Corso di Algebra 1 – a.a. 2012-2013

Prova scritta del 14.2.2013

1. Si consideri il gruppo $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$.
   (a) Si contino gli elementi di ordine 9 in G;
   (b) si contino i sottogruppi ciclici di G di ordine 9;
   (c) si stabilisca se G è isomorfo o meno al gruppo $\mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$.

2. Sia H il sottogruppo del gruppo simmetrico S_6 generato dalle trasposizioni:
$$\sigma_1 = (1\ 2), \quad \sigma_2 = (3\ 4), \quad \sigma_3 = (5\ 6).$$
   Si consideri il sottoinsieme $K = \{\tau \in S_6 : \tau H \tau^{-1} = H\}$.
   (a) Si verifichi che K è un sottogruppo di S_6 e che H è un sottogruppo normale di K;
   (b) si dimostri che K coincide con il centralizzatore dell'elemento $\sigma = (1\ 2)(3\ 4)(5\ 6)$;
   (c) si costruisca un isomorfismo tra K/H e il gruppo simmetrico S_3.

3. Sia F un campo e $p(X) \in F[X]$ un polinomio irriducibile. Fissato $n \geq 2$ sia I l'ideale di $F[X]$ generato da $p(X)^n$ e si consideri l'anello $A = F[X]/I$. Dato un polinomio $q(X) \in F[X]$ indichiamo con $\overline{q(X)}$ la classe di $q(X)$ in A.
   (a) Si verifichi che la classe $\overline{q(X)}$ è un divisore di zero in A se e solo se $p(X)$ divide $q(X)$ e $q(X) \notin I$;
   (b) si verifichi che $\overline{q(X)}$ è invertibile se e solo se $p(X)$ non divide $q(X)$;
   (c) si descrivano tutti gli ideali di A.

4. Sia p un numero primo. Indichiamo con L il campo $\mathbb{Z}/(p)$. Sia $P \in L[X]$ il polinomio $X^4 - 4X^2 + 2$. Sia E un campo di spezzamento di P su L. Decomporre P in fattori irriducibili e trovare il grado $[E : L]$ in ognuno dei seguenti casi:
   (a) $p = 7$;
   (b) $p = 5$.

Soluzioni

1. (a) Sono gli elementi (a_1, a_2, a_3) tali che $9a_i = 0$ per ogni i e a_i ha ordine 9 per almeno un i. Quindi a_1 è arbitrario; inoltre, o a_2 ha ordine 9 e a_3 è un elemento arbitrario del sottogruppo Γ di ordine 9 di $\mathbb{Z}/27\mathbb{Z}$ oppure a_2 non ha ordine 9 e a_3 è un generatore di $\Gamma \simeq \mathbb{Z}/9\mathbb{Z}$. Dato che in $\mathbb{Z}/9\mathbb{Z}$ vi sono esattamente $\varphi(9) = 3(3-1) = 6$ generatori, il numero cercato è
$$3 \cdot 6 \cdot 9 + 3 \cdot 3 \cdot 6 = 216$$
   (b) Ogni sottogruppo ciclico di G di ordine 9 contiene 6 generatori, quindi 6 elementi di ordine 9. Dunque il numero di questi sottogruppi è $216/6 = 36$.
   (c) Ragionando come al punto (a) si conclude che $\mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$ contiene esattamente 72 elementi di ordine 9. La risposta è quindi no.

2. (a) K non è vuoto perché contiene l'identità. Se $\sigma, \tau \in K$,

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

Dato che S_6 è un gruppo finito ne segue che K è un sottogruppo. Che H sia normale in K segue dalla definizione stessa di K.

(b) Dato che i σ_i sono cicli disgiunti il gruppo H è il prodotto diretto dei tre sottogruppi (di ordine 2) che essi generano. Inoltre i σ_i sono le sole trasposizioni contenute in H. Quindi il coniugio per un elemento di K permuta tra loro i σ_i. Ne segue che ogni elemento di K è contenuto nel centralizzatore di σ. Viceversa, se

$$\sigma = \tau\sigma\tau^{-1} = (\tau(1)\ \tau(2))(\tau(3)\ \tau(4))(\tau(5)\ \tau(6))\,,$$

per l'unicità della decomposizione di una permutazione in prodotto di cicli disgiunti, $\{(\tau(1)\ \tau(2)), (\tau(3)\ \tau(4)), (\tau(5)\ \tau(6))\} = \{\sigma_1, \sigma_2, \sigma_3\}$. In altre parole il coniugio per τ permuta tra loro i σ_i, e quindi porta elementi di H in elementi di H.

(c) Come spiegato nel punto precedente, il coniugio per un elemento di K permuta tra loro i σ_i. Questo dà un omomorfismo $\alpha : K \to S(\{\sigma_1, \sigma_2, \sigma_3\}) = S_3$. Dato che H è abeliano, è contenuto nel nucleo di α. Viceversa, se un elemento di K agisce come la permutazione banale, è chiaro che deve essere un prodotto di σ_i, e quindi un elemento di H. Per il primo teorema di isomorfismo per gruppi, resta da mostrare che α è suriettivo. Sia ρ una permutazione dei σ_i, e scriviamo $\rho(\sigma_1) = (a\ b)$, $\rho(\sigma_2) = (c\ d)$, $\rho(\sigma_3) = (e\ f)$. Se poniamo $\tau(1) = a$, $\tau(2) = b$, $\tau(3) = c$, $\tau(4) = d$, $\tau(5) = e$, $\tau(6) = f$, si verifica immediatamente che $\tau \in K$ e che $\alpha(\tau) = \rho$.

3. (a) Se $p \mid q$, allora $p^n \mid p^{n-1}q$, cioè $\overline{p}^{n-1}\overline{q} = 0$. Se inoltre $q \notin I$, allora $\overline{q} \neq 0$. D'altra parte $p^{n-1} \notin I$, quindi $\overline{p}^{n-1} \neq 0$. Viceversa, supponiamo che $\overline{q}$ sia un divisore di zero, cioè che ci sia $s \in F[X]$, $s \notin I$, tale che $\overline{qs} = 0$. In altri termini, stiamo supponendo che $p^n \mid qs$ ma anche che $p^n \nmid q$ e che $p^n \nmid s$. Ne segue che necessariamente $p \mid q$.

(b) Se $p \nmid q$ i polinomi p^n e q sono primi fra loro, quindi ci sono altri polinomi r e s tali che $rp^n + sq = 1$. Riducendo modulo I ne segue che $\overline{sq} = 1$. Supponiamo viceversa che esista un polinomio s tale che $\overline{sq} = 1$. Ciò significa che $1 - sq \in I$, cioè che esiste un altro polinomio r tale che $1 - sq = rp^n$. Ne segue che $p \nmid q$, perché altrimenti $p \mid 1$ (!!!).

(c) A è un PID in quanto quoziente di un PID. Quindi ogni ideale non nullo J di A è della forma $(\overline{q})$, dove $q \notin I$. Se scriviamo $q = p^h r$, dove r non è divisibile per p, questo equivale a dire che $h < n$. Come visto nel punto precedente, $\overline{r}$ è invertibile, e quindi $J = (\overline{p}^h)$. Se ne conclude che gli ideali di A sono tutti e soli quelli della forma $(\overline{p}^h)$ con $0 \leq h \leq n$ (dove $h = 0$ corrisponde all'ideale A e $h = n$ all'ideale nullo).

4. (a) In questo caso $P = X^4 + 3X^2 + 2 = (X^2 + 1)(X^2 + 2)$. I due fattori sono irriducibili perché i quadrati in L sono 1, $2 = 3^2$ e $4 = 2^2$. Un campo di spezzamento di P è $L[\zeta]$, dove $\zeta^2 = -1$. Infatti anche $X^2 + 2$ si spezza su $L[\zeta]$, dato che $-2 = (3\zeta)^2$. Dunque $[E : L] = 2$.

(b) In questo caso $P = X^4 + X^2 + 2$. Si verifica immediatamente che questo polinomio non ha radici in L. Supponiamo che si possa scrivere $P = (X^2 + aX + b)(X^2 + cX + d)$ con $a, b, c, d \in L$. In questo caso $c = -a$, $ad - ab = 0$ e $2 = bd$. Se $a \neq 0$ allora $d = b$ e $2 = b^2$, il che è impossibile dato che i quadrati in L sono 1 e $-1 = 4 = 2^2$. Se invece

$a = 0$ allora b e d sono radici del polinomio di secondo grado $Q(Y) = Y^2 + Y + 2$. Ma anche questo è impossibile dato che il discriminante di Q è $1^2 - 4 \cdot 2 = -2$, che non è un quadrato in L. La conclusione è che P è irriducibile in $L[X]$.

Sia ξ una radice di P in una estensione di L. Mostriamo che $L[\xi]$ è un campo di spezzamento di P e quindi che $[E : L] = 4$. Notiamo che anche $\xi^p, \xi^{p^2}, \xi^{p^3}, \ldots$ sono radici di P. Ora basta mostrare che $\xi, \xi^p, \xi^{p^2}, \xi^{p^3}$ sono distinti. In questo caso infatti essi costituiscono la totalità delle radici di P, e d'altra parte appartengono a $L[\xi]$. Ragionando per assurdo supponiamo che $\xi^{p^i} = \xi^{p^j}$ per $0 \leq j < i \leq 3$. In questo caso $\xi^{p^h} = \xi$, dove $h = i - j \leq 3$. Ciò significa che ξ appartiene al campo $\mathbb{F}_{p^h}$ con p^h elementi, e quindi che $L[\xi] \subset \mathbb{F}_{p^h}$. Ma questo è assurdo perché $[L[\xi] : L] = 4 > h = [\mathbb{F}_{p^h} : L]$.