Algebra 1

Prof. A. D'Andrea, A. De Sole, G. Mondello

Prova scritta del 14-6-2022

Nome e Cognome: _____

Numero di Matricola: _____

Docente: **D'Andrea \ De Sole - Mondello** (cerchiare il/i docente/i).

Esercizio	Punti totali	Punteggio
1	6	
2	6	
3	6	
4	6	
5	6	
Totale	30	

Esercizio 1. Sia $G = \mathbb{F}_{17}\backslash\{0\}$ il gruppo moltiplicativo degli elementi non nulli nel campo $\mathbb{F}_{17}$.

(a) Trovare un generatore x di G.

(b) Sia $\phi : G \to G'$ un omomorfismo non banale da G ad un gruppo G' di ordine 6. Quali possono essere il nucleo e l'immagine di ϕ?

Soluzione:

(a) Il gruppo moltiplicativo $\mathbb{F}_{17}^{\times}$ ha ordine 16: dobbiamo quindi trovare un elemento di ordine moltiplicativo 16. La cosa più immediata è provare un po' a caso. Dopo aver verificato che 1 è l'identità e ha quindi ordine 1, mentre 2 ha ordine 8, si vede facilmente che

$$3^2 = 9, \qquad 3^4 = 13, \qquad 3^8 = 16, \qquad 3^{16} = 1.$$

Pertanto 3 ha ordine che divide 16, ma non è $1, 2, 4, 8$. In altre parole, 3 ha ordine 16.

Per la cronaca, un gruppo ciclico di ordine 16 possiede $\varphi(16) = 8$ generatori ciclici distinti. Gli altri sono 3^i dove i è primo con 16, cioè dispari. Se fate i conti, ottenete $3, 5, 6, 7, 10, 11, 12, 14$. Ciascuno di questi elementi costituisce una risposta corretta all'esercizio.

(b) G è un gruppo ciclico di ordine 16, e l'immagine di ϕ è isomorfa ad un suo quoziente, il cui ordine deve dividere 16. D'altro canto, l'immagine di ϕ è anche un sottogruppo di G' e deve avere ordine che divide 6. Possiamo allora concludere che l'ordine dell'immagine di ϕ deve dividere $MCD(16, 6) = 2$. L'immagine di un omomorfismo $\phi : G \to G'$ possiede quindi un solo elemento oppure due.

Nel primo caso, ϕ manda ogni elemento nell'identità ed è l'omomorfismo banale. Nel secondo caso, che ci interessa, l'immagine è un sottogruppo di ordine 2 di G' (ne esistono sicuramente, ad esempio per il Teorema di Sylow) e il nucleo è un sottogruppo di indice 2 di G. Ad ogni modo, un gruppo ciclico di ordine 16 possiede un solo sottogruppo di ordine 8; nel nostro caso, è dato dalle potenze con esponente pari di un generatore ciclico o più esplicitamente dal sottogruppo costituito dagli elementi

$$\{1, 2, 4, 8, 9, 13, 15, 16\} = (2).$$

Risposta: (a) $x =$ $\square$ (b) $\ker \phi =$ $\square$ $\operatorname{Im} \phi =$ $\square$

Esercizio 2. G è un gruppo di ordine 105.

(a) Mostrare che i 5− e i 7−Sylow di G non possono essere tutti non normali.

(b) Mostrare che G contiene elementi di ordine 35.

Soluzione:

(a) Il numero dei p-Sylow in un gruppo finito G è $\equiv 1 \mod p$ e divide $|G|$. Nel nostro caso, si conclude rapidamente che il numero dei 5−Sylow è 1 oppure 21, mentre quello dei 7-Sylow è 1 oppure 15. Come abbiamo visto più volte a lezione, due sottogruppi distinti di ordine 5 (rispettivamente 7) si intersecano nella sola identità e ogni elemento di ordine 5 (risp. 7) genera un sottogruppo di ordine 5. Pertanto gli elementi di ordine 5 (risp. 7) sono tutti e soli quelli contenuti in qualche 5-Sylow (risp. 7-Sylow) con l'esclusione dell'identità.

Se né i 5−, né i 7−Sylow, che in questo caso sono sicuramente ciclici, sono normali, avremo quindi $21 \cdot (5-1) = 84$ elementi di ordine 5 e $15 \cdot (7-1) = 90$ elementi di ordine 7 in un gruppo il cui ordine è $105 < 84 + 90$, da cui un assurdo.

(b) Se P è un 5-Sylow e Q è un 7-Sylow di G, allora il prodotto PQ è sicuramente un sottogruppo, poiché almeno uno tra P e Q è normale. Il sottogruppo PQ ha ordine $35 = 5 \cdot 7$ e abbiamo visto a lezione che ogni gruppo di ordine 35 è ciclico, in quanto gruppo di ordine pq, con $p < q$ primi tali che p non divida $q - 1$. In conclusione, PQ contiene elementi di ordine 35 e quindi anche G ne possiede.

Una precisazione: col senno di poi, sia P che Q sono normalizzati da tutto il sottogruppo abeliano PQ e quindi il numero di 5− e 7−Sylow è inferiore a $|G|/|PQ| = 3$. Pertanto sia P che Q sono normali in G. Se avete dimostrato che uno tra P e Q è necessariamente non normale, avete sbagliato.

Esercizio 3. Se I, J sono ideali dell'anello commutativo con unità A, si definisce

$$(I : J) = \{a \in A \,|\, aJ \subset I\}.$$

(a) Mostrare che $(I : J)$ è un ideale di A.

(b) Mostrare che $I \subset (I : J)$.

(c) Calcolare $(I : J)$ quando $A = \mathbb{Z}, I = (24), J = (36)$.

Soluzione:

(a) $(I : J)$ contiene 0 in quanto $0J = (0) \subset I$; se $a, b \in (I : J)$, allora $aJ, bJ \subset I$ e quindi se $j \in J$ avremo che $(a + b)j = aj + bj \in aJ + bJ \subset I$, perciò $a + b \in (I : J)$. Infine, se $a \in (I : J)$ e $r \in A$, allora $aJ \subset I$ e poiché I è un ideale, allora $(ra)J = r(aJ) \subset rI \subset I$. In conclusione, $(I : J)$ è un ideale di A. Non serve mostrare che $a \in (I : J) \implies -a \in (I : J)$ poiché $-a$ si ottiene come $-1 \cdot a$.

(b) Se $a \in I$, allora $aJ \subset IJ \subset I$, dal momento che I è un ideale.

(c) Ci viene chiesto per quali valori di $a \in \mathbb{Z}$ succeda che moltiplicando a per un multiplo di $36 = 2^2 \cdot 3^2$ si ottenga sempre un multiplo di $24 = 2^3 \cdot 3$. Questo deve accadere in particolare moltiplicando a per 36, e deve quindi valere $24|36a$. Ma allora $2|3a$ e poiché 2 è primo con 3, si ottiene $2|a$.

Ricapitolando, $a(36) \subset (24)$ accade esattamente quando a è un numero pari e quindi in questo caso $(I : J) = (2)$.

Risposta: (c) $(I : J) =$ $\boxed{}$

Esercizio 4. Determinare tutti i modi di scrivere 2450 come somma di due quadrati.

Soluzione:

Un primo modo di risolvere l'esercizio, senza usare nulla di ciò che abbiamo visto nel corso, è osservare che se $2450 = a^2 + b^2$, allora uno dei due quadrati è sicuramente $\geq 2450/2 = 1225$. Provando come a^2 ciascun quadrato compreso tra 1225 e 2450 si verifica, a mano, che $2450 - a^2$ è un quadrato perfetto nei soli due casi

$$2450 = 1225 + 1225 = 35^2 + 35^2, \qquad 2450 = 2401 + 49 = 49^2 + 7^2.$$

Ma in fondo il corso lo abbiamo seguito, e sappiamo che nel dominio $\mathbb{Z}[i]$ degli interi di Gauss la norma euclidea $N(a + bi) = a^2 + b^2$ è moltiplicativa e vale la fattorizzazione unica.

Scrivere 2450 nella forma a^2+b^2 equivale a trovare tutti gli interi di Gauss $a+bi$ la cui norma euclidea coincide con $2450 = 2 \cdot 5^2 \cdot 7^2$. La fattorizzazione unica di $a + bi$ in primi di Gauss sarà della forma

$$a + bi = u\pi_1 \cdot \cdots \cdot \pi_k$$

dove u è uno dei quattro invertibili $\pm 1, \pm i$ mentre $\pi_1, \ldots, \pi_k$ sono primi di Gauss, la cui norma euclidea deve dividere 2450. Le uniche possibilità, a meno di moltiplicare per invertibili, sono $1 + i$, che ha norma euclidea 2; $2 \pm i$, che hanno norma euclidea 5; 7, che ha norma euclidea 7^2. Concludiamo allora che ogni possibile scelta di $a + bi$ deve essere (in modo unico!) della forma

$$a + bi = u \cdot (1 + i) \cdot \pi_2 \cdot \pi_3 \cdot 7,$$

dove $\pi_2, \pi_3 \in \{2 \pm i\}$. Le possibili scelte per $a + bi$ sono allora 12:

$$u(1 + i)(2 + i)^2 \cdot 7, \qquad u(1 + i)(2 + i)(2 - i) \cdot 7, \qquad u(1 + i)(2 - i)^2 \cdot 7,$$

che svolgendo i conti diventano

$$u(-7 + 49i), \qquad u(35 + 35i), \qquad u(49 - 7i).$$

Dopo aver moltiplicato per $u \in \{\pm 1, \pm i\}$ otteniamo per (a, b) le dodici soluzioni $(\pm 7, \pm 49)$, $(\pm 49, \pm 7)$, $(\pm 35, \pm 35)$, che corrispondono alle due decomposizioni che avevamo trovato precedentemente anche a mano.

Risposta: $2450 =$ 

Esercizio 5. Si consideri l'anello $R = \mathbb{Z}[\sqrt[3]{2}]$. Trovare un intero primo p tale che (p) sia un ideale primo di R. (Giustificare la risposta.)

Soluzione: L'esercizio chiede per quali scelte di p primo in $\mathbb{Z}$ il quoziente $R/(p)$ sia un dominio d'integrità. Osserviamo innanzitutto che R è isomorfo a $\mathbb{Z}[x]/(x^3 - 2)$. In effetti, l'omomorfismo di valutazione

$$\mathbb{Z}[x] \ni f(x) \mapsto f(\sqrt[3]{2}) \in \mathbb{Z}[\sqrt[3]{2}]$$

è suriettivo per costruzione e ammette $x^3 - 2$ nel suo nucleo. Più precisamente, $x^3 - 2 \in \mathbb{Z}[x]$ è il polinomio minimo, su $\mathbb{Q}$, dell'algebrico $\sqrt[3]{2}$; inoltre è primitivo (è monico!) e per il Lemma di Gauss ogni polinomio a coefficienti in $\mathbb{Z}$ che ne è multiplo in $\mathbb{Q}[x]$ deve esserne multiplo anche in $\mathbb{Z}[x]$. Ricapitolando, i polinomi che stanno nel nucleo dell'omomorfismo di valutazione sono tutti e soli i multipli di $x^3 - 2$. Uno dei teoremi di isomorfismo ci fornisce allora un isomorfismo tra $R = \mathbb{Z}[\sqrt[3]{2}]$ e l'anello quoziente $\mathbb{Z}[x]/(x^3 - 2)$.

Possiamo sfruttare questo fatto per osservare che $R/(p)$ è allora isomorfo a $\mathbb{Z}[x]/(x^3 - 2, p)$ che è a sua volta isomorfo a $\mathbb{F}_p[x]/(x^3 - 2)$. Questo quoziente è un dominio d'integrità esattamente quando l'ideale $(x^3 - 2)$ è primo nel dominio euclideo $\mathbb{F}_p[x]$ e cioè quando il polinomio $x^3 - 2$ è irriducibile in $\mathbb{F}_p[x]$.

L'esercizio ammette allora la nuova formulazione: trovare un numero primo p tale che $x^3 - 2$ non abbia radici in $\mathbb{F}_p$. Le prime scelte piccole sono

- $p = 2$; $x^3 - 2 = x \cdot x \cdot x$;
- $p = 3$; $x^3 - 2 = x^3 + 1 = (x + 1)^3$;
- $p = 5$; $x^3 - 2 = (x - 3)(x^2 + 3x + 4)$,

e in questi casi $x^3 - 2$ è riducibile.

Scegliendo invece $p = 7$, si vede che $x^3 - 2$ non si annulla per nessuna scelta di $x \in \mathbb{F}_7$ ed è quindi irriducibile in $\mathbb{F}_7[x]$.

Risposta: $p =$ $\boxed{}$

Foglio per la brutta copia

Foglio per la brutta copia

Foglio per la brutta copia