Esercitazioni di algebra 2

Francesco Genovese

4 giugno 2015

1 Il teorema di omomorfismo e i suoi amici (12/03/2015)

1.1 Relazioni e funzioni

Definizione 1.1. Una *relazione* tra l'insieme X e l'insieme Y è un sottoinsieme $R \subseteq X \times Y$.

Proposizione 1.2. *Le relazioni tra X e Y sono in corrispondenza biunivoca con le funzioni $X \to \mathcal{P}(Y)$.*

La proposizione sopra discende da un risultato un po' più generale. Dati due insiemi X e Y, poniamo:

$$Y^X := \{f : X \to Y\}, \tag{1.1}$$

l'insieme di tutte le funzioni $X \to Y$. Abbiamo allora:

Teorema 1.3. *Esiste una biezione naturale:*

$$Z^{X \times Y} \longleftrightarrow (Z^Y)^X. \tag{1.2}$$

Dimostrazione. Data $f : X \times Y \to Z$, definiamo $\tilde{f} : X \to Z^Y$ mediante

$$x \mapsto \tilde{f}_x,$$
$$\tilde{f}_x(y) = f(x, y).$$

Dando questa stessa definizione "alla rovescia", si ottiene direttamente la corrispondenza inversa. □

Ora, si può dimostrare direttamente la Proposizione 1.2 semplicemente ricordando che i sottoinsiemi $R \subseteq X \times Y$ sono in corrispondenza biunivoca con le funzioni $X \times Y \to \{0, 1\}$.

Nota 1.4. Una relazione $R \subseteq X \times Y$ si identifica ad una funzione $X \to Y$ se e solo se la corrispondente funzione $\tilde{R} : X \to \mathcal{P}(Y)$ è tale che $|\tilde{R}(x)| = 1$ per ogni $x \in X$.

1.2 Variazioni sul tema del teorema di omomorfismo

Teorema 1.5 (Teorema di omomorfismo per gruppi)**.** *Sia $f\colon G \to G'$ un omomorfismo di gruppi, e sia $N \subseteq G$ un sottogruppo normale. Supponiamo che $N \subseteq \ker(f)$. Allora, esiste un unico omomorfismo $f'\colon G/N \to G'$ tale che il seguente diagramma è commutativo:*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow{\scriptstyle \pi} & \nearrow_{f'} & \\ G/N. & & \end{array} \tag{1.3}$$

Inoltre, se $N = \ker(f)$, allora f' è iniettiva.

Dimostrazione. È formalmente ovvia. Bisogna solo stare attenti alla *buona definizione* di f'. Si inizia definendo f' solo come relazione, e mostrando poi che in realtà è una funzione, e anzi è un omomorfismo. Ricordando la Proposizione 1.2, definiamo $f' : G/N \to \mathcal{P}(G')$ nell'unico modo sensato:

$$f'(x) = \{f(g) : g \in \pi^{-1}(x)\}.$$

Dimostriamo che, per ogni $x \in G/N$, $f'(x)$ è un singoletto. Siano $f(g_1), f(g_2) \in f'(x)$. Allora, $g_1 g_2^{-1} \in \pi^{-1}(1_{G/N}) = N \subseteq \ker(f)$, dunque $f(g_1 g_2^{-1}) = 1_{G'}$, dunque $f(g_1) = f(g_2)$. Abbiamo dimostrato che due qualsiasi elementi di $f'(x)$ coincidono, cioè esattamente che $|f'(x)| = 1$, dunque f' definisce in realtà una funzione $G/N \to G'$. Per vedere che è un omomorfismo, basta appoggiarsi al fatto che f è un omomorfismo (esercizio). □

Proposizione 1.6. *Siano G, G' due gruppi, e siano $N \subseteq G$, $N' \subseteq G'$ due sottogruppi normali rispettivamente di G e G'. Sia $f\colon G \to G'$ un omomorfismo tale che $f(N) \subseteq N'$. Allora, esiste un unico omomorfismo $f'\colon G/N \to G'/N'$ tale che il seguente diagramma è commutativo:*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow & & \downarrow \\ G/N & \xrightarrow{f'} & G'/N'. \end{array} \tag{1.4}$$

Dimostrazione. Applicare il teorema di omomorfismo alla composizione $G \xrightarrow{f} G' \to G'/N'$. □

Il teorema di omomorfismo vale in tantissimi contesti, oltre che per i gruppi. È vero per anelli, spazi vettoriali, e in una forma più involuta persino per insiemi e funzioni.

Esercizi e applicazioni

Sia $F : V \to W$ un'applicazione lineare tra spazi vettoriali. Un famoso risultato di algebra lineare ci dice che

$$\dim(V) = \dim(\ker(F)) + \dim(\mathrm{im}(F)).$$

Tale risultato è intimamente legato al teorema di omomorfismo per spazi vettoriali e applicazioni lineari. Nella teoria dei gruppi finiti esiste il suo preciso analogo:

Proposizione 1.7. *Sia $f : G \to G'$ un omomorfismo di gruppi, e supponiamo che G sia finito. Allora*

$$|G| = |\ker(f)||\mathrm{im}(f)|. \tag{1.5}$$

Dimostrazione. Il teorema di omomorfismo ci dice che $G/\ker(f) \cong \mathrm{im}(f)$. Dunque, basta dimostrare che $|G/\ker(f)| = |G|/|\ker(f)|$. Sia $\pi : G \to G/\ker(f)$ la proiezione. Notiamo che, per ogni $[g] \in G/\ker(f)$, $\pi^{-1}([g]) = g\ker(f)$ (il laterale di g), e la sua cardinalità è sempre quella di $\ker(f)$. Ora, abbiamo:

$$|G| = \sum_{x \in G/\ker(f)} |\pi^{-1}(x)| = \sum_{x \in G/\ker(f)} |\ker(f)| = |G/\ker(f)||\ker(f)|. \qquad \square$$

Il risultato appena visto ha una certa utilità nello studio delle proprietà degli omomorfismi di gruppi finiti. Potrà capitare di impiegarlo in seguito.

Proposizione 1.8. *Sia G un gruppo. Un sottogruppo $H \subseteq G$ è normale se e solo se è il nucleo di un qualche omomorfismo $G \to G'$.*

Dimostrazione. Se H è normale, è il nucleo dell'omomorfismo di proiezione $G \to G/H$. Viceversa, i nuclei di omomorfismi sono sempre sottogruppi normali (esercizio). $\square$

Esercizio 1.9. *Esistono omomorfismi suriettivi $D_3 \to C_2$? Quanti sono? E $D_3 \to C_3$?*

Risoluzione. Ricordiamo che D_3 ha un sottogruppo normale di ordine 3, ma non ha sottogruppi normali di ordine 2. $\square$

1.3 Una breve digressione

Al matematico, una cosa che interessa moltissimo è *risolvere equazioni*, ossia, detto in termini un po' generali, date funzioni $f, g \colon X \to Y$, determinare l'insieme

$$\mathrm{eq}(f, g) = \{x \in X : f(x) = g(x)\}. \tag{1.6}$$

Se X e Y (e f, g con loro) sono muniti di struttura addizionale, per esempio se f e g sono applicazioni lineari di spazi vettoriali, allora $f(x) = g(x)$ equivale a dire $(f - g)(x) = 0_Y$, e ciò che in definitiva conta è il *luogo degli zeri*, che è poi il nucleo

$\ker(F)$ di $F = f - g$. Nel seguito della discussione, per semplicità, ci limiteremo a considerare problemi di questo tipo, ambientati nella categoria degli spazi vettoriali.

In alcuni casi, il matematico non intende solo trovare gli zeri di una certa applicazione lineare $F\colon X \to Y$. Può essere (perversamente?) interessato a *fabbricarsi* un posto dove $F(x) = 0$ sia verificata *per ogni* $x \in X$. Questo implica modificare Y e sostituirlo con uno spazio vettoriale in cui gli elementi del tipo $F(x)$ siano nulli. È una costruzione *duale* a quella di $\ker(F)$, e che chiameremo *conucleo di* F, denotandolo $\operatorname{coker}(F)$. Cosa pretendiamo da questo conucleo? Sensatamente, vogliamo che esista una mappa $\pi\colon Y \to \operatorname{coker}(F)$ (quella che ci permette di proiettare gli elementi di Y in questo spazio) fatta in modo che la composizione

$$X \xrightarrow{F} Y \xrightarrow{\pi} \operatorname{coker}(F)$$

sia zero. Questo cattura l'idea che "$F(x) = 0$ in $\operatorname{coker}(F)$ per ogni x". D'altra parte, non vogliamo essere spreconi. Infatti, potremmo essere tentati di porre $\operatorname{coker}(F) = 0$, e così facendo avremmo sicuramente annullato tutti gli elementi $F(x)$, ma anche tanti altri elementi che vogliamo preservare... Insomma noi vogliamo che, proiettando in $\operatorname{coker}(F)$, gli elementi $F(x)$ siano tutti e soli quelli che si annullano. Questo, un po' più formalmente, equivale a pretendere che

$$\ker(\pi) = \operatorname{im}(F).$$

A questo punto, abbiamo la possibilità di indovinare la definizione più sensata:

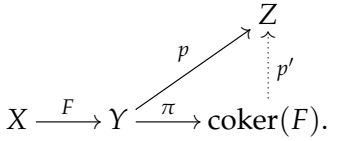
$$\operatorname{coker}(F) = Y / \operatorname{im}(F). \tag{1.7}$$

La matematica moderna, a questo punto, è così raffinata che permette persino di formalizzare l'idea che "non siamo stati spreconi". Infatti, il conucleo così costruito soddisfa una proprietà di "minimalità" (più precisamente, si dovrebbe dire *inizialità*), nel senso del seguente risultato.

Proposizione 1.10. *Sia $F : X \to Y$ un'applicazione lineare di spazi vettoriali. Sia $p : Y \to Z$ una qualsiasi applicazione lineare tale che la composizione*

$$X \xrightarrow{F} Y \xrightarrow{p} Z$$

sia zero, in altre parole $\operatorname{im}(F) \subseteq \ker(p)$. *Allora, esiste un'unica applicazione lineare $p' :$ $\operatorname{coker}(F) \to Z$ tale che il seguente diagramma è commutativo:*



Dimostrazione. È un'immediata applicazione del teorema di omomorfismo nella categoria degli spazi vettoriali. □

Quello che si nota dal diagramma sopra è proprio che la proiezione $\pi : Y \to \operatorname{coker}(F)$ è "iniziale" tra tutte le mappe $p : Y \to Z$ che annullano F. Questo ci assicura del fatto che la definizione di $\operatorname{coker}(F)$ che abbiamo dato è effettivamente quella sensata.

Nota 1.11. I conuclei esistono in tantissime categorie oltre a quella degli spazi vettoriali. Per quanto riguarda i gruppi, bisogna fare un po' attenzione: l'immagine di un omomorfismo di gruppi non è in generale un sottogruppo normale, e non è possibile fare il quoziente. Si può ovviare a questo problema nel modo più ovvio: considerare il più piccolo sottogruppo normale che contiene l'immagine.

Per fare pratica con conuclei e quozienti, dimostriamo la seguente:

Proposizione 1.12 ("Mayer-Vietoris lineare")**.** *Sia Z uno spazio vettoriale (pensato come "ambiente"), e siano $V, W \subseteq Z$ due suoi sottospazi. Indichiamo con $V + W$ il sottospazio somma di V e W in Z, e con $V \oplus W$ la somma diretta esterna di V e W. Allora, esiste una successione di applicazioni lineari*

$$V \cap W \xrightarrow{i} V \oplus W \xrightarrow{f} V + W,$$

con $i(v) = (v, v)$, $f(v, w) = v - w$, tale che i è iniettiva, f è suriettiva, e $\operatorname{im} i = \ker f$. In particolare

$$V + W \cong (V \oplus W)/i(V \cap W) = \operatorname{coker} i.$$

Inoltre, se V e W hanno dimensione finita, deduciamo che

$$\dim(V + W) = \dim V + \dim W - \dim(V \cap W).$$

Dimostrazione. i e f definiscono applicazioni lineari (esercizio). i è chiaramente iniettiva; f è suriettiva, infatti ogni elemento $z \in V + W$ si scrive come $z = v + w = v - (-w)$ per qualche $v \in V, w \in W$. Dato $v \in V \cap W$, $f(i(v)) = f(v, v) = v - v = 0$, e questo dimostra che $\operatorname{im} i \subseteq \ker f$. Viceversa, se $(v, w) \in \ker f$, allora $v - w = 0$ in Z, cioè $v = w$, da cui deduciamo che $v \in V \cap W$ e $(v, w) = i(v)$. Applicando direttamente il teorema di omomorfismo a f e tenendo presente che $\ker f = \operatorname{im} i$, allora, vediamo che esiste un isomorfismo $\widetilde{f} : \operatorname{coker} i \to V + W$ tale che il seguente diagramma è commutativo:

$$\begin{array}{ccc} V \oplus W & \xrightarrow{f} & V + W \\ \downarrow & \nearrow_{\widetilde{f}} & \\ \operatorname{coker} i & & \end{array}$$

(ricordiamo infatti che $\operatorname{coker} i = (V \oplus W)/\operatorname{im} i = (V \oplus W)/\ker f$). La formula delle dimensioni, a questo punto, segue immediatamente, ricordando che in generale $\dim(Z_1/Z_2) = \dim Z_1 - \dim Z_2$. □

Nota 1.13. Si faccia sempre molta attenzione a distinguere le costruzioni *interne* (es. la somma di due sottospazi di un dato spazio ambiente) dalle costruzioni *esterne* (dati due spazi vettoriali, è possibile costruire in astratto la loro somma diretta). Il risultato appena visto ci dà, in un certo senso, un modo per confrontare la costruzione interna della somma di V e W, che potrebbero intersecarsi non banalmente, con la costruzione esterna della somma diretta di V e W, che prescinde dal loro vivere nello spazio ambiente Z.

2 Esercizi sui teoremi di Sylow (26/03/2015)

Richiamiamo il teorema di Sylow e i risultati ad esso collegati:

Teorema 2.1. *Sia G un gruppo finito, sia p un primo che divide $|G|$, e scriviamo $|G| = p^a b$, con $p \nmid b$. Allora:*

1. *G ammette un p-sottogruppo di Sylow, cioè un sottogruppo di ordine p^a.*
2. *I sottogruppi di Sylow formano una classe di coniugio di sottogruppi di G.*
3. *Il numero n_p dei p-Sylow di G è congruo a 1 modulo p.*
4. *Se P è un p-Sylow di G, allora $n_p = |G|/|N_G(P)|$, dove $N_G(P) = \{g \in G : gPg^{-1} = P\}$ è il normalizzante di P in G. In particolare, $n_p \mid |G|$, e anzi $n_p \mid b$ (per il fatto che è coprimo con p).*

Useremo estensivamente questi risultati per risolvere i prossimi esercizi.

Esercizio 2.2. *Sia G un gruppo di ordine 12. Allora, se $n_3 > 1$, G è isomorfo al gruppo alterno A_4.*

Risoluzione. Se $n_3 > 1$, allora (soliti argomenti) necessariamente $n_3 = 4$. Sian $X = \{P_1, \dots, P_4\}$ l'insieme dei 3-Sylow di G. G agisce su X per coniugio, dando origine ad un omomorfismo

$$\begin{aligned} \varphi : G &\to \mathrm{Perm}(X) \equiv S_4, \\ g &\mapsto \varphi_g, \\ \varphi_g(P) &= gPg^{-1}. \end{aligned}$$

L'obiettivo è far vedere che φ è iniettivo e $\operatorname{im}\varphi = A_4$. Iniziamo notando che

$$\ker\varphi = \{g \in G : gPg^{-1} = P \quad \forall P \in X\} = \bigcap_{n=1}^{3} N_G(P_i).$$

D'altra parte, $|G|/|N_G(P_i)| = n_3 = 4$, dunque $|N_G(P_i)| = 3$. Inoltre, $P_i \subseteq N_G(P_i)$ ed entrambi hanno ordine 3, dunque $P_i = N_G(P_i)$ e $\ker\varphi = \bigcap_{i=1}^{3} P_i$. I P_i sono distinti e

hanno ordine primo, dunque $P_i \cap P_j = \{1\}$ se $i \neq j$. Concludiamo che $\ker \varphi = \{1\}$, e φ è un omomorfismo iniettivo.

Controlliamo ora che $\operatorname{im} \varphi = A_4$. Per farlo, vediamo un po' più da vicino la struttura di G. I P_i hanno ordine 3, e sono in tutto 4, dunque ho in totale $2 \cdot 4 = 8$ elementi di ordine 3. Questo, in particolare, è vero per $\operatorname{im} \varphi \subset S_4$. Ricordiamo che gli elementi di ordine 3 in S_4 sono i 3-cicli, che sono permutazioni pari. Dunque, $\operatorname{im} \varphi \cap A_4$ contiene questi 8 elementi di ordine 3, e d'altra parte è un sottogruppo di A_4. Ma allora, è necessariamente tutto A_4, da cui otteniamo $\operatorname{im} \varphi \subseteq A_4$. Poiché, del resto, $|\operatorname{im} \varphi| = |A_4| = 12$, concludiamo che $\operatorname{im} \varphi = A_4$. □

Il prossimo esercizio si dimostra con le stesse tecniche del precedente, ed è anzi più semplice.

Esercizio 2.3. *Sia G un gruppo di ordine 6 che ammette più di un 2-Sylow. Allora G è isomorfo a S_3.*

Risoluzione. Denotiamo con n_p il numero dei p-Sylow di G. Sappiamo che $n_3 \mid 2$ ed è congruo a 1 modulo 3. Dunque, $n_3 = 1$ e il 3-Sylow è normale. Allo stesso modo, $n_2 \mid 3$ ed è un numero dispari. Per ipotesi $n_2 > 1$, dunque necessariamente $n_2 = 3$. Sia

$$X = \{H_1, H_2, H_3\}$$

l'insieme dei 2-Sylow di G. Sappiamo che G agisce su X per coniugio. In altre parole, abbiamo un omomorfismo di gruppi

$$\begin{aligned} \varphi : G &\to \operatorname{Perm}(X), \\ g &\mapsto \varphi_g, \\ \varphi_g(H) &= gHg^{-1}. \end{aligned}$$

G ha ordine 6 e $\operatorname{Perm}(X)$ si identifica a S_3. Per concludere ci basta dimostrare che φ è iniettivo. Abbiamo che

$$\ker \varphi = \{g \in G : gHg^{-1} = H \quad \forall H \in X\} = \bigcap_{n=1}^{3} N_G(H_i),$$

dove $N_G(H_i)$ è il normalizzatore di H_i in G. Ora, ricordiamo che

$$3 = n_2 = |G|/|N_G(H)| = 6/|N_G(H)|,$$

per un qualsiasi $H \in X$. Dunque, $|N_G(H)| = 2$. D'altra parte, $H \subseteq N_G(H)$ e gli ordini coincidono, quindi deduciamo che $H = N_G(H)$, per ogni $H \in X$. Ora, osserviamo che $H_i \cap H_j = \{1\}$ se $i \neq j$. Concludiamo che $\ker \varphi = \{1\}$, cioè φ è iniettivo, dunque (gli ordini di dominio e codominio coincidono) è un isomorfismo. □

Esercizio 2.4. *Sia G un gruppo di ordine $1125 = 3^2 \cdot 5^3$, tale che il 5-Sylow sia ciclico. Allora G è abeliano.*

Risoluzione. Sia K il 5-Sylow ciclico e sia H un 3-Sylow (di ordine 9). Sappiamo che G è isomorfo ad un prodotto semidiretto $K \rtimes_\varphi H$, per un qualche omomorfismo

$$\varphi : H \to \mathrm{Aut}(K).$$

Poiché K è ciclico di ordine 5^3, abbiamo che $\mathrm{Aut}(K)$ è un gruppo di ordine $5^3 - 5^2 = 100$. D'altra parte

$$9 = |H| = |\varphi(H)||\ker\varphi|,$$

dunque $|\varphi(H)| \mid 9$ e del resto $|\varphi(H)| \mid 100$. Concludiamo che $|\varphi(H)| = 1$, quindi φ è l'omomorfismo banale e G è isomorfo al prodotto diretto $K \times H$. Ora, H ha ordine il quadrato di un primo, dunque è abeliano; concludiamo che $G \cong K \times H$ è abeliano. □

Enunciamo e dimostriamo un risultato vero in una certa generalità, che potrà essere utile tener presente.

Proposizione 2.5. *Sia p un primo, e sia G un gruppo finito semplice di ordine $p^r m$, con $m \nmid p$, $m > 1$, $r \geq 1$. Sia $n = n_p$ il numero dei p-Sylow di G. Allora, G è isomorfo ad un sottogruppo del gruppo alterno A_n. In particolare, $|G| \mid \frac{n!}{2}$.*

Dimostrazione. $n = n_p > 1$, perché altrimenti avremmo un sottogruppo normale proprio di G di ordine p^r, che è contro l'ipotesi di semplicità. Sia

$$X = \{p\text{-Sylow di } G\};$$

G agisce su X per coniugio, cioè esiste un omomorfismo di gruppi:

$$\begin{aligned} \varphi : G &\to \mathrm{Perm}(X) \equiv S_n, \\ g &\mapsto \varphi_g, \\ \varphi_g(P) &= gPg^{-1}. \end{aligned}$$

Sicuramente φ non è l'omomorfismo banale, altrimenti avremmo un (unico) p-Sylow normale. Il nucleo $\ker(\varphi)$ è dunque un sottogruppo normale proprio di G, che per semplicità è banale: $\ker(\varphi) = \{1\}$. Quindi, φ è un omomorfismo iniettivo. Ora, notiamo che l'omomorfismo

$$\varphi(G) \hookrightarrow S_n \to S_n/A_n$$

ha nucleo $\varphi(G) \cap A_n$, e induce un omomorfismo iniettivo

$$\varphi(G)/(\varphi(G) \cap A_n) \to S_n/A_n.$$

Dunque, $\varphi(G) \cap A_n$ ha indice 1 o 2 in $\varphi(G)$, ma se tale indice fosse 2 si tratterebbe di un sottogruppo normale proprio di $\varphi(G)$, e dunque per semplicità $\varphi(G) \cap A_n = \{1\}$; troveremmo un omomorfismo iniettivo $\varphi(G) \to S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$, e dunque in particolare $|G| \leq 2$, ma questo è contro le nostre ipotesi di partenza. Deduciamo che l'indice è 1, da cui $\varphi(G) \cap A_n = \varphi(G)$, cioè

$$\varphi(G) \subseteq A_n,$$

e concludiamo. □

Esercizio 2.6. *Sia G un gruppo di ordine $112 = 2^4 \cdot 7$. Allora G non è semplice.*

Risoluzione. Per assurdo G sia un gruppo semplice di ordine 112. Sia n_2 il numero dei 2-Sylow di G. Allora necessariamente $n_2 = 7$. Per il risultato precedente, abbiamo che l'ordine di G deve dividere l'ordine di A_7, cioè $112 \mid 2520$, il che è falso. Contraddizione! □

Esercizio 2.7. *Sia G un gruppo finito di ordine 351. Allora, G non è semplice.*

Risoluzione. Abbiamo $|G| = 351 = 3^3 \cdot 13$. Sappiamo che $n_{13} \equiv 1 \pmod{13}$, e $n_{13} \mid 27$. Dunque, sono possibili solo due casi: $n_{13} = 1$ oppure $n_{13} = 27$. Se $n_{13} = 1$ abbiamo finito, perché in tal caso il 13-Sylow è normale. Allora, supponiamo che $n_{13} = 27$ e proviamo a dimostrare che $n_3 = 1$ (da cui dedurremo che il 3-Sylow è normale).

Ho 27 distinti 13-Sylow: $H_1, \ldots, H_{27}$. Poiché tali sottogruppi hanno ordine primo e sono distinti, devono intersecarsi banalmente: $H_i \cap H_j = \{1\}$ per ogni $i \neq j$. Infatti, $H_i \cap H_j$ è sottogruppo di H_i e H_j, e può avere ordine solo 1 oppure 13, e se fosse 13 avremmo necessariamente che $H_i \cap H_j = H_i = H_j$. Ora, ogni H_i contiene 12 elementi di ordine 13. Dunque, in tutto, G contiene $12 \cdot 27 = 324$ elementi di ordine 13. Mi restano, allora, $351 - 324 = 27$ elementi di ordine non 13. Ora, sia K un 3-Sylow, che necessariamente ha ordine 27. Dunque, K non contiene elementi di ordine 13, e deduciamo che è formato esattamente dai 27 elementi di ordine non 13. In definitiva, esiste solo un 3-Sylow, che dunque è normale in G. □

3 Esercizi su gruppi di Galois (29/04/2015)

3.1 Scaletta standard per lo svolgimento dei problemi

Gli esercizi sui gruppi di Galois seguono tutti una scaletta abbastanza standard. Si parte da un dato polinomio $p(X) \in K[X]$, dove K è spesso (non per forza sempre) il campo dei razionali $\mathbb{Q}$.

1. Il primo passo consiste nel fattorizzare $p(X)$, oppure dimostrare che è irriducibile. Nel cercare una qualche fattorizzazione, può valere la pena controllare se $p(X)$ è multiplo di un qualche polinomio ciclotomico, ossia provare a sostituire

a X una qualche radice primitiva dell'unità. Per quanto riguarda l'irriducibilità, vi sono i noti criteri (Eisenstein, riduzione modulo un primo ...).

2. Di seguito, bisogna scrivere un campo di spezzamento del polinomio $p(X)$. Poniamo, per farci un'idea, che $p(X) \in \mathbb{Q}[X]$. Se $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ sono le radici di $p(X)$, allora $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ è un campo di spezzamento di $p(X)$ su $\mathbb{Q}$. Se il polinomio non è troppo complicato, potrà essere utile trovare a mano tutte le sue radici.

3. Questo punto è cruciale. Detto L un campo di spezzamento di $p(X)$ su K, bisogna calcolare il grado dell'estensione $[L : K]$. La tecnica che vale *sempre* la pena di ricordare è la "regola della torre": se ho estensioni (finite) di campi $K \subseteq F \subseteq L$, allora
$$[L : K] = [L : F][F : K]. \tag{3.1}$$

4. Supponiamo che $[L : K] = d$. Siccome L è un campo di spezzamento di $p(X)$ su K, è un'estensione normale di K. Sotto buone ipotesi su K (per es. se la caratteristica di K è 0 o se K è perfetto) tale estensione è anche automaticamente separabile. Si tratta dunque di un'estensione di Galois, e in particolare
$$\#\mathrm{Gal}(L|K) = d. \tag{3.2}$$
Dunque, bisogna capire la classe di isomorfismo di $G = \mathrm{Gal}(L|K)$. Per fare ciò, vi sono svariate possibili tecniche, che vedremo nei vari esercizi svolti.

5. Per finire, resta da scrivere esplicitamente la corrispondenza di Galois, applicando direttamente il teorema fondamentale della teoria di Galois. Conoscendo il reticolo dei sottogruppi di G, è possibile risalire al reticolo delle estensioni intermedie tra K e L.

3.2 Alcune cose da segnarsi

Per risolvere al meglio gli esercizi, si fa spesso uso di piccoli risultati *quasi ovvi* che tuttavia vale sempre la pena ricordare. Iniziamo con il seguente:

Proposizione 3.1. *Sia $K \subseteq L$ un'estensione di campi. Allora, $K = L$ se e solo se $[L : K] = 1$.*

Questo risultato viene utilizzato spessissimo, spesso in combinazione con la regola della torre (3.1). Può essere utile vedere anche la seguente (quasi immediata) conseguenza:

Corollario 3.2. *Siano $K \subseteq F_1 \subseteq L$ e $K \subseteq F_2 \subseteq L$ estensioni (finite) di campi. Supponiamo che $[F_1 : K] = [F_2 : K] = d$. Allora, se $F_1 \subseteq F_2$ oppure $F_2 \subseteq F_1$, abbiamo $F_1 = F_2$.*

Dimostrazione. Supponiamo che $F_1 \subseteq F_2$ (l'altro caso è del tutto analogo). Allora, applichiamo direttamente la regola della torre:

$$[F_2 : K] = [F_2 : F_1][F_1 : K], \tag{3.3}$$

da cui troviamo che, per ipotesi, $d = [F_2 : F_1]d$, e quindi necessariamente $[F_2 : F_1] = 1$, e concludiamo. □

Quando si tratta di capire la struttura di un certo gruppo di Galois, una tecnica (come si vedrà dagli esercizi) è quella di cercare a mano gli automorfismi di cui è fatto. Spesso, uno si occupa di automorfismi $\sigma : K(\alpha) \to K(\alpha)$ che ristretti a K sono l'identità. Verrebbe voglia di affermare che per definire un σ siffatto basta stabilire il valore $\sigma(\alpha)$. Questo in effetti è vero, ma con un *caveat*:

Proposizione 3.3. *Sia $K \subseteq L$ un'estensione di campi, e sia $\alpha \in L$ algebrico su K. Sia $p_\alpha(X) \in K[X]$ il polinomio minimo di α su K. Allora, ponendo $\sigma(\alpha) = \alpha'$, con α'* una radice di p_α, *posso estendere univocamente tale definizione ad un ben definito $\sigma \in \mathrm{Gal}(K(\alpha)|K)$.*

Dimostrazione. Anche potrebbe non sembrare, si tratta di un'applicazione del teorema di omomorfismo! □

Polinomi ciclotomici

Nel "bagaglio di risultati noti" che è bene portare con sé, vale la pena di ricordare i *polinomi ciclotomici*. Per semplicità, lavoriamo sul campo $\mathbb{Q}$ dei razionali. Per definizione, l'n-esimo polinomio ciclotomico è il polinomio le cui radici sono esattamente le radici *primitive* n-esime dell'unità:

$$\Phi_n(X) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(X - \exp\left(2\pi i \frac{k}{n} \right) \right). \tag{3.4}$$

Si dimostra che $\Phi_n(X)$ è un polinomio *a coefficienti interi, monico, irriducibile*. Un campo di spezzamento di $\Phi_n(X)$ su $\mathbb{Q}$ è dato da $\mathbb{Q}(\omega_n)$, ove ω_n è una radice primitiva n-esima dell'unità (per esempio, $e^{\frac{2\pi i}{n}}$); il gruppo di Galois $\mathrm{Gal}(\mathbb{Q}(\omega_n)|\mathbb{Q})$ è isomorfo al gruppo moltiplicativo $\mathbb{Z}_n^*$ degli interi modulo n. Può essere utile ricordare i polinomi ciclotomici Φ_n per n piccolo oppure "facile", tipo $n = p$ (un numero primo), oppure $n = p^k$ (la potenza di un primo).

Gruppi: generatori e relazioni

Spesso conviene scrivere un gruppo tramite *generatori e relazioni*. Non entriamo nel dettaglio della definizione formale, e ci accontentiamo di capire il senso di ciò direttamente dagli esempi. Consideriamo un gruppo G ciclico infinito, dunque isomorfo a $\mathbb{Z}$. Siamo soliti scrivere:

$$G = \langle g \rangle,$$

dove g è un generatore. Ci accorgiamo che G *non ha relazioni non banali*, dove le "relazioni banali" sono quelle date dall'esistenza del neutro ($g \cdot e = g$) e degli inversi ($gg^{-1} = e$): un qualsiasi elemento di G si scrive come g^n per un qualche $n \in \mathbb{Z}$. Questo è il più semplice esempio di *gruppo libero*. Esistono gruppi liberi con un numero arbitrario di generatori. Ad esempio, il gruppo libero su due generatori g_1 e g_2 si realizza tramite stringhe finite in cui compaiono g_1, g_2 oppure i loro inversi, tipo $g_1 g_2 g_1^{-1} g_2^4$.

In generale, comunque, un gruppo non sarà libero, ma avrà anche "relazioni non banali". Ad esempio, un gruppo ciclico finito C_n ha un generatore x e la relazione non banale $x^n = 1$. Sinteticamente, si scrive:

$$C_n = \langle x \mid x^n = 1 \rangle.$$

Di fatto, questa scrittura *caratterizza* C_n. L'idea è quella di prendere gli elementi del gruppo libero generato da x, che sono tutte le potenze intere di x e sostituire $x^n = 1$ ogni volta che compare. Ciò forse è più chiaro considerando un tipico esempio di gruppo con due generatori, ossia il diedrale:

$$D_n = \langle \sigma, \rho \mid \sigma^2 = 1, \rho^n = 1, \sigma\rho = \rho^{-1}\sigma \rangle.$$

I suoi elementi sono dunque dati da stringhe come per esempio $\sigma\rho^5\sigma^3\rho^{-2}$, che possono essere opportunamente ridotte grazie alle relazioni che abbiamo imposto. Per esempio, in D_5 avremo

$$\sigma\rho^5\sigma^3\rho^{-2} = \sigma\sigma\rho^3 = \rho^3.$$

Un risultato semplice ma profondo afferma che *ogni gruppo si può esprimere in termini di generatori e relazioni.* In generale, però, sia i primi che le seconde potrebbero essere infinite.

3.3 Gli esercizi

Esercizio 3.4. *Sia $p(X) = X^4 - 10X^2 + 20$. Calcolare il gruppo di Galois di $p(X)$ sui razionali e descrivere esplicitamente la corrispondenza di Galois.*

Risoluzione. Osserviamo, per cominciare, che il polinomio $p(X)$ è irriducibile per il criterio di Eisenstein applicato al primo 5. Effettuiamo il cambio di variabile $Y = X^2$ e risolviamo l'equazione

$$Y^2 - 10Y + 20 = 0.$$

Si vede facilmente che le sue soluzioni sono $5 \pm \sqrt{5}$. Ora, siano $\alpha, \beta \in \mathbb{C}$ tali che

$$\alpha^2 = 5 + \sqrt{5},$$
$$\beta^2 = 5 - \sqrt{5}.$$

Allora, le radici di $p(X)$ sono $\{\pm\alpha, \pm\beta\}$. Notiamo che $(\alpha\beta)^2 = 20$, dunque possiamo supporre che

$$\alpha\beta = \sqrt{20} = 2\sqrt{5},$$

a meno di scambiare α con $-\alpha$. Dunque, le radici di $p(X)$ sono $\{\pm\alpha, \pm\frac{2\sqrt{5}}{\alpha}\}$, e un campo di spezzamento di $p(X)$ su $\mathbb{Q}$ è dato da $\mathbb{Q}(\alpha, \sqrt{5})$. Osserviamo però che

$$\sqrt{5} = \alpha^2 - 5 \in \mathbb{Q}(\alpha),$$

dunque $\mathbb{Q}(\alpha, \sqrt{5}) = \mathbb{Q}(\alpha)$. Poiché $p(X)$ è irriducibile, troviamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Ora, sia $G = \mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q})$. Sappiamo che $|G| = 4$. Un elemento $f \in G$ è determinato dal suo valore $f(\alpha)$, che a sua volta deve essere una radice di $p(X)$. Poniamo

$$f(\alpha) = \frac{2\sqrt{5}}{\alpha}.$$

Notiamo ora che

$$\begin{aligned} f(\sqrt{5}) = f(\alpha^2 - 5) &= f(\alpha)^2 - 5 \\ &= \frac{20}{\alpha^2} - 5 = \frac{20}{5 + \sqrt{5}} - 5 \\ &= \frac{20(5 - \sqrt{5})}{20} - 5 \\ &= -\sqrt{5}. \end{aligned}$$

Un calcolo diretto ci mostra che $f^2(\alpha) = f(f(\alpha)) = -\alpha$. Dunque, f non ha ordine 2 in G, e necessariamente ha ordine 4. Concludiamo che $G = \langle f \rangle \cong C_4$. L'unico sottogruppo non banale di G è quello generato da f^2. Notiamo subito che $f^2(\sqrt{5}) = \sqrt{5}$, e deduciamo così che il campo fisso del sottogruppo $\langle f^2 \rangle$ è $\mathbb{Q}(\sqrt{5})$. □

Esercizio 3.5. *Si determini il gruppo di Galois del polinomio $p(X) = X^4 + 4X^2 - 2$ sui razionali.*

Soluzione. Per cominciare, osserviamo che $p(X)$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein applicato al primo 2. Effettuiamo il cambio variabile $Y = X^2$ e risolviamo l'equazione quadratica

$$Y^2 + 4Y - 2 = 0,$$

trovando le soluzioni

$$Y_{1,2} = -2 \pm \sqrt{6}.$$

Siano $\alpha, \beta \in \mathbb{C}$ tali che

$$\begin{aligned} \alpha^2 &= -2 + \sqrt{6}, \\ \beta^2 &= -2 - \sqrt{6}. \end{aligned}$$

Troviamo che $(\alpha\beta)^2 = -2$. Notiamo che $-2 + \sqrt{6} > 0$. Possiamo scegliere $\alpha \in \mathbb{R}$ tale che

$$\alpha\beta = i\sqrt{2}.$$

Allora, le radici di $p(X)$ sono date da $\{\pm\alpha, \pm\frac{i\sqrt{2}}{\alpha}\}$, e un campo di spezzamento è dato da $\mathbb{Q}(\alpha, i\sqrt{2})$. Abbiamo:

$$[\mathbb{Q}(\alpha, i\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\alpha, i\sqrt{2}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Sia $G = \mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$. Cerchiamo di fabbricare elementi di G definendoli sui generatori α e $i\sqrt{2}$. Ponendo:

$$\rho : \begin{cases} \alpha & \mapsto \frac{i\sqrt{2}}{\alpha}, \\ i\sqrt{2} & \mapsto -i\sqrt{2} \end{cases},$$

troviamo un ben definito elemento di G, tale che $\rho^4 = 1$. Poniamo poi

$$\sigma : \begin{cases} \alpha & \mapsto \alpha, \\ i\sqrt{2} & \mapsto -i\sqrt{2} \end{cases}.$$

Abbiamo che $\sigma^2 = 1$. Inoltre, con un calcolo diretto otteniamo la relazione

$$\sigma\rho = \rho^3\sigma.$$

Questo ci assicura che il gruppo G è isomorfo al gruppo diedrale D_4. □

4 Esercizi riassuntivi (27/05/2015)

Esercizio 4.1. *Sia $p(X) = X^8 + 3X^6 + X^5 + 3X^3 + X^2 + 3 \in \mathbb{Q}[X]$. Calcolare il gruppo di Galois di $p(X)$ su $\mathbb{Q}$ e descrivere esplicitamente la corrispondenza di Galois.*

Risoluzione. Abbiamo:

$$\begin{aligned} p(X) &= X^2(X^6 + X^3 + 1) + 3(X^6 + X^3 + 1) \\ &= (X^2 + 3)(X^6 + X^3 + 1). \end{aligned}$$

Notiamo che $X^6 + X^3 + 1 = \Phi_9(X)$, il nono polinomio ciclotomico. Sia ζ una radice nona primitiva dell'unità (prendiamo, per fissare le cose, $\zeta = \exp(\frac{2\pi i}{9})$). Un campo di spezzamento di $p(X)$ su $\mathbb{Q}$ è dato da $\mathbb{Q}(i\sqrt{3}, \zeta)$. Osserviamo che

$$\begin{aligned} \zeta^3 &= \exp\left(\frac{2\pi i}{3}\right) = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) \\ &= \frac{1}{2} + i\frac{\sqrt{3}}{2}. \end{aligned}$$

Dunque, $i\sqrt{3} \in \mathbb{Q}(\zeta)$, e $\mathbb{Q}(i\sqrt{3}, \zeta) = \mathbb{Q}(\zeta)$. È noto che $G = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong \mathbb{Z}_9^*$, ed è un gruppo ciclico di ordine 6, in particolare è risolubile. Un generatore è dato dall'automorfismo α tale che $\alpha(\zeta) = \zeta^2$.

G ha un sottogruppo H di ordine 3 (indice 2), $H = \langle \alpha^2 \rangle$, e un sottogruppo di ordine 2 (indice 3), $K = \langle \alpha^3 \rangle$. A H corrisponde un'estensione quadratica su $\mathbb{Q}$, che è sicuramente $\mathbb{Q}(i\sqrt{3})$. Di seguito, determiniamo l'estensione (di grado 3) corrispondente a K. α^3 ha ordine 2 in G, dunque

$$\alpha^3(\zeta + \alpha^3(\zeta)) = \zeta + \alpha^3(\zeta) = \zeta + \zeta^{-1} = e^{\frac{2\pi i}{9}} + e^{-\frac{2\pi i}{9}} = 2\cos\frac{2\pi}{9}$$

è un elemento lasciato fisso da α^3. Ora, osserviamo che

$$\begin{aligned} &\zeta^6 + \zeta^3 + 1 = 0 \\ &\Rightarrow \zeta^3 + \zeta^{-3} + 1 = 0, \end{aligned}$$

inoltre $(\zeta + \zeta^{-1})^3 = \zeta^3 + \zeta^{-3} + 3\zeta + 3\zeta^{-1}$, e dunque

$$0 = \zeta^3 + \zeta^{-3} + 1 = (\zeta + \zeta^{-1})^3 - 3(\zeta + \zeta^{-1}) + 1.$$

In altre parole, $\zeta + \zeta^{-1}$ è radice di $X^3 - 3X + 1$, che è un polinomio irriducibile su $\mathbb{Q}$. Concludiamo che $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{9})$ è l'estensione di grado 3 corrispondente a K. □

Esercizio 4.2. *Dimostrare che, a meno di isomorfismo, esiste un unico gruppo non abeliano G di ordine $5^2 11^2$ con sottogruppi di Sylow ciclici.*

Risoluzione. Sia G come da ipotesi. Al solito, n_p denota la cardinalità dei p-Sylow di G. Sappiamo che $n_{11} \mid 25$ e $n_{11} \equiv 1 \pmod{11}$. Dunque, necessariamente $n_{11} = 1$. Sia K l'11-Sylow, che è normale in G, e sia H un 5-Sylow. Allora, sappiamo che

$$G \cong K \rtimes_\varphi H,$$

per un qualche $\varphi\colon H \to \mathrm{Aut}(K)$. Bisogna capire quali possibilità vi sono per φ. Per ipotesi, H e K sono gruppi ciclici. Dunque, $H \cong \mathbb{Z}_{25}$ e $\mathrm{Aut}(K) \cong (\mathbb{Z}_{121})^*$. Poiché 11 è un primo dispari, il gruppo moltiplicativo di $\mathbb{Z}_{121}$ è ciclico di ordine $11^2 - 11 = 110 = 11 \cdot 2 \cdot 5$, e in definitiva $\mathrm{Aut}(K) \cong \mathbb{Z}_{110}$.

Ora, sia g un generatore di $H \cong \mathbb{Z}_{25}$. Allora, $\varphi(g)$ ha ordine che divide l'ordine di g, cioè $\mathrm{ord}\,\varphi(g) \mid 25$. Dunque, a priori, abbiamo che $\mathrm{ord}\,\varphi(g) \in \{1, 5, 25\}$. Se tale ordine è 1, allora G è abeliano, caso che abbiamo escluso; $\mathrm{ord}\,\varphi(g) = 25$ porta ad una contraddizione, poiché $25 \nmid 110$. Concludiamo che necessariamente $\mathrm{ord}\,\varphi(g) = 5$. Gli elementi di ordine 5 di $\mathrm{Aut}(K) \cong \mathbb{Z}_{110}$ sono quattro, e tutti appartenenti al suo unico sottogruppo di ordine 5: più precisamente, essi sono $\varphi(g), \varphi(g)^2, \varphi(g)^3, \varphi(g)^4$. Finalmente, possiamo controllare che l'omomorfismo φ è essenzialmente unico, cosicché $K \rtimes_\varphi H$ sia univocamente determinato a meno di isomorfismo. Sia $\varphi'\colon H \to \mathrm{Aut}(K)$ un

altro qualsiasi omomorfismo. Sappiamo che $\varphi'(g)$ ha ordine 5, dunque $\varphi'(g) = \varphi(g^i)$ per un qualche $i \in \{1,2,3,4\}$. D'altra parte, se g è un generatore di H, anche g^i (con $i \in \{1,2,3,4\}$) lo è. Sia $\psi_i \colon H \xrightarrow{\sim} H$ l'automorfismo di H che manda g in g^i. Troviamo un diagramma commutativo:

$$\begin{array}{ccc} H & \xrightarrow{\varphi'} & \mathrm{Aut}(K) \\ {\scriptstyle \psi_i}\downarrow & \nearrow_{\varphi} & \\ H. & & \end{array}$$

Questo ci basta per affermare che $K \rtimes_{\varphi} H \cong K \rtimes_{\varphi'} H$ (perché? esercizio). Per l'arbitrarietà di φ', concludiamo. □

Esercizio 4.3. *Sia $p(X) = X^6 - 3X^4 + 3X^2 - 2 \in \mathbb{Q}[X]$. Determinare il gruppo di Galois di $p(X)$ sui razionali.*

Risoluzione. Scriviamo

$$\begin{aligned} p(X) &= X^6 - X^4 + X^2 - 2X^4 + 2X^2 - 2 \\ &= (X^2 - 2)(X^4 - X^2 + 1). \end{aligned}$$

Notiamo che $X^4 - X^2 + 1 = \Phi_{12}(X)$, il 12° polinomio ciclotomico. Sia

$$\zeta = e^{\frac{i\pi}{6}} = \frac{\sqrt{3}}{2} + \frac{i}{2}.$$

ζ è una radice dodicesima primitiva dell'unità. Osserviamo che $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{3} + i) = \mathbb{Q}(\sqrt{3}, i)$. Infatti, $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\sqrt{3}, i)$ ed entrambe le estensioni hanno grado 4 su $\mathbb{Q}$. Dunque, un campo di spezzamento di $p(X)$ su $\mathbb{Q}$ è dato da $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$. Inoltre,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8,$$

poiché $i \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

Notiamo che $K_1 = \mathbb{Q}(\sqrt{2}), K_2 = \mathbb{Q}(\sqrt{3}), K_3 = \mathbb{Q}(i)$ sono estensioni normali (quadratiche) di $\mathbb{Q}$. Allora, sono ben definiti gli omomorfismi di restrizione:

$$\mathrm{res}_i : \mathrm{Gal}(K|\mathbb{Q}) \to \mathrm{Gal}(K_i|\mathbb{Q}).$$

Prendendo il loro prodotto diretto, otteniamo un omomorfismo

$$F = (\mathrm{res}_1, \mathrm{res}_2, \mathrm{res}_3) : \mathrm{Gal}(K|\mathbb{Q}) \to \prod_{i=1}^{3} \mathrm{Gal}(K_i|\mathbb{Q}).$$

F è iniettivo: infatti, se $\alpha \in \ker F$, allora $\alpha_{|K_i} = \mathrm{id}$ per ogni i, ma i K_i generano K come estensione su $\mathbb{Q}$, dunque $\alpha = \mathrm{id}$. Inoltre, F è suriettivo. Infatti, sia $(\alpha_1, \alpha_2, \alpha_3) \in$

$\prod_{i=1}^{3} \mathrm{Gal}(K_i|\mathbb{Q})$; poiché $K_i \cap K_j = \mathbb{Q}$ per $i \neq j$, possiamo definire $\alpha \in \mathrm{Gal}(K|\mathbb{Q})$ semplicemente sui generatori:

$$\alpha : \begin{cases} \sqrt{2} & \mapsto \alpha_1(\sqrt{2}) \\ \sqrt{3} & \mapsto \alpha_2(\sqrt{3}) \\ i & \mapsto \alpha_3(i) \end{cases}$$

ed estenderlo univocamente su K. Tale α, per costruzione, è un elemento della controimmagine di $(\alpha_1, \alpha_2, \alpha_3)$. Concludiamo che F è un isomorfismo, e in particolare $\mathrm{Gal}(K|\mathbb{Q}) \cong C_2 \times C_2 \times C_2$. □

Esercizio 4.4. *Calcolare il gruppo di Galois di $p(X) = X^{104} - 1$ sul campo $\mathbb{F}_{13}$.*

Risoluzione. Osserviamo che $104 = 8 \cdot 13$. Grazie all'omomorfismo di Frobenius, possiamo scrivere

$$p(X) = (X^8 - 1)^{13}.$$

Dunque, ci riduciamo a cercare un campo di spezzamento di $X^8 - 1$. Esso è dato chiaramente da $\mathbb{F}_{13}[\omega]$, dove ω è una radice ottava primitiva dell'unità. Abbiamo la scomposizione ovvia

$$X^8 - 1 = (X^4 - 1)(X^4 + 1),$$

e ω è radice di $X^4 + 1$ (perché?). D'altra parte, notiamo che -1 è un residuo quadratico modulo 13: $5^2 \equiv -1 \pmod{13}$. Dunque, possiamo ulteriormente scomporre:

$$X^4 + 1 = (X^2 - 5)(X^2 + 5) = (X^2 - 5)(X^2 - 8).$$

Un calcolo diretto (basta scrivere tutti i possibili residui quadratici) mostra che né $X^2 - 5$ né $X^2 + 5$ hanno radici in $\mathbb{F}_{13}$, dunque sono irriducibili. Allora, ω è radice di uno di questi due polinomi. Si conclude che $[\mathbb{F}_{13}[\omega] : \mathbb{F}_{13}] = 2$, e il gruppo di Galois del nostro polinomio è necessariamente ciclico di ordine 2. □

5 Esercizi su teoria di Galois e campi finiti (4/6/2015)

Esercizio 5.1. *Sia $P(X) = X^4 + 1$. Dimostrare che $P(X)$ è irriducibile su $\mathbb{Z}$, ma riducibile su $\mathbb{F}_p$ per ogni primo p.*

Risoluzione. Sappiamo che $P(X)$ è irriducibile su $\mathbb{Z}$ se e solo se $P(X + 1)$ lo è. D'altra parte

$$\begin{aligned} P(X + 1) &= (X + 1)^4 + 1 \\ &= X^4 + 4X^3 + 6X^2 + 4X + 2, \end{aligned}$$

dunque possiamo applicare il criterio di Eisenstein rispetto al primo 2 e concludere con l'irriducibilità in $\mathbb{Z}[X]$.

Vediamo ora la riducibilità su $\mathbb{F}_p$. Se $p = 2$, troviamo immediatamente

$$P(X) = X^4 + 1 = (X+1)^4.$$

Sia dunque p un qualunque primo dispari. Osserviamo che

$$p^2 \equiv 1 \pmod 8.$$

Infatti, siccome p è dispari, allora è congruo a $1, 3, 5$ oppure 7 modulo 8, e il suo quadrato è sempre congruo a 1. Otteniamo le seguenti relazioni di divisibilità di polinomi:

$$X^4 + 1 \mid X^8 - 1 \mid X^{p^2-1} - 1 \mid X^{p^2} - X$$

Ricordiamo ora che il campo $\mathbb{F}_{p^2}$ può essere identificato alle radici di $X^{p^2} - X \in \mathbb{F}_p[X]$. Sia α una qualsiasi radice di $X^4 + 1$. Allora, essa è anche radice di $X^{p^2} - X$. Dunque, $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^2}$. Poiché il grado di $\mathbb{F}_{p^2}$ su $\mathbb{F}_p$ è 2, deduciamo che

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] \leq 2.$$

Concludiamo che $X^4 + 1$ non può essere irriducibile su $\mathbb{F}_p$. In tal caso, dovremmo avere che $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = 4$, che è una contraddizione con quanto visto. □

Esercizio 5.2. *Sia K un campo di caratteristica $p > 0$, e sia F una sua estensione di grado finito. Sia $\phi\colon F \to F$ l'omomorfismo di Frobenius. Supponiamo che $\phi^n \in \mathrm{Gal}(F|K)$ per un qualche intero positivo n.*

1. *Dimostrare che K è un campo finito e determinare il massimo numero N di elementi che può contenere.*
2. *Mostrare che $\#K = N$ se e solo se $\mathrm{Gal}(F|K) = \langle \phi^n \rangle$.*

Risoluzione. Sia $a \in K$. Poiché $\phi^n \in \mathrm{Gal}(F|K)$, abbiamo che $\phi^n(a) = a$, cioè $a^{p^n} = a$. Dunque, a è radice del polinomio $X^{p^n} - X$, ossia appartiene al campo $\mathbb{F}_{p^n}$. In altre parole, $K \subseteq \mathbb{F}_{p^n}$, e il massimo numero N dei suoi elementi è p^n.

Siccome K è finito e $F|K$ è un'estensione finita, è anche un'estensione di Galois. sia L il campo fisso di ϕ^n. Allora, L è un campo intermedio tra K e F, e dalla corrispondenza di Galois deduciamo immediatamente che $L = K$ se e solo se $\langle \phi^n \rangle = \mathrm{Gal}(F|K)$. D'altra parte, L è per definizione esattamente $\mathbb{F}_{p^n}$, e concludiamo. □

Esercizio 5.3. *Sia $P(X) = X^5 - 2 \in \mathbb{F}_p[X]$. Dire se $P(X)$ è irriducibile e calcolare il gruppo di Galois di $P(X)$ nei casi $p = 3$ e $p = 11$.*

Risoluzione. Poiché $P(X)$ è della forma $X^q - \theta$ con q primo, abbiamo che (teorema di Abel) $P(X)$ è irriducibile se e solo se non ha radici in $\mathbb{F}_p$. Distinguiamo i casi:

1. $p = 3$. Abbiamo che $X^5 - 2 = X^5 + 1$, dunque fattorizziamo:

$$X^5 + 1 = (X + 1)(X^4 - X^3 + X^2 - X + 1).$$

Il polinomio $q(X) = X^4 - X^3 + X^2 - X + 1$ non ha radici in $\mathbb{F}_3$, dunque se fosse riducibile necessariamente sarebbe un prodotto della forma

$$\begin{aligned}&(X^2 + aX + b)(X^2 + cX + d)\\ &\quad = X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd.\end{aligned}$$

A questo punto, si tratta di vedere se il sistema

$$\begin{cases} a + c = -1 \\ b + d + ac = 1 \\ ad + bc = -1 \\ bd = 1 \end{cases}$$

ammette soluzioni oppure no. Dall'ultima equazione ricaviamo $b = d = 1$ oppure $b = d = -1$. Nel secondo caso, però, la terza equazione diventerebbe $-a - c = -1$ cioè $a + c = 1$, in contraddizione con la prima. Ci riduciamo dunque al sistema:

$$\begin{cases} b = d = 1 \\ 2 + ac = 1 \\ a + c = -1. \end{cases}$$

Troviamo allora $ac = -1$, insieme con $a + c = 1$. La prima identità ci dice che a e c sono opposti, ma ciò è in contraddizione con la seconda identità. Concludiamo che $q(X)$ è irriducibile.

Ora, il gruppo di Galois di $P(X)$ coincide con quello di $q(X)$. Sia α una radice di $q(X)$. Poiché le estensioni finite di campi finiti sono normali, abbiamo che $\mathbb{F}_3(\alpha)$ è un campo di spezzamento di $q(X)$ su $\mathbb{F}_3$. L'estensione ha grado 4, e dalla teoria sappiamo che il gruppo di Galois $\mathrm{Gal}(\mathbb{F}_3(\alpha)|\mathbb{F}_3)$ è ciclico (di ordine 4, giustappunto), generato dall'omomorfismo di Frobenius.

2. $p = 11$. Un calcolo diretto mostra che 2 non è la quinta potenza di un qualche elemento di $\mathbb{F}_{11}$. Dunque, $P(X)$ è irriducibile su $\mathbb{F}_{11}$. Per calcolare il gruppo di Galois di $P(X)$, basta ragionare come nel punto precedente: troviamo un gruppo ciclico di ordine 5, generato dall'omomorfismo di Frobenius. □

Esercizio 5.4. *Sia $P(X) = X^4 + 2X^2 + 2 \in \mathbb{F}_p[X]$. Dire se $P(X)$ è irriducibile e calcolare il gruppo di Galois di $P(X)$ nei casi $p = 3$ e $p = 7$.*

Risoluzione. Si tratta di un polinomio biquadratico, dunque per prima cosa studiamo il polinomio $Y^2 + 2Y + 2$ ottenuto con il cambio variabile $Y = X^2$. Il suo discriminante è $4 - 8 = -2^2$. Dunque, tale polinomio ha radici in $\mathbb{F}_p$ se e solo se -1 è un quadrato in $\mathbb{F}_p$. Un'ispezione diretta ci dice che ciò non è vero in nessuno dei casi $p = 3$ e $p = 7$. Del resto, se $P(X)$ avesse radici in $\mathbb{F}_p$, lo stesso sarebbe vero per $Y^2 + 2Y + 2$, dunque $P(X)$ non ha radici in $\mathbb{F}_p$. Inoltre, non può esistere una fattorizzazione di $P(X)$ della forma

$$(X^2 - h)(X^2 - k).$$

Dunque, vediamo se possiamo trovare una fattorizzazione del tipo

$$\begin{aligned} P(X) &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd. \end{aligned}$$

con $a \neq 0$. Abbiamo il sistema:

$$\begin{cases} a + c = 0 \\ b + d + ac = 2 \\ ad + bc = 0 \\ bd = 2 \end{cases}$$

Dalla prima equazione troviamo $a = -c$, da cui poi $ad - ab = 0$; poiché $a \neq 0$, abbiamo $d = b$. La quarta equazione dunque diventa $b^2 = 2$, e ciò è una contraddizione in $\mathbb{F}_3$, da cui deduciamo che $P(X)$ è irriducibile su $\mathbb{F}_3$. Se invece $p = 7$, abbiamo che $2 = 3^2 = (-3)^2$. Se prendiamo $b = -3$, dalla seconda equazione troviamo $a^2 = -1$, che non è possibile. Invece, prendendo $b = 3$, troviamo $a^2 = 4$, da cui $a = \pm 2$. In definitiva in $\mathbb{F}_7$ troviamo la fattorizzazione

$$P(X) = (X^2 - 2X + 3)(X^2 + 2X + 3).$$

Notiamo che questi due fattori sono irriducibili (basta calcolare i discriminanti, che in entrambi i casi fanno -1).

A questo punto, calcoliamo i gruppi di Galois. Se $p = 3$, un campo di spezzamento di $P(X)$ è dato da $\mathbb{F}_3(\alpha)$, dove α è una radice di $P(X)$. Il grado dell'estensione è 4, e il gruppo di Galois è ciclico di ordine 4, generato dall'omomorfismo di Frobenius. Se invece $p = 7$, per spezzare completamente $P(X)$ basta aggiungere una radice quadrata β di -1. Un campo di spezzamento è dato da $\mathbb{F}_7(\beta)$, e il gruppo di Galois è ciclico di ordine 2. □

Esercizio 5.5. *Sia $P(X) = X^3 + X + 1 \in \mathbb{F}_5[X]$. Dimostrare che $P(X)$ è irriducibile e calcolare il suo gruppo di Galois.*

Risoluzione. Lasciata al lettore! □

Esercizio 5.6. *Sia* $P(X) = X^3 - 2 \in \mathbb{F}_p[X]$. *Determinare il gruppo di Galois di* $P(X)$ *per* $p = 5$ *e* $p = 7$.

Risoluzione. Lasciata al lettore! □