli autovalori di A e di B rispettivamente, contati con molteplicità. Allora si hanno i seguenti fatti.*

1. $\det(A \otimes B) = \det(A)^m \det(B)^n$.
2. $\sigma(A \otimes B) = \{\lambda_i \mu_j \ : \ i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\}$ *e il polinomio caratteristico di $A \otimes B$ è $\prod_{i,j}(X - \lambda_i \mu_j)$ dove nel prodotto i varia tra 1 e n e j tra 1 e m.*
3. $\sigma(A \oplus B) = \{\lambda_i + \mu_j \ : \ i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\}$ *e il polinomio caratteristico di $A \oplus B$ è $\prod_{i,j}(X - (\lambda_i + \mu_j))$ dove nel prodotto i varia tra 1 e n e j tra 1 e m.*

4.3 Un esempio

Troviamo per esempio un polinomio a coefficienti interi che ha $\sqrt{2}+\sqrt[3]{2}$ come zero. Dobbiamo trovare il polinomio caratteristico della somma di Kronecker delle matrici compagne di $P(X)=X^2-2$ e $Q(X)=X^3-2$. Si ha

$$C(P)=\begin{pmatrix}0&2\\1&0\end{pmatrix},\qquad C(Q)=\begin{pmatrix}0&0&2\\1&0&0\\0&1&0\end{pmatrix}.$$

Ne segue che

$$\begin{aligned}C(P)\oplus C(Q) &= C(P)\otimes I_3 + I_2\otimes C(Q)\\ &= \begin{pmatrix}0&0&0&2&0&0\\0&0&0&0&2&0\\0&0&0&0&0&2\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\end{pmatrix}+\begin{pmatrix}0&0&2&0&0&0\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&0&0&0&2\\0&0&0&1&0&0\\0&0&0&0&1&0\end{pmatrix}\\ &= \begin{pmatrix}0&0&2&2&0&0\\1&0&0&0&2&0\\0&1&0&0&0&2\\1&0&0&0&0&2\\0&1&0&1&0&0\\0&0&1&0&1&0\end{pmatrix}.\end{aligned}$$

Quindi il polinomio caratteristico di $C(P)\oplus C(Q)$ vale

$$\begin{aligned}\det(X\cdot I_6 - C(P)\oplus C(Q)) &= \det\begin{pmatrix}X&0&-2&-2&0&0\\-1&X&0&0&-2&0\\0&-1&X&0&0&-2\\-1&0&0&X&0&-2\\0&-1&0&-1&X&0\\0&0&-1&0&-1&X\end{pmatrix}\\ &= X^6-6X^4-4X^3+12X^2-24X-4.\end{aligned}$$

Questo polinomio ha $\sqrt{2}+\sqrt[3]{2}$ come zero.

5 La successione di Fibonacci

5.1 La successione di Fibonacci

La *successione di Fibonacci*, di seguito denotata $(F_n)_{n\in\mathbb{N}}$, è la successione definita ricorsivamente come segue.

$$F_0:=0,\ F_1:=1,\ F_{n+1}:=F_{n-1}+F_n.$$

I suoi primi termini sono i seguenti.

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ \ldots$$

La definizione data è ricorsiva. Cominciamo col trovare una formula chiusa, cioè una formula "ragionevole" che esprime F_n in funzione di n. Per fare questo conviene scrivere la formula ricorsiva che definisce F_n in termini matriciali:

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix}.$$

Questo ovviamente implica che

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \qquad (*)$$

Per capire come sono fatte le potenze di una matrice conviene *diagonalizzarla*. Il polinomio caratteristico di $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ è $P(X) = X^2 - X - 1$. I suoi zeri sono $a := \frac{1}{2}(1 + \sqrt{5})$ e $1 - a$. Un autovettore di a è $\begin{pmatrix} a \\ 1 \end{pmatrix}$, un autovettore di $1 - a$ è $\begin{pmatrix} 1 \\ -a \end{pmatrix}$. Abbiamo quindi che

$$\begin{pmatrix} a & 1 \\ 1 & -a \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 1 \\ 1 & -a \end{pmatrix}^{-1} = \begin{pmatrix} a & 0 \\ 0 & 1-a \end{pmatrix}.$$

Sostituendo in $(*)$, e ricordando che $(A^{-1}BA)^n = A^{-1}B^nA$ (il coniugio è un omomorfismo di gruppi) otteniamo allora

$$\begin{aligned} \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} &= \left(\begin{pmatrix} a & 1 \\ 1 & -a \end{pmatrix}^{-1} \begin{pmatrix} a & 0 \\ 0 & 1-a \end{pmatrix} \begin{pmatrix} a & 1 \\ 1 & -a \end{pmatrix} \right)^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} a & 1 \\ 1 & -a \end{pmatrix}^{-1} \begin{pmatrix} a^n & 0 \\ 0 & (1-a)^n \end{pmatrix} \begin{pmatrix} a & 1 \\ 1 & -a \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \end{aligned}$$

Svolgendo i conti troviamo allora che

$$F_n = \frac{a^n - (1-a)^n}{a - (1-a)}.$$

Questa è una formula chiusa per F_n. Un altro modo "a posteriori" per trovarla è il seguente, ora che sappiamo che c'entra il polinomio $X^2 - X - 1$:

- Siano a e b i due zeri reali del polinomio $X^2 - X - 1$, con $a > 0$ e $b < 0$. Sia c uno qualsiasi tra a e b. Allora svolgendo le potenze successive di c e ricordando che $c^2 = c + 1$ abbiamo:

$$c^2 = c + 1,\ c^3 = c(c+1) = 2c + 1,\ c^4 = c(2c+1) = 3c + 2,$$

$$c^5 = c(3c+2) = 5c+3,\ c^6 = c(5c+3) = 8c+5,\ c^7 = c(8c+5) = 13c+8,$$
$$c^8 = c(13c+8) = 21c+13,\ c^9 = c(21c+13) = 34c+21,\ \ldots$$

Questo ci ricorda qualcosa, portandoci a congetturare che sia $c^n = F_n c + F_{n-1}$ per ogni $n \geq 1$. Questo si dimostra facilmente per induzione:

$$\begin{aligned} c^{n+1} &= cc^n = c(F_n c + F_{n-1}) = F_n(c+1) + F_{n-1}c \\ &= (F_{n-1} + F_n)c + F_n = F_{n+1}c + F_n. \end{aligned}$$

Siccome questo vale per $c \in \{a, b\}$ abbiamo

$$a^n = F_n a + F_{n-1}, \qquad b^n = F_n b + F_{n-1}.$$

Sottraendo queste uguaglianze tra loro otteniamo $a^n - b^n = F_n(a-b)$ da cui, essendo $a \neq b$, $F_n = \frac{a^n - b^n}{a-b}$, e ricordando che $b = 1-a$ otteniamo proprio quanto trovato sopra.

Osserviamo che usando la formula $F_n = \frac{a^n - (1-a)^n}{a-(1-a)}$ otteniamo facilmente che il rapporto F_{n+1}/F_n tende ad $a = \frac{1}{2}(1+\sqrt{5})$. Questo numero è noto come *sezione aurea*.

5.2 $MCD(F_n, F_m) = F_{MCD(n,m)}$

Tra le varie belle proprietà della successione di Fibonacci c'è la seguente: essa rispetta il massimo comun divisore, nel senso che $MCD(F_n, F_m) = F_{MCD(n,m)}$. Ora lo dimostriamo. Come sopra, sia $a = \frac{1}{2}(1+\sqrt{5})$ la sezione aurea, cioè la radice positiva di $X^2 - X - 1$.

1. Mostriamo che F_n rispetta l'ordine di divisibilità, nel senso che se n, x sono interi positivi allora F_n divide F_{nx}. Si ha

$$\begin{aligned} F_{nx}a + F_{nx-1} &= a^{nx} = (a^n)^x = (F_n a + F_{n-1})^x \\ &= \sum_{i=0}^{x} \binom{x}{i} F_n^i a^i F_{n-1}^{x-i} = \sum_{i=0}^{x} \binom{x}{i} F_n^i (F_i a + F_{i-1}) F_{n-1}^{x-i}. \end{aligned}$$

   Questa è un'uguaglianza che vale in $\mathbb{Q}[a]$. Siccome 1 e a sono linearmente indipendenti su $\mathbb{Q}$ (perché a ha grado 2 su $\mathbb{Q}$, essendo $X^2 - X - 1$ il suo polinomio minimo) i coefficienti di a devono essere gli stessi: $F_{nx} = \sum_{i=0}^{x} \binom{x}{i} F_n^i F_i F_{n-1}^{x-i}$. Siccome $F_0 = 0$, da questo segue che F_n divide F_{nx}.

2. Ora siano n, m interi positivi e sia $d = MCD(n, m)$ il loro massimo comun divisore. Da quanto mostrato nel punto precedente F_d divide F_n e F_m. Per mostrare che $F_d = MCD(F_n, F_m)$ basta allora mostrare che F_d si può esprimere come combinazione lineare di F_n e F_m a coefficienti interi. Cominciamo con l'osservare che, a meno di scambiare n e m tra loro,

l'algoritmo di Euclide fornisce due interi *positivi* α e β tali che $d = \alpha n - \beta m$. Si ha allora

$$F_d a + F_{d-1} = a^d = a^{\alpha n - \beta m} = \frac{a^{\alpha n}}{a^{\beta m}} = \frac{F_{\alpha n} a + F_{\alpha n - 1}}{F_{\beta m} a + F_{\beta m - 1}}.$$

Siccome vogliamo un'espressione polinomiale, ci serve esprimere l'inverso di $0 \neq xa + y \in \mathbb{Q}[a]$ come polinomio in a. Questo si può fare semplicemente risolvendo il sistema $(xa + y)(za + w) = 1$ nelle incognite z, w. Risulta che l'inverso di $xa + y$ è

$$(xa + y)^{-1} = \left(-\frac{x}{y^2 - x^2 + xy} \right) a + \left(\frac{x + y}{y^2 - x^2 + xy} \right).$$

Ne segue che

$$F_d a + F_{d-1} = \frac{F_{\alpha n} a + F_{\alpha n - 1}}{F_{\beta m} a + F_{\beta m - 1}} = \frac{(F_{\alpha n} a + F_{\alpha n - 1})(-F_{\beta m} a + F_{\beta m} + F_{\beta m - 1})}{F_{\beta m - 1}^2 - F_{\beta m}^2 + F_{\beta m} F_{\beta m - 1}}.$$

Detto $k = \beta m$ il denominatore è uguale a $G_k := F_{k-1}^2 - F_k^2 + F_k F_{k-1}$. Perché la nostra idea funzioni è cruciale che ci sbarazziamo di questo scomodo denominatore, e fortunatamente ci riusciamo: esaminando i primi valori di G_k è naturale congetturare che sia $G_k = (-1)^k$ (*identità di Cassini*). Questo si vede per induzione: $G_1 = F_0^2 - F_1^2 + F_1 F_0 = -1$ e

$$\begin{aligned} G_{k+1} &= F_k^2 - F_{k+1}^2 + F_{k+1} F_k = F_k^2 - (F_{k-1} + F_k)^2 + (F_{k-1} + F_k) F_k \\ &= F_k^2 - F_{k-1}^2 - F_k^2 - 2F_{k-1} F_k + F_{k-1} F_k + F_k^2 \\ &= -F_{k-1}^2 - F_{k-1} F_k + F_k^2 = -G_k. \end{aligned}$$

Otteniamo allora che vale

$$F_d a + F_{d-1} = (-1)^{\beta m} (F_{\alpha n} a + F_{\alpha n - 1})(-F_{\beta m} a + F_{\beta m} + F_{\beta m - 1}).$$

Questa è un'uguaglianza in $\mathbb{Q}[a]$. Siccome 1 e a sono linearmente indipendenti su $\mathbb{Q}$ i coefficienti di a sono gli stessi a sinistra e a destra. Otteniamo allora dopo qualche conto e semplificazione che

$$F_d = (-1)^{\beta m} (F_{\alpha n} F_{\beta m - 1} - F_{\beta m} F_{\alpha n - 1}).$$

Per il punto precedente F_n divide $F_{\alpha n}$ e F_m divide $F_{\beta m}$, quindi questa uguaglianza esprime F_d come combinazione lineare intera di F_n e F_m.

6 Fattorizzazioni modulo i primi e la teoria di Galois dietro le quinte

Quanto segue è ispirato a uno scritto di Hendrik Lenstra che si può trovare al link

http://websites.math.leidenuniv.nl/algebra/Lenstra-Chebotarev.pdf

6.1 Fattorizzazioni modulo i primi

Le seguenti due tabelle riassumono le fattorizzazioni dei due polinomi $P(X) = X^3 + X^2 + X + 3$ e $Q(X) = X^3 - 3X + 1$ su $\mathbb{F}_p$ al variare del primo $p \leq 127$.

p	$X^3 + X^2 + X + 3$	p	$X^3 + X^2 + X + 3$
2	$(X+1)^3$	53	$(X+43)(X^2+11X+5)$
3	$X(X+2)^2$	59	$(X+12)(X^2+48X+15)$
5	$X^3 + X^2 + X + 3$	61	$(X+6)(X^2+56X+31)$
7	$(X+4)(X^2+4X+6)$	67	$(X+23)(X+52)(X+60)$
11	$X^3 + X^2 + X + 3$	71	$(X+38)(X+52)(X+53)$
13	$X^3 + X^2 + X + 3$	73	$(X+34)(X^2+40X+28)$
17	$(X+5)(X+15)^2$	79	$(X+74)(X^2+6X+31)$
19	$X^3 + X^2 + X + 3$	83	$(X+45)(X^2+39X+72)$
23	$X^3 + X^2 + X + 3$	89	$(X+32)(X^2+58X+14)$
29	$(X+11)(X+23)(X+25)$	97	$(X+59)(X^2+39X+28)$
31	$(X+15)(X^2+17X+25)$	101	$(X+75)(X^2+27X+97)$
37	$(X+25)(X^2+13X+9)$	103	$X^3 + X^2 + X + 3$
41	$X^3 + X^2 + X + 3$	107	$X^3 + X^2 + X + 3$
43	$X^3 + X^2 + X + 3$	113	$X^3 + X^2 + X + 3$
47	$(X+31)(X^2+17X+38)$	127	$X^3 + X^2 + X + 3$

p	$X^3 - 3X + 1$	p	$X^3 - 3X + 1$
2	$X^3 + X + 1$	53	$(X+18)(X+39)(X+49)$
3	$(X+1)^3$	59	$X^3 + 56X + 1$
5	$X^3 + 2X + 1$	61	$X^3 + 58X + 1$
7	$X^3 + 4X + 1$	67	$X^3 + 64X + 1$
11	$X^3 + 8X + 1$	71	$(X+16)(X+25)(X+30)$
13	$X^3 + 10X + 1$	73	$(X+14)(X+25)(X+34)$
17	$(X+3)(X+4)(X+10)$	79	$X^3 + 76X + 1$
19	$(X+10)(X+12)(X+16)$	83	$X^3 + 80X + 1$
23	$X^3 + 20X + 1$	89	$(X+12)(X+36)(X+41)$
29	$X^3 + 26X + 1$	97	$X^3 + 94X + 1$
31	$X^3 + 28X + 1$	101	$X^3 + 98X + 1$
37	$(X+14)(X+28)(X+32)$	103	$X^3 + 100X + 1$
41	$X^3 + 38X + 1$	107	$(X+7)(X+40)(X+60)$
43	$X^3 + 40X + 1$	113	$X^3 + 110X + 1$
47	$X^3 + 44X + 1$	127	$(X+53)(X+87)(X+114)$

Si osserva un fenomeno strano: quando p è un primo minore o uguale di 127, su $\mathbb{F}_p$ mentre $P(X)$ ammette fattorizzazioni di tutte le strutture possibili, cioè $(1,1,1)$, $(1,2)$ e (3) (dove per esempio $(1,2)$ significa: un fattore irriducibile di grado 1 e un fattore irriducibile di grado 2), $Q(X)$ non ammette fattorizzazioni di tipo $(1,2)$.

Cosa c'è sotto?

6.2 La teoria di Galois dietro le quinte

Sia $f(X) = \sum_{i=0}^{n} a_i X^i$ un qualsiasi polinomio irriducibile di $\mathbb{Q}[X]$ di grado n.

Lemma 2. *Se $\alpha \in \mathbb{C}$ allora $(X-\alpha)^2$ non divide $f(X)$ in $\mathbb{C}[X]$.*

Dimostrazione. Supponiamo che $(X-\alpha)^2$ divida $f(X)$ per assurdo e scriviamo $f(X) = (X-\alpha)^2 h(X)$ con $h(X) \in \mathbb{C}[X]$. Derivando abbiamo

$$f'(X) = 2(X-\alpha)h(X) + (X-\alpha)^2 h'(X) = (X-\alpha)(2h(X) + (X-\alpha)h'(X)).$$

Quindi $f(X)$ e $f'(X)$ non sono coprimi in $\mathbb{C}[X]$ (hanno $X-\alpha$ come fattore comune), quindi non sono coprimi nemmeno in $\mathbb{Q}[X]$, questo segue subito applicando l'algoritmo di Euclide: se esistessero $a(X), b(X) \in \mathbb{Q}[X]$ con $a(X)f(X) + b(X)f'(X) = 1$ allora sostituendo $X = \alpha$ avremmo $0 = 1$ assurdo. Ma siccome $f(X)$ è irriducibile l'unica possibilità è che $f(X)$ divida $f'(X)$, e questo è assurdo perché il grado di $f'(X)$ è $n-1$, minore del grado di $f(X)$. □

Sia E il campo di spezzamento di $f(X)$ su $\mathbb{Q}$ contenuto in $\mathbb{C}$. Il "gruppo di Galois" di $f(X)$, denotato $\mathcal{G}_f$, è il gruppo degli isomorfismi di anelli $E \to E$ con la composizione, cioè $\mathcal{G}_f = \mathrm{Aut}(E)$.

N.B. La definizione di gruppo di Galois su un campo qualunque è diversa da questa. Nella definizione di gruppo di Galois si richiede infatti che ogni $g \in \mathcal{G}_f$ fissi puntualmente il campo base. Nel caso di $\mathbb{Q}$ però questo è automatico, come vediamo qui di seguito.

Dimostriamo che se $t \in \mathbb{Q}$ e $g \in \mathcal{G}_f$ allora $g(t) = t$. Scritto $t = a/b$ con a, b interi e $b \neq 0$, siccome $a = tb$ abbiamo $g(a) = g(tb) = g(t)g(b)$ quindi basta mostrare che $g(a) = a$ e $g(b) = b$, in altre parole basta mostrare che $g(t) = t$ quando t è intero. Supponiamo quindi che t sia intero. Se $t = 0$ allora $g(t) = g(0) = 0 = t$. Se $t > 0$ allora t è una somma di uni: $t = 1 + \cdots + 1$. Siccome $g(1) = 1$ (gli omomorfismi di anelli mandano 1 in 1) si ha $g(t) = g(1 + \cdots + 1) = g(1) + \cdots + g(1) = 1 + \cdots + 1 = t$. Se invece $t < 0$ allora $-t > 0$ quindi $g(t) = -(-g(t)) = -g(-t) = -(-t) = t$.

Ora facciamo un'osservazione cruciale: se $g \in \mathcal{G}_f$ e $u \in E$ con $f(u) = 0$ allora $f(g(u)) = 0$. Infatti $g(a_i) = a_i$ per ogni $i = 0, \ldots, n$ essendo gli a_i in $\mathbb{Q}$ e quindi

$$\begin{aligned} f(g(u)) &= \sum_{i=0}^{n} a_i (g(u))^i = \sum_{i=0}^{n} g(a_i) g(u^i) \\ &= \sum_{i=0}^{n} g(a_i u^i) = g(\sum_{i=0}^{n} a_i u^i) = g(f(u)) = g(0) = 0. \end{aligned}$$

Questo significa che se u è uno zero di $f(X)$ allora $g(u)$ è anch'esso uno zero di $f(X)$. In altre parole, detto $U := \{u_1, \ldots, u_n\}$ l'insieme degli zeri di $f(X)$ in E (notiamo che sono proprio n, tanti quant'è il grado di $f(X)$, perché per

il Lemma 2 $f(X)$ non ha zeri multipli) si ha che $\mathcal{G}_f$ agisce su U nel seguente modo: $\mathcal{G}_f \times U \ni (g, u) \mapsto g(u)$. Il nucleo di questa azione è $\{1\}$, cioè questa azione è fedele. Infatti se $g \in \mathcal{G}_f$ è tale che $g(u_i) = u_i$ per ogni $i = 1, \ldots, n$ allora, siccome g è un omomorfismo di anelli che fissa ogni elemento di $\mathbb{Q}$ ed E è generato da $u_1, \ldots, u_n$ su $\mathbb{Q}$, g fissa ogni elemento di E, cioè g è l'automorfismo identico. Come sappiamo ad un'azione fedele su n punti corrisponde un omomorfismo iniettivo verso il gruppo simmetrico S_n. Ne deduciamo un omomorfismo iniettivo $\mathcal{G}_f \to S_n$. In particolare $\mathcal{G}_f$ è isomorfo ad un sottogruppo di S_n. Un elemento di $\mathcal{G}_f$ è cioè completamente determinato da come muove gli zeri di $f(X)$.

Se K è un qualunque campo un polinomio $h(X) \in K[X]$ si dice "separabile su K" se per ogni zero u di $h(X)$ in un campo di spezzamento F di $h(X)$ su K, $(X - u)^2$ non divide $h(X)$ in $F[X]$. Ora invochiamo un risultato molto interessante dovuto a Frobenius e Dedekind.

Teorema 3 (Frobenius-Dedekind)**.** *Sia $f(X)$ un polinomio monico irriducibile di $\mathbb{Z}[X]$ di grado n. Le seguenti affermazioni sono equivalenti.*

- *Esiste un primo p tale che $f(X)$ è separabile su $\mathbb{F}_p$ (un tale primo p si dice "non ramificato") e la struttura della fattorizzazione di $f(X)$ modulo p è $(n_1, \ldots, n_t)$ (cioè, ci sono t fattori irriducibili di gradi $n_1, \ldots, n_t$ rispettivamente).*
- *Il gruppo di Galois di $f(X)$ su $\mathbb{Q}$, visto come sottogruppo del gruppo simmetrico S_n, contiene un elemento di struttura ciclica $(n_1, \ldots, n_t)$ (cioè un prodotto di t cicli disgiunti di lunghezze $n_1, \ldots, n_t$).*

In particolare,

- *esiste sempre un primo p tale che $f(X)$ modulo p si fattorizza in fattori distinti di grado 1 (tale fattorizzazione corrisponde all'elemento neutro del gruppo di Galois);*
- *$f(X)$ è irriducibile modulo qualche primo p se e solo se il gruppo di Galois di $f(X)$ su $\mathbb{Q}$, visto come sottogruppo di S_n, contiene un n-ciclo.*

Per la cronaca, i primi ramificati sono un numero finito (sono i divisori primi del discriminante di $f(X)$). Per esempio facendo riferimento alle tabelle sopra, i primi ramificati di $P(X)$ sono 2, 3 e 17, mentre l'unico primo ramificato di $Q(X)$ è 3.

Possiamo ora spiegare lo strano fenomeno riscontrato nelle tabelle sopra nel seguente modo: il gruppo di Galois di $P(X)$ è S_3, il gruppo di Galois di $Q(X)$ è A_3. Le fattorizzazioni di tipo $(1, 2)$ corrispondono ai 2-cicli, che sono permutazioni dispari quindi non stanno in A_3 (!) Se si fa attenzione, osservando le tabelle si nota anche che la proporzione delle fattorizzazioni di una data struttura è circa uguale alla proporzione degli elementi della corrispondente struttura ciclica nel gruppo di Galois. Questo fatto è formalizzabile e generale ed è un'istanza del teorema di densità di Chebotarev.

7 Fattorizzazione unica per risolvere equazioni diofantee

7.1 Su $\mathbb{Z}[\sqrt{-n}]$ con $n > 0$

Sia n un intero positivo e sia $u = \sqrt{-n} = i\sqrt{n} \in \mathbb{C}$.

Nel seguito mostriamo che l'anello $A_n = \mathbb{Z}[u] \cong \mathbb{Z}[X]/(X^2+n)$ è un dominio euclideo se e solo se $n \in \{1, 2\}$.

Mostriamo che se $n > 2$ allora 2 è irriducibile in A_n. Scriviamo $2 = (a + ub)(c + ud)$ con $a, b, c, d \in \mathbb{Z}$. Prendendo le norme otteniamo $4 = (a+ub)(a-ub)(c+ud)(c-ud) = (a^2+nb^2)(c^2+nd^2)$, quindi $a^2+nb^2 \in \{1, 2, 4\}$. Se $a^2 + nb^2 = 1$ allora siccome $n > 0$ si ha $a = 0$ oppure $b = 0$; se $a = 0$ allora $b = \pm 1$ e $n = 1$, se $b = 0$ allora $a = \pm 1$ - otteniamo quindi che $a + ub = \pm 1$ se $n > 1$, mentre se $n = 1$ allora $a + ub = \pm 1$ oppure $\pm i$. Analogamente se $c^2 + nd^2 = 1$ allora $c + ud$ è invertibile. Ora supponiamo che $a + ub$ e $c + ud$ non siano invertibili: allora $a^2 + nb^2 = 2$ da cui se $n = 1$ allora $a, b = \pm 1$, se $n = 2$ allora $a = 0$ e $b = \pm 1$ e non può aversi $n > 2$.

Ora supponiamo che $n > 2$ sia pari. Allora 2 divide $n = -u^2$ ma 2 non divide u, infatti se $2(a + ub) = u$ allora $2a = 0$ e $2b = 1$, assurdo (b è intero). Questo contraddice la fattorizzazione unica. Ora supponiamo che n sia dispari. Allora 2 divide $1 + n = 1 - u^2 = (1 + u)(1 - u)$ ma 2 non divide $1 \pm u$, infatti se $2(a + ub) = 1 \pm u$ allora $2a = 1$ e $2b = \pm 1$ assurdo (a e b sono interi). Siccome i domini euclidei sono fattoriali, cioè sono domini a fattorizzazione unica, deduciamo che A_n non è un dominio euclideo se $n > 2$.

Cosa possiamo dire dei casi $n = 1, 2$? $A_1 = \mathbb{Z}[i]$ è l'anello degli interi di Gauss e sappiamo che è euclideo con la funzione norma, $N(x) = x\overline{x}$ (che ricordiamo essere moltiplicativa, cioè $N(\alpha\beta) = N(\alpha)N(\beta)$ per ogni $\alpha, \beta \in \mathbb{C}$), ristretta ad A_1. Ora mostriamo che lo stesso vale per $A_2 = \mathbb{Z}[i\sqrt{2}]$.

Proposizione 4. *A_2 è un dominio euclideo con la funzione $N|_{A_2}$, cioè la funzione norma ristretta ad A_2.*

Dimostrazione. Ora siano $a + ub, c + ud \in A_2$ con $c + ud \neq 0$. Vogliamo trovare $q, r \in A_2$ con $a + ub = (c + ud)q + r$ e $N(r) < N(c + ud)$. Abbiamo

$$\frac{a + ub}{c + ud} = \frac{(a + ub)(c - ud)}{(c + ud)(c - ud)} = \frac{(a + ub)(c - ud)}{c^2 + 2d^2} = e + uf \in \mathbb{Q}[u]$$

per opportuni $e, f \in \mathbb{Q}$. Esistono $g, h \in \mathbb{Z}$ tali che $|e-g|, |f-h| \leq 1/2$. Scegliamo

$q = g + uh$ e $r = a + ub - (c + ud)q$ cosicché $a + ub = (c + ud)q + r$. Si ha

$$\begin{aligned}\frac{N(r)}{N(c+ud)} &= N\left(\frac{r}{c+ud}\right) = N\left(\frac{a+ub}{c+ud} - q\right) = N(e + uf - (g + uh)) \\ &= N((e-g) + u(f-h)) = (e-g)^2 + 2(f-h)^2 \\ &\leq (1/2)^2 + 2(1/2)^2 = \frac{3}{4} < 1.\end{aligned}$$

Deduciamo che $N(r) < N(c + ud)$ e il risultato è dimostrato. □

7.2 Applicazione: un'equazione diofantea

Per "equazione diofantea" si intende un'equazione le cui soluzioni si cercano intere, cioè in $\mathbb{Z}$. Un esempio famoso è il seguente: $X^n + Y^n = Z^n$ nelle incognite X, Y, Z, dove n è un intero positivo. Il cosiddetto "ultimo teorema di Fermat", una congettura di Pierre de Fermat del 1637, afferma che tale equazione non ha soluzioni intere non banali (cioè tali che $XYZ \neq 0$) se $n > 2$. Tale congettura è stata dimostrata nel 1995 da Andrew Wiles, ecco un riferimento bibliografico: Wiles, Andrew (1995) "Modular elliptic curves and Fermat's Last Theorem". Annals of Mathematics 141 (3): 443551.

Tornando a noi, ora applichiamo quanto discusso nella sezione 7.1 per trovare tutte le soluzioni intere dell'equazione

$$X^2 + 2 = Y^3.$$

Siano x, y due interi tali che $x^2 + 2 = y^3$. Nel seguito $u = i\sqrt{2} \in \mathbb{C}$.

1. y è dispari. Infatti se y fosse pari allora y^3 sarebbe divisibile per 4 e quindi $x^2 \equiv 2 \mod (4)$. Questo è assurdo perché 2 non è un residuo quadratico modulo 4, cioè non è un quadrato in $\mathbb{Z}/4\mathbb{Z}$. I quadrati modulo 4 sono $0^2 = 0$, $1^2 = 1$, $2^2 = 0$, $3^2 = 1$.

2. Da $x^2 + 2 = y^3$ segue $y^3 = (x + u)(x - u)$. Mostriamo che $x + u$ e $x - u$ sono coprimi in A_2. Sia α un divisore comune di $x + u$ e $x - u$ in A_2. Vogliamo mostrare che α è invertibile in A_2. Siccome α divide $x + u$ e $x - u$, α divide $(x + u) - (x - u) = 2u$ quindi $N(\alpha)$ divide $N(2u) = 8$, in particolare $N(\alpha)$ è una potenza di 2. D'altra parte da $(x + u)(x - u) = y^3$ segue che $N(\alpha)$ divide $N(y^3) = y^6$, che è dispari essendo y dispari per il punto (1). Quindi $N(\alpha)$ è una potenza di 2 dispari, quindi $N(\alpha) = 1$. Scriviamo $\alpha = a + ub$ con $a, b \in \mathbb{Z}$. Allora $1 = N(\alpha) = a^2 + 2b^2 \geq 2b^2$ e questo implica $b = 0$, da cui $a^2 = 1$, e quindi $\alpha = a = \pm 1$ è invertibile.

3. Siccome il cubo y^3 si scrive come prodotto dei due elementi coprimi $x + u$ e $x - u$, dal fatto che A_2 è un dominio a fattorizzazione unica (come ogni dominio euclideo) segue che tali due elementi sono entrambi cubi (!). In particolare esistono $a, b \in \mathbb{Z}$ tali che $x + u = (a + bu)^3$. D'ora in poi sono

conti. Sviluppando il prodotto si ottengono le relazioni $a^3 - 6ab^2 = x$, $3a^2b - 2b^3 = 1$. Dalla seconda otteniamo che b è invertibile in $\mathbb{Z}$ e quindi $b = \pm 1$. Se $b = 1$ allora dalla seconda $3a^2 - 2 = 1$, cioè $a^2 = 1$, cioè $a = \pm 1$. Se $b = -1$ allora dalla seconda $-3a^2 + 2 = 1$, cioè $3a^2 = 1$, impossibile (a è intero). In conclusione $a = \pm 1$ e $b = 1$. Sostituendo nella prima otteniamo che i possibili valori per x sono ± 5, a cui corrisponde il valore $y = 3$. Queste sono soluzioni della nostra equazione. In conclusione, le uniche soluzioni intere di $X^2 + 2 = Y^3$ sono $X = 5, Y = 3$ e $X = -5, Y = 3$.

8 Un caso particolare del Teorema di Dirichlet

Mostriamo che se n è un intero positivo allora ci sono infiniti primi della forma $nt+1$, con t intero positivo. Questo è un caso particolare del teorema di Dirichlet sulle progressioni aritmetiche, che dice che se a, b sono interi positivi coprimi allora ci sono infiniti primi della forma $at + b$ con t intero positivo.

Lemma 3. *Sia $P(X) \in F[X]$, con F campo, e sia a un elemento di una estensione E di F. Allora $(X-a)^2$ divide $P(X)$ in $E[X]$ se e solo se $P(a) = 0$ e $P'(a) = 0$, dove $P'(X)$ indica il polinomio derivato di $P(X)$.*

Dimostrazione. Supponiamo che $(X - a)^2$ divida $P(X)$ in $E[X]$, e scriviamo $P(X) = (X - a)^2 Q(X)$ con $Q(X) \in E[X]$. Allora $P(a) = 0$ e $P'(X) = 2(X - a)Q(X) + (X - a)^2 Q'(X)$ quindi $P'(a) = 0$. Viceversa supponiamo che sia $P(a) = 0$ e $P'(a) = 0$. Da $P(a) = 0$ segue, per il teorema di Ruffini, che $X - a$ divide $P(X)$, scriviamo $P(X) = (X - a)Q(X)$ con $Q(X) \in E[X]$. Per mostrare che $(X - a)^2$ divide $P(X)$ basta quindi mostrare che $Q(a) = 0$, di nuovo per il teorema di Ruffini. Abbiamo $P'(X) = Q(X) + (X - a)Q'(X)$, quindi $P'(a) = Q(a)$ è uguale a zero per ipotesi. □

Supponiamo per assurdo che i numeri primi della forma $nt + 1$ con t intero positivo siano un numero finito, e chiamiamoli $p_1, \ldots, p_h$. Sia $a := np_1 \cdots p_h$. Sia p un divisore primo di $\Phi_n(a)$. Allora $\overline{a} = a + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ è zero del polinomio ridotto $\overline{\Phi_n}(X) \in \mathbb{F}_p[X]$. Riducendo l'uguaglianza $X^n - 1 = \prod_{d|n} \Phi_d(X)$ modulo p otteniamo

$$X^n - 1 = \prod_{d|n} \overline{\Phi_d}(X) \in \mathbb{F}_p[X].$$

Siccome p divide $\Phi_n(a)$, valutando in $X = \overline{a}$ abbiamo $\overline{a}^n - 1 = 0$, e siccome n divide a, questo implica che p non divide n. Segue dal Lemma 3 che $X^n - 1$ non ha zeri multipli in nessuna estensione di $\mathbb{F}_p$, infatti il suo polinomio derivato è nX^{n-1}, che non è il polinomio nullo (perché p non divide n) quindi il suo unico zero è 0, che non è uno zero di $X^n - 1$. Quindi se d_1, d_2 sono due divisori distinti di n allora $\overline{\Phi_{d_1}}(X)$ e $\overline{\Phi_{d_2}}(X)$ non hanno zeri comuni in nessuna estensione di $\mathbb{F}_p$. Sicome $\overline{a}$ è zero di $\overline{\Phi_n}(X)$, segue che $\overline{\Phi_d}(\overline{a}) \neq 0$ per ogni divisore d di n tale

che $d < n$. Quindi se $d < n$ è un divisore di n allora nel campo $\mathbb{F}_p$ si ha

$$\overline{a}^d - 1 = \prod_{d'|d} \overline{\Phi_{d'}}(\overline{a}) \neq 0,$$

cioè $\overline{a}^d \neq 1$. D'altra parte $\overline{\Phi_n}(\overline{a}) = 0$, quindi $\overline{a}^n = 1$. Ne segue che $\overline{a}$ ha ordine n nel gruppo moltiplicativo $\mathbb{F}_p - \{0\}$. Siccome questo gruppo ha ordine $p-1$, dal teorema di Lagrange segue che n divide $p-1$, cioè p è congruo a 1 modulo n, quindi divide a (per definizione di a), cioè $\overline{a} = 0$ e questo contraddice $\overline{a}^n = 1$.

9 Indice di un ideale di $\mathbb{Z}[i]$

Teorema 4. *Sia $0 \neq a + ib \in \mathbb{Z}[i]$. Allora $|\mathbb{Z}[i]/(a+ib)| = N(a+ib) = a^2 + b^2$.*

Prima di procedere alla dimostrazione ci servono alcuni lemmi.

Lemma 4. *Sia n un intero positivo. Allora $|\mathbb{Z}[i]/(n)| = n^2$.*

Dimostrazione. Sia $A := \mathbb{Z}[i]/(n)$ e sia $x+iy+(n) \in A$. Effettuiamo la divisione con resto di x e y per n, trovando $q, r, q', r' \in \mathbb{Z}$ tali che $x = qn+r$ e $y = q'n+r'$ e $0 \leq r < n$, $0 \leq r' < n$. Segue che $x + iy + (n) = (qn + r) + i(q'n + r') = r + ir' + n(q + iq') + (n) = r + ir' + (n)$. Siccome ci sono n scelte per r e n scelte per r' segue che $|A| \leq n^2$. Per mostrare che $|A| = n^2$ rimane da verificare che se $x + iy + (n) = z + iw + (n)$ allora $x \equiv z \mod n\mathbb{Z}$ e $y \equiv w \mod n\mathbb{Z}$. Dire $x+iy+(n) = z+iw+(n)$ è come dire che n divide $x+iy-(z+iw)$ in $\mathbb{Z}[i]$, cioè esiste $a+ib \in \mathbb{Z}[i]$ con $x+iy-(z+iw) = (a+ib)n$, cioè $(x-z)+i(y-w) = an+ibn$ da cui $an = x - z$ e $bn = y - w$, in particolare $x \equiv z \mod n\mathbb{Z}$ e $y \equiv w \mod n\mathbb{Z}$. □

Lemma 5. *Sia $a + ib \in \mathbb{Z}[i]$. Allora gli anelli $\mathbb{Z}[i]/(a+ib)$ e $\mathbb{Z}[i]/(a-ib)$ sono isomorfi.*

Dimostrazione. Un isomorfismo è dato da $\mathbb{Z}[i]/(a+ib) \to \mathbb{Z}[i]/(a-ib)$, $x+iy+(a+ib) \mapsto x - iy + (a - ib)$. □

Lemma 6. *Sia $a + ib \in \mathbb{Z}[i]$. Allora $a + ib$ e $a - ib$ sono associati in $\mathbb{Z}[i]$ se e solo se $a = 0$ oppure $b = 0$ oppure $a = b$ oppure $a = -b$.*

Dimostrazione. Se $a = 0$ allora $a + ib = ib$ e $\overline{ib} = -ib$ è associato a b essendo $-i$ invertibile. Se $b = 0$ allora $a + ib = a$ e $\overline{a} = a = 1 \cdot a$ è associato ad a essendo 1 invertibile. Se $a = b$ allora $a+ib = a(1+i)$ e quindi $(-i)(a+ib) = -ia(1+i) = a(1-i) = a - ia = a - ib$, da cui $a + ib$ e $a - ib$ sono associati. Analogamente se $a = -b$ allora $a + ib = a(1 - i)$ e quindi $i(a + ib) = ia(1 - i) = a(1 + i) = a + ia = a - ib$, da cui $a + ib$ e $a - ib$ sono associati.

Mostriamo il viceversa. Supponiamo che $a + ib$ e $a - ib$ siano associati e mostriamo che $a = 0$ oppure $b = 0$ oppure $a = b$ oppure $a = -b$. Siccome gli invertibili di $\mathbb{Z}[i]$ sono $1, -1, i, -i$ si hanno quattro casi.

- $a+ib = a-ib$. In questo caso $b = -b$ cioè $b = 0$.
- $a+ib = -(a-ib)$. In questo caso $a = -a$ cioè $a = 0$.
- $a+ib = i(a-ib)$. In questo caso $a = b$.
- $a+ib = -i(a-ib)$. In questo caso $a = -b$.

La dimostrazione è conclusa. □

Mostriamo ora il Teorema 4. Se $a+ib$ è invertibile allora $(a+ib) = \mathbb{Z}[i]$ e $N(a+ib) = 1$, quindi il risultato è vero. Supponiamo ora che $a+ib$ non sia invertibile. Per cominciare fattorizziamo $a+ib$ in irriducibili, $a+ib = r_1^{a_1} \cdots r_t^{a_t}$, con $r_1, \ldots, r_t$ irriducibili a due a due non associati (due elementi x, y si dicono "associati" se esiste un elemento invertibile u tale che $y = ux$ - equivalentemente, x e y generano lo stesso ideale principale, cioè $(x) = (y)$). Siccome r_i, r_j sono irriducibili non associati se $i \neq j$, essi sono coprimi, quindi lo sono anche $r_i^{a_i}$ e $r_j^{a_j}$, e quindi per il teorema cinese del resto

$$\mathbb{Z}[i]/(a+ib) = \mathbb{Z}[i]/(r_1^{a_1} \cdots r_t^{a_t}) \cong \mathbb{Z}[i]/(r_1^{a_1}) \times \cdots \times \mathbb{Z}[i]/(r_t^{a_t}).$$

Siccome la funzione norma $N(x+iy) = x^2+y^2$ è moltiplicativa, segue che basta mostrare che il risultato vale per gli elementi del tipo r^a con r irriducibile, infatti se così è allora

$$\begin{aligned} |\mathbb{Z}[i]/(a+ib)| &= |\mathbb{Z}[i]/(r_1^{a_1}) \times \cdots \times \mathbb{Z}[i]/(r_t^{a_t})| = |\mathbb{Z}[i]/(r_1^{a_1})| \cdots |\mathbb{Z}[i]/(r_t^{a_t})| \\ &= N(r_1^{a_1}) \cdots N(r_t^{a_t}) = N(r_1^{a_1} \cdots r_t^{a_t}) = N(a+ib). \end{aligned}$$

Supponiamo quindi ora che $a+ib$ sia della forma r^a con $r = x+iy$ irriducibile. Se $r = x+iy$ e uno tra x e y è zero allora $(r) = (x)$ oppure $(r) = (y)$ quindi il risultato segue dal Lemma 4. Supponiamo ora che sia $x \neq 0 \neq y$. Allora $N(r) = r\overline{r}$ è un numero primo p.

Supponiamo dapprima che r e $\overline{r}$ non siano associati. Allora, essendo irriducibili, sono coprimi (non avendo fattori irriducibili in comune) e quindi anche r^a e $\overline{r^a} = \overline{r}^a$ sono coprimi. Segue dal teorema cinese del resto che

$$\mathbb{Z}[i]/(p^a) = \mathbb{Z}[i]/((r\overline{r})^a) = \mathbb{Z}[i]/(r^a\overline{r^a}) \cong \mathbb{Z}[i]/(r^a) \times \mathbb{Z}[i]/(\overline{r^a}).$$

Per i Lemmi 4 e 5 si ha allora

$$p^{2a} = |\mathbb{Z}[i]/(p^a)| = |\mathbb{Z}[i]/(r^a) \times \mathbb{Z}[i]/(\overline{r^a})| = |\mathbb{Z}[i]/(r^a)| \cdot |\mathbb{Z}[i]/(\overline{r^a})| = |\mathbb{Z}[i]/(r^a)|^2.$$

Estraendo le radici quadrate otteniamo $|\mathbb{Z}[i]/(r^a)| = p^a = N(r)^a = N(r^a)$.

Supponiamo ora che r e $\overline{r}$ siano associati. Allora siccome $x \neq 0 \neq y$, segue dal Lemma 6 che $r = x(1+i)$ con $x \neq 0$, e siccome r è irriducibile segue che x è invertibile, quindi r^a e $(1+i)^a$ generano lo stesso ideale principale. Siamo

quindi ridotti a mostrare che $|\mathbb{Z}[i]/((1+i)^a)| = N((1+i)^a) = 2^a$. Abbiamo la catena di inclusioni proprie

$$\mathbb{Z}[i] \supset (1+i) \supset ((1+i)^2) \supset \cdots \supset ((1+i)^a) \supset \cdots \supset ((1+i)^{2a}) = (2^a).$$

Tali inclusioni sono proprie perché se fosse $((1+i)^k) = ((1+i)^{k+1})$ allora esisterebbe un invertibile u di $\mathbb{Z}[i]$ con $u(1+i)^k = (1+i)^{k+1}$ da cui $(1+i)^k(u-(1+i)) = 0$ e siccome $\mathbb{Z}[i]$ è un dominio di integrità e $1+i \neq 0$ segue $u = 1+i$, assurdo perché $1+i$ non è invertibile (ha norma 2). Mostriamo che i gruppi additivi $((1+i)^k)/((1+i)^{k+1})$ sono tutti isomorfi. Per farlo basta trovare isomorfismi di gruppi additivi

$$((1+i)^k)/((1+i)^{k+1}) \cong ((1+i)^{k+1})/((1+i)^{k+2})$$

per ogni $k \geq 0$, dove $((1+i)^0)$ indica $\mathbb{Z}[i]$. Per ottenere tale isomorfismo basta mandare $x + ((1+i)^{k+1})$ in $x(1+i) + ((1+i)^{k+2})$. Si verifica facilmente che questo è un ben definito isomorfismo di anelli. Segue che detto $t := |\mathbb{Z}[i]/(1+i)|$ si ha $|((1+i)^k)/((1+i)^{k+1})| = t$ per ogni $k \geq 0$. Facendo riferimento alla catena di cui sopra, per la formula degli indici nei gruppi finiti (quella che dice che se $K \leq H \leq G$ in un gruppo finito G allora $|G:K| = |G:H| \cdot |H:K|$) si ha $t^{2a} = |\mathbb{Z}[i]/(2^a)| = 2^{2a}$ da cui $t = 2$ e quindi, di nuovo per la formula degli indici, $|\mathbb{Z}[i]/((1+i)^a)| = t^a = 2^a = N((1+i)^a)$. Questo conclude la dimostrazione del Teorema 4.

Osserviamo che l'ideale $(a+ib)$ di $\mathbb{Z}[i]$ come sottogruppo additivo è generato dai due elementi $a+ib$ e $-b+ia$, infatti $(a+ib)(c+id) = c(a+ib)+d(-b+ia)$. Notiamo che $\left|\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right| = a^2+b^2$, e naturalmente la funzione $a+ib \mapsto (a,b)$ determina un isomorfismo di gruppi additivi $\mathbb{Z}[i] \to \mathbb{Z}^2$.

Più in generale se H è un sottogruppo additivo di $\mathbb{Z}^2$ generato da due elementi (x,y) e (z,w) linearmente indipendenti su $\mathbb{Q}$ allora l'indice $|\mathbb{Z}^2 : H|$ è uguale a $\left|\det \begin{pmatrix} x & y \\ z & w \end{pmatrix}\right|$.

10 Un elemento non costruibile di grado 4

Un elemento $\alpha \in \mathbb{C}$ si dice costruibile (con riga e compasso) se esiste una catena di sottocampi

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n$$

tali che $\alpha \in L_n$ e $|L_{i+1} : L_i| = 2$ per ogni $i = 0, \ldots, n-1$. Tale catena si chiama "*torre di radici quadrate*". In particolare segue dalla formula dei gradi che $|L_n : \mathbb{Q}| = 2^n$ quindi α appartiene a un'estensione di $\mathbb{Q}$ di grado 2^n, in particolare, di nuovo dalla formula dei gradi, essendo $|L_n : \mathbb{Q}| = |L_n : \mathbb{Q}(\alpha)| \cdot |\mathbb{Q}(\alpha) : \mathbb{Q}|$ segue che anche il grado di α su $\mathbb{Q}$ è una potenza di 2. Sappiamo inoltre che l'insieme degli elementi costruibili è un sottocampo di $\mathbb{C}$, e tale sottocampo è chiuso per

estrazione di radici quadrate (segue infatti subito dalla definizione di elemento costruibile che le radici quadrate di un elemento costruibile sono costruibili) e per passaggio al coniugato complesso (per vederlo basta osservare che coniugando una torre di radici quadrate si ottiene una torre di radici quadrate).

Per esempio $\sin(2\pi/11)$ non è costruibile su $\mathbb{Q}$, infatti se lo fosse allora anche $\cos(2\pi/11) = \pm\sqrt{1-\sin^2(2\pi/11)}$ lo sarebbe (gli elementi costruibili formano un campo chiuso per estrazione di radici quadrate), quindi siccome i è costruibile (essendo una radice quadrata di -1) anche $e^{i\pi/11} = \cos(2\pi/11) + i\sin(2\pi/11)$ è costruibile. Ma questo è assurdo perché $e^{i\pi/11}$ è una radice primitiva undicesima di 1, quindi il suo polinomio minimo è l'undicesimo polinomio ciclotomico, che ha grado $\varphi(11) = 10$, non una potenza di 2. Usando la teoria di Galois si dimostra che le radici primitive n-esime di 1 (e quindi gli n-agoni regolari) sono costruibili se e solo se $\varphi(n)$ è una potenza di 2.

Ora viene spontaneo chiedersi: è vero che essere costruibili equivale ad avere grado una potenza di 2? La risposta è no, ed ora forniamo un controesempio.

10.1 Un elemento non costruibile di grado 4

Vogliamo esibire un elemento non costruibile di grado 4 su $\mathbb{Q}$.

Sia $f(X) = X^4 - 4X + 2 \in \mathbb{Q}[X]$. Si tratta di un polinomio irriducibile, per il criterio di Eisenstein applicato al primo 2. Siano α_1, α_2, α_3, α_4 gli zeri di $f(X)$ in $\mathbb{C}$. Da un semplice studio di funzione si deduce che due di essi sono reali e gli altri due no, diciamo che quelli reali sono α_1 e α_2, e diciamo che $\alpha_4 = \overline{\alpha_3}$ (dove $\overline{a+ib} = a - ib$ indica il coniugio). Fattorizziamo $f(X)$ su $\mathbb{R}$: scriviamo $(X-\alpha_1)(X-\alpha_2) = X^2 + aX + b$, $(X-\alpha_3)(X-\alpha_4) = X^2 + cX + d$ con $a, b, c, d \in \mathbb{R}$, da cui

$$X^2 - 4X + 2 = (X^2 + aX + b)(X^2 + cX + d) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4).$$

Svolgendo i calcoli si ottiene $c = -a$, $b + d = a^2$, $a(d-b) = -4$ e $bd = 2$, e anche $a = -(\alpha_1 + \alpha_2)$, $b = \alpha_1\alpha_2$, $c = -(\alpha_3 + \alpha_4)$ e $d = \alpha_3\alpha_4$.

Nel seguito dimostriamo che α_3 non è costruibile. Se lo fosse, siccome gli elementi costruibili formano un campo chiuso per passaggio al coniugato e $\alpha_4 = \overline{\alpha_3}$, $c = -(\alpha_3 + \overline{\alpha_3})$ e $d = \alpha_3\overline{\alpha_3}$ sono costruibili, quindi anche $a = -c$ è costruibile e anche $b = a^2 - d$ è costruibile. Quindi anche $t := b + d$ è costruibile. Ora,

$$t(t^2 - 8) = a^2((b+d)^2 - 8) = a^2((b+d)^2 - 4bd) = a^2(b-d)^2 = 16,$$

dove il primo passaggio segue da $b + d = a^2$, il secondo da $bd = 2$, e il quarto da $a(d-b) = -4$. Quindi t è zero del polinomio $X^3 - 8X - 16$, irriducibile su $\mathbb{Z}$ (ha grado 3 e non ha zeri interi), dunque su $\mathbb{Q}$ (per il Lemma di Gauss). $b + d$ risulta essere un elemento costruibile di grado 3, assurdo: 3 non è una potenza di 2.

Siccome il polinomio minimo di t sembra un po' tirato fuori dal cappello, ora indaghiamo alcune ragioni un po' meno casuali per cui accade questo fenomeno.

10.2 Alcune ragioni profonde

Consideriamo di nuovo il nostro polinomio $f(X) = X^4 - 4X + 2 \in \mathbb{Q}[X]$. Sia E il suo campo di spezzamento contenuto in $\mathbb{C}$, $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, e consideriamo l'insieme $\mathcal{G}_f$ degli isomorfismi di campo $E \to E$. Tale insieme, denotato anche con $\mathrm{Aut}(E)$ (l'insieme degli automorfismi di E) ha struttura di gruppo data dalla composizione. Si chiama il "gruppo di Galois" di $f(X)$ (Nota Bene: su un campo che non è $\mathbb{Q}$ la definizione di gruppo di Galois è diversa da questa, si richiede anche che tali isomorfismi ristretti al campo base siano l'identità - nel caso di $\mathbb{Q}$ questo è automatico).

Sia $L_{\mathcal{G}_f}$ l'insieme dei sottogruppi di $\mathcal{G}_f$ e sia L_E l'insieme dei sottocampi di E. Per ogni $H \in L_{\mathcal{G}_f}$ definiamo

$$H' := \{x \in E \ : \ \sigma(x) = x \ \forall \sigma \in H\}$$

e per ogni $K \in L_E$ definiamo

$$K' := \{\sigma \in \mathcal{G}_f \ : \ \sigma(x) = x \ \forall x \in K\}.$$

Risulta che le due funzioni (dette corrispondenze di Galois)

$$L_{\mathcal{G}_f} \to L_E, \ H \mapsto H', \qquad L_E \to L_{\mathcal{G}_f}, \ K \mapsto K'$$

sono biiezioni, una l'inversa dell'altra, che invertono le inclusioni, nel senso che se $H_1 \leq H_2$ sono sottogruppi di $\mathcal{G}_f$ allora $H_2' \subseteq H_1'$ e se $K_1 \subseteq K_2$ sono sottocampi di E allora $K_2' \leq K_1'$. Inoltre $|H_2 : H_1| = |H_1' : H_2'|$ e $|K_1 : K_2| = |K_2' : K_1'|$ dove la scrittura $|A : B|$ indica da una parte un indice, dall'altra un grado. Inoltre $\mathbb{Q}' = \mathcal{G}_f$, $\mathcal{G}_f' = \mathbb{Q}$ e $|\mathcal{G}_f| = |E : \mathbb{Q}|$.

Ebbene ora sia $K := \mathbb{Q}(\alpha_3)$. Abbiamo visto che α_3 non è costruibile, e $|K : \mathbb{Q}| = 4$. Ne segue che non ci sono sottogruppi di $\mathcal{G}_f$ propriamente compresi tra K' e $\mathcal{G}_f$, infatti se esistesse H sottogruppo di $\mathcal{G}_f$ con $K' < H < \mathcal{G}_f$ allora $\mathbb{Q} = \mathcal{G}_f' < H' < K'' = K$ e siccome $|K : \mathbb{Q}| = 4$ si avrebbe $|H' : \mathbb{Q}| = 2$, e quindi $\mathbb{Q} \subset H' \subset K$ sarebbe una torre di radici quadrate, assurdo. In altre parole il fatto che α_3 non è costruibile si traduce nel fatto che $\mathbb{Q}(\alpha_3)'$ è un sottogruppo massimale di $\mathcal{G}_f$, di indice $|\mathcal{G}_f : K'| = |K'' : \mathcal{G}_f'| = |K : \mathbb{Q}| = 4$. Usando la teoria di Galois si vede che $\mathcal{G}_f \cong S_4$, il gruppo simmetrico di grado 4 (in particolare $|E : \mathbb{Q}| = |\mathcal{G}_f| = |S_4| = 24$) ed effettivamente gli stabilizzatori dei punti di S_4 sono sottogruppi massimali di indice 4.

Per la cronaca, detto $\alpha \in \mathbb{C}$ e detto E il campo di spezzamento contenuto in $\mathbb{C}$ del polinomio minimo $f(X)$ di α su $\mathbb{Q}$, dire che α è costruibile è come dire

che $|E : \mathbb{Q}| = |\mathcal{G}_f|$ è una potenza di 2. Quindi ora il mistero è se non svelato perlomeno chiarito: non basta che un elemento abbia grado una potenza di 2 perché sia costruibile, serve che il campo di spezzamento del suo polinomio minimo abbia grado una potenza di 2.