

Svolgimento Appello di Algebra 2 del 16 luglio 2014.

1 Esercizio 1

Sia $f(x)$ un polinomio a coefficienti in un campo F ; provare che $f(x)$ ha radici multiple (in un opportuno campo di spezzamento) se e solo se $(f(x), f'(x)) \neq 1$.

Svolgimento. Supponiamo che $f(x)$ abbia radici multiple in un campo di spezzamento E . Allora per il teorema di Ruffini esistono un certo elemento $a \in E$ e $g(x) \in E[X]$ tali che $f(x) = (x-a)^2 g(x)$. Derivando abbiamo $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x)$. Sostituendo $x = a$ troviamo $f'(a) = 0$ per cui, ancora per il teorema di Ruffini, $x-a$ divide $f'(x)$. Quindi $x-a$ divide sia $f(x)$ che $f'(x)$ e quindi divide il massimo comun divisore tra $f(x)$ e $f'(x)$, che quindi è diverso da 1.

Supponiamo ora che il massimo comun divisore tra $f(x)$ e $f'(x)$ sia diverso da 1. Detto $m(x)$ tale massimo comun divisore, si ha allora che $m(x)$ è un polinomio di grado positivo. Esiste quindi $a \in E$, con E campo di spezzamento di $m(x)$ su F , con $m(a) = 0$ per cui siccome $m(x)$ divide $f(x)$ e $f'(x)$ anche $f(a) = 0$ e $f'(a) = 0$. Da $f(a) = 0$ e dal teorema di Ruffini troviamo $g(x) \in E[X]$ con $f(x) = (x-a)g(x)$. Si ha quindi $f'(x) = g(x) + (x-a)g'(x)$ per cui $f'(a) = g(a)$. Ma sappiamo che $f'(a) = 0$ per cui $g(a) = 0$, cioè esiste $h(x) \in E[X]$ con $g(x) = (x-a)h(x)$ per cui $f(x) = (x-a)g(x) = (x-a)^2 h(x)$ quindi a è una radice multipla di $f(x)$.

2 Esercizio 2

Sia G un gruppo finito, p un primo e sia N un sottogruppo normale di G tale che p non divide $|G : N|$. Si provi che ogni p -sottogruppo di Sylow di G è contenuto in N .

Svolgimento. Cominciamo col mostrare che N contiene un sottogruppo di Sylow di G . Sia P un p -sottogruppo di Sylow di N , diciamo $|N| = |P|m$ con p che non divide m . Detto $n = |G : N|$ si ha allora $|G| = |G : N||N| = |P|mn$, e siccome p non divide né m né n , p non divide mn , per cui $|P|$ è anche l'ordine di un p -sottogruppo di Sylow di G . Ne segue, per definizione di sottogruppo di Sylow, che P è anche un p -sottogruppo di Sylow di G .

Ora mostriamo che ogni altro p -sottogruppo di Sylow di G è contenuto in N . Sia Q un p -sottogruppo di Sylow di G . Per il teorema di Sylow P e Q sono coniugati in G , cioè esiste $g \in G$ con $gPg^{-1} = Q$. Ma allora siccome $P \subseteq N$ e N è normale abbiamo $Q = gPg^{-1} \subseteq gNg^{-1} = N$, per cui anche Q è contenuto in N .

3 Esercizio 3

Sia $\sigma = (1, 2, 3, 4)(5, 6, 7)(8, 9)$.

1. Determinare il numero di coniugati di $\sigma \in S_9$.
2. Determinare il centralizzante di σ in S_9 .
3. Elencare i sottogruppi di $\langle \sigma \rangle$, determinando un generatore per ognuno di essi.

Svolgimento. Punto (1). Il numero di coniugati di σ in S_9 è il numero di elementi di S_9 con la stessa struttura ciclica di σ . Ci sono $\binom{9}{4}$ scelte per l'insieme degli elementi mossi dal 4-ciclo, $\binom{5}{3}$ scelte per l'insieme degli elementi mossi dal 3-ciclo e una sola scelta per l'insieme degli elementi mossi dal 2-ciclo, e ci sono $3!$ scelte per un 4-ciclo che muove quattro dati elementi e $2!$ scelte per un 3-ciclo che muove tre dati elementi (ogni volta fisso un elemento del ciclo e permuta gli altri in tutti i modi possibili), per cui il numero di coniugati di σ in S_9 è $\binom{9}{4} 3! \binom{5}{3} 2! = \frac{9! 3! 5! 2!}{4! 3! 2!} = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$.

Punto (2). Siccome σ ha $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ coniugati, per l'equazione delle classi il centralizzante di σ in S_9 ha ordine $\frac{9!}{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5} = 4! = 24$. Siccome σ ha ordine $4 \cdot 3 = 12$ e $\langle \sigma \rangle$ è contenuto in $C_{S_9}(\sigma)$, $\langle \sigma \rangle$ è un sottogruppo di $C_{S_9}(\sigma)$ di indice 2. Ora certamente i cicli che compaiono nella struttura ciclica di σ centralizzano σ (cicli disgiunti commutano), quindi $H = \langle (1, 2, 3, 4), (5, 6, 7)(8, 9) \rangle$ è contenuto in $C_{S_9}(\sigma)$. Per mostrare che $C_{S_9}(\sigma) = H$ ci resta da mostrare che $|H| = 24$. Siccome H contiene $(1, 2, 3, 4)(5, 6, 7)$, che ha ordine 12, e $|H|$ divide $|C_{S_9}(\sigma)| = 24$ (per il teorema di Lagrange), e $\langle (1, 2, 3, 4)(5, 6, 7) \rangle$ non contiene $(8, 9)$, segue che $|H|$ divide 24 ed è diviso da 12 e diverso da 12, quindi $|H| = 24$. Concludiamo che $C_{S_9}(\sigma) = \langle (1, 2, 3, 4), (5, 6, 7), (8, 9) \rangle$.

Punto (3). I sottogruppi del gruppo ciclico $\langle \sigma \rangle$ sono tanti quanti i divisori di $|\langle \sigma \rangle| = 12$, esplicitamente si tratta di $\langle 1 \rangle$, $\langle \sigma \rangle$, $\langle \sigma^2 \rangle$, $\langle \sigma^3 \rangle$, $\langle \sigma^4 \rangle$, $\langle \sigma^6 \rangle$. I loro generatori sono 1 , $\sigma = (1, 2, 3, 4)(5, 6, 7)(8, 9)$, $\sigma^2 = (1, 3)(2, 4)(5, 7, 6)$, $\sigma^3 = (1, 4, 3, 2)(8, 9)$, $\sigma^4 = (5, 6, 7)$, $\sigma^6 = (1, 3)(2, 4)$.

4 Esercizio 4

Sia G un gruppo di ordine 3000.

1. Sia $n_5(G)$ il numero dei 5-sottogruppi di Sylow di G . Si provi che $n_5(G) \in \{1, 6\}$.
2. Dedurre che se il 5-sottogruppo di Sylow di G non è normale in G allora esiste un omomorfismo non banale $\phi : G \rightarrow S_6$.
3. Concluderne che G possiede almeno un sottogruppo normale proprio non banale.

Svolgimento. Punto (1). Si ha $3000 = 2^3 \cdot 3 \cdot 5^3$. Per il teorema di Sylow $n_5(G)$ divide $2^3 \cdot 3 = 24$ ed è congruo a 1 modulo 5, e gli unici divisori di 24 che sono congrui a 1 modulo 5 sono 1 e 6.

Punto (2). Supponiamo che i 5-sottogruppi di Sylow di G non siano normali in G . In altre parole $n_5(G) \neq 1$ (infatti per il teorema di Sylow, tutti i p -sottogruppi di Sylow sono coniugati, quindi dire che sono normali è come dire che ce n'è solo uno). Ma allora dal punto (1) segue $n_5(G) = 6$. Sia $\mathcal{P}$ l'insieme dei 5-sottogruppi di Sylow di $|G|$. Si ha $|\mathcal{P}| = n_5(G) = 6$. Per il teorema di Sylow, l'azione di coniugio di G su $\mathcal{P}$ è transitiva (in altre parole, i 5-sottogruppi di Sylow sono tutti coniugati), in particolare è non banale (non fissa tutto), quindi l'omomorfismo associato $G \rightarrow \text{Sym}(6)$ è non banale (non manda tutto in 1).

Punto (3). Se $n_5(G) = 1$ allora il 5-sottogruppo di Sylow è un sottogruppo normale proprio non banale di G . Supponiamo ora che sia $n_5(G) \neq 1$. Allora per il punto (2) esiste un omomorfismo non banale $\varphi : G \rightarrow \text{Sym}(6)$, il cui nucleo, chiamiamolo N , è quindi un sottogruppo normale di G e

$N \neq G$ (essendo φ non banale) per cui per concludere che N è un sottogruppo proprio non banale di G basta mostrare che $N \neq \{1\}$. Supponiamo per assurdo che sia $N = \{1\}$. Allora φ è iniettiva, quindi $\varphi(G)$ è un sottogruppo di $\text{Sym}(6)$ isomorfo a G . In particolare dal teorema di Lagrange $|G| = 3000$ divide $|\text{Sym}(6)| = 6!$ e questo è assurdo: $3000 = 2^3 \cdot 3 \cdot 5^3$ non divide $6! = 2^4 \cdot 3^2 \cdot 5$.

5 Esercizio 5

Sia $u = i\sqrt{2\sqrt{3}-3}$.

1. Determinare il polinomio minimo $f(x)$ di u su $\mathbb{Q}$.
2. E' vero che $f(x)$ ha radici reali?
3. Sia E il campo di spezzamento di $f(x)$ su $\mathbb{Q}$. Determinare $|E : \mathbb{Q}|$.
4. E' vero che E contiene i ?

Svolgimento. Punto (1). Si ha $u^2 = -(2\sqrt{3}-3)$ da cui $(u^2-3)^2 = 4 \cdot 3 = 12$. Ne segue che u è zero di $f(x) = x^4 - 6x^2 - 3$. Per il criterio di Eisenstein applicato al primo 3, $f(x)$ è irriducibile in $\mathbb{Q}[X]$, quindi essendo monico con u come zero è proprio il polinomio minimo di u su $\mathbb{Q}$.

Punto (2). $f(x) = 0$ si riscrive, come visto sopra, come $(x^2-3)^2 = 12$ cioè $x^2-3 = \pm\sqrt{12}$. Scegliendo il segno $+$ otteniamo che $v = \sqrt{3+\sqrt{12}}$ è una radice di $f(x)$, ed è reale. Quindi la risposta è sì, $f(x)$ ha radici reali.

Punto (3). Sappiamo che $u = i\sqrt{2\sqrt{3}-3}$ e $v = \sqrt{3+\sqrt{12}}$ sono radici di $f(x)$. In particolare, siccome $f(x)$ è irriducibile su $\mathbb{Q}$, u e v hanno grado 4 su $\mathbb{Q}$. Inoltre le quattro radici di $f(x)$ sono $u, -u, v, -v$ quindi il campo di spezzamento di $f(x)$ in $\mathbb{C}$ è $\mathbb{Q}(u, v)$. D'altra parte siccome v è reale, $\mathbb{Q}(v) \subseteq \mathbb{R}$ e $u \notin \mathbb{R}$, quindi il grado $|\mathbb{Q}(u, v) : \mathbb{Q}(v)|$ è maggiore di 1. Per la formula dei gradi $|E : \mathbb{Q}| = |E : \mathbb{Q}(v)| \cdot |\mathbb{Q}(v) : \mathbb{Q}| = |E : \mathbb{Q}(v)| \cdot 4$. Siamo ridotti a calcolare $|E : \mathbb{Q}(v)|$. Siccome $E = \mathbb{Q}(u, v) = \mathbb{Q}(v)(u)$, questo numero è uguale al grado del polinomio minimo di u su $\mathbb{Q}(v)$. Ma $u^2 = 3 - 2\sqrt{3} = -v^2 + 6$ quindi u è zero di $x^2 + v^2 - 6 \in \mathbb{Q}(v)[x]$, per cui u ha grado 2 su $\mathbb{Q}(v)$. Ne segue che $|E : \mathbb{Q}| = 2 \cdot 4 = 8$.

Punto (4). Si ha

$$uv = i\sqrt{\sqrt{12}-3}\sqrt{\sqrt{12}+3} = i\sqrt{12-9} = i\sqrt{3} = i\frac{1}{2}(v^2-3)$$

per cui $i = \frac{2uv}{v^2-3} \in E$.

6 Esercizio 6

Sia $F = \mathbb{Z}/2\mathbb{Z}$ e si consideri il polinomio $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1 \in F[X]$. Sia inoltre E un campo di spezzamento di $f(x)$ su F e si consideri l'anello $A = F[x]/(f(x))$.

1. Fattorizzare $f(x)$ in F .
2. Determinare il numero di ideali dell'anello A .
3. Quanti sono gli ideali massimali di A ?
4. Qual è l'ordine di E ?

Svolgimento. Punto (1). Ricordando la fattorizzazione di $x^6 - 1$ in polinomi ciclotomici, $x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$ e ricordando che siamo in caratteristica 2 otteniamo $f(x) = \frac{x^6 - 1}{x - 1} = (x + 1)(x^2 - x + 1)(x^2 + x + 1) = (x + 1)(x^2 + x + 1)^2$.

Punto (2). Siccome $F[x]$ è un PID, per il teorema di corrispondenza per gli ideali un ideale di A ha la forma $(g(x))/(f(x))$ con $g(x)$ divisore di $f(x)$ in $F[x]$. Quindi il numero degli ideali di A è uguale al numero di divisori di $f(x) = (x + 1)(x^2 + x + 1)^2$ in $F[x]$, cioè 6 ($x + 1$ appare zero volte oppure una, e $x^2 + x + 1$ appare zero, una oppure due volte, quindi in totale ho $2 \cdot 3$ modi di produrre un divisore).

Punto (3). Siccome $F[x]$ è un PID, per il teorema di corrispondenza per gli ideali un ideale massimale di A ha la forma $(g(x))/(f(x))$ con $g(x)$ divisore *irriducibile* di $f(x)$, per cui A ha due ideali massimali (i divisori irriducibili di $f(x)$ in $F[x]$ sono $x + 1$ e $x^2 + x + 1$).

Punto (4). E è generato dagli zeri di $f(x) = (x + 1)(x^2 + x + 1)^2$. Detta a una radice di $x^2 + x + 1$ in E abbiamo $x^2 + x + 1 = (x - a)(x - a - 1)$ e otteniamo quindi che $E = F(a)$. Siccome a ha grado 2 su F otteniamo $|E| = 2^2 = 4$.