Corso di Algebra 2 – a.a. 2012-2013

Prova scritta del 9.7.2013

1. (a) Calcolare il gruppo di Galois del polinomio $X^{104} - 1$ sul campo $F = \mathbb{Z}/(13)$.
   (b) Stessa domanda con $F = \mathbb{Z}/(2)$.

2. Sia $P(X) \in \mathbb{Q}[X]$ il polinomio $X^3 - X + 1$. Sia ζ una radice terza primitiva dell'unità e sia L un campo di spezzamento di P su $\mathbb{Q}[\zeta]$.
   (a) Mostrare che P è irriducibile sia su $\mathbb{Q}$ che su $\mathbb{Q}[\zeta]$.
   (b) Calcolare i gruppi di Galois di P su $\mathbb{Q}$ e su $\mathbb{Q}[\zeta]$.
   (c) Calcolare il gruppo di Galois $Gal(L/\mathbb{Q})$.
   (d) Descrivere esplicitamente tutti i sottocampi di L di grado 2 su $\mathbb{Q}$.

3. Sia G un gruppo finito e sia P un suo sottogruppo. Ogni elemento g del normalizzante $N(P)$ determina un automorfismo φ_g di P definito da $\varphi_g(x) = gxg^{-1}$.
   (a) Verificare che l'applicazione $\varphi : N(P) \to \mathrm{Aut}(P)$ data da $g \mapsto \varphi_g$ è un omomorfismo di gruppi.
   (b) Mostrare che il nucleo di φ è $C(P) = \{g \in G : gx = xg \text{ per ogni } x \in P\}$ (il *centralizzante* di P).

   Sia P un p-sottogruppo di Sylow di G, dove p è il minimo primo che divide l'ordine di G.
   (c) Mostrare che, se P è abeliano, tutti i fattori primi di $\#(\varphi(N(P)))$ sono strettamente maggiori di p.
   (d) Mostrare che, se P è ciclico, allora $N(P) = C(P)$.

Soluzioni

1. (a) Notiamo che $104 = 8 \cdot 13$. Dato che in caratteristica 13 l'elevamento alla tredicesima potenza è un omomorfismo (l'omomorfismo di Frobenius), $X^{104} - 1 = (X^8 - 1)^{13}$. Quindi un campo di spezzamento L per $X^8 - 1$ è anche un campo si spezzamento per $X^{104} - 1$. Ora $L = F[\alpha]$, dove α è una radice ottava primitiva dell'unità. A sua volta, α è una radice del polinomio ciclotomico $\Phi_8(X) = X^4 + 1$. Osserviamo che -1 è un quadrato in $\mathbb{Z}/(13)$. Infatti $5^2 = 25 \equiv -1 \mod 13$. Ne segue che

   $$X^4 + 1 = (X^2 - 5)(X^2 + 5) \text{ in } F[X]$$

   Si verifica per ispezione diretta che $X^2 - 5$ e $X^2 + 5$ sono irriducibili in quanto non hanno radici in F. Possiamo dunque prendere come α una radice quadrata di 5 (andrebbe ugualmente bene una radice quadrata di -5, ad esempio $\alpha^3 = 5\alpha$). In conclusione $Gal_F(X^{104} - 1) = Gal(L/F)$ è ciclico di ordine 2.

   (b) Ragionando come nel punto precedente si vede che $X^{104} - 1 = (X^{13} - 1)^8$, e quindi che il campo di spezzamento cercato coincide con quello di $X^{13} - 1$ ed è perciò della forma $F[\beta]$, dove β è una radice tredicesima primitiva dell'unità. Si sa che $Gal(F[\beta]/F)$ è

ciclico e generato dall'omomorfismo di Frobenius, cioè dall'elevamento al quadrato, che indichiamo con ϕ. Bisogna solo determinare l'ordine di ϕ, cioè il minimo $n > 0$ tale che

$$\beta = \phi^n(\beta) = \beta^{2^n}$$

o ancora il minimo $n > 0$ tale che

$$2^n \equiv 1 \mod 13$$

Usando quest'ultima descrizione si verifica immediatamente che l'ordine di ϕ è 12, o in altre parole che la classe di 2 genera il gruppo moltiplicativo di $\mathbb{Z}/(13)$.

2. Dato che il campo di spezzamento è unico a meno di isomorfismo possiamo supporre che $L \subset \mathbb{C}$.

   (a) Il polinomio $P(X)$ è irriducibile su $\mathbb{Q}$ perché non ha radici razionali. Infatti una radice dovrebbe dividere il termine noto e quindi essere uguale a ± 1. Sia α una radice di P. Il grado di $\mathbb{Q}[\alpha, \zeta]$ su $\mathbb{Q}$ è divisibile per $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ e per $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 2$, quindi vale 6. Ne segue che $[\mathbb{Q}[\alpha, \zeta] : \mathbb{Q}[\zeta]] = 3$ e dunque che P è irriducibile su $\mathbb{Q}[\zeta]$.

   (b) Il discriminante di P è -23, che non è un quadrato in $\mathbb{Q}[\zeta]$. Infatti, visto che $\zeta = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$, i numeri immaginari puri in $\mathbb{Q}[\zeta] = \mathbb{Q}[\sqrt{3}i]$ sono tutti della forma $q\sqrt{3}i$, dove q è razionale, e nessuno di questi ha quadrato -23. Di conseguenza $Gal_{\mathbb{Q}[\zeta]}(P) = Gal(L/\mathbb{Q}[\zeta])$ è il gruppo simmetrico S_3.

   (c) Segue da (b) che $[L : \mathbb{Q}] = [L : \mathbb{Q}[\zeta]][\mathbb{Q}[\zeta] : \mathbb{Q}] = 6 \cdot 2 = 12$. Sia $M \subset L$ il campo di spezzamento di P su $\mathbb{Q}$ e poniamo $N = \mathbb{Q}[\zeta]$. I gruppi $H = Gal(L/M)$ e $K = Gal(L/N)$ sono sottogruppi di $G = Gal(L/\mathbb{Q})$ di ordini $[L : M] = 2$ e $[L : N] = 6$. Sono sottogruppi normali perché M e N sono estensioni normali di $\mathbb{Q}$. Inoltre $H \cap K = \{1\}$ perché nella corrispondenza di Galois questo sottogruppo corrisponde al più piccolo sottocampo di L che contiene sia M che N, cioè $M[\zeta] = L$. Ne segue che G è prodotto diretto di H e K e quindi che

   $$Gal(L/\mathbb{Q}) \cong S_3 \times C_2$$

   (d) Nella corrispondenza di Galois questi sottocampi corrispondono ai sottogruppi di indice 2 di $S_3 \times C_2 \cong Gal(L/\mathbb{Q})$, che sono S_3 e $A_3 \times C_2$. I campi corrispondenti sono $N = \mathbb{Q}[\sqrt{-3}]$ e $\mathbb{Q}[\sqrt{-23}]$.

3. (a) $\varphi_{hg}(x) = hgx(hg)^{-1} = hgxg^{-1}h^{-1} = \varphi_h(gxg^{-1}) = \varphi_h(\varphi_g(x)) = \varphi_h \circ \varphi_g(x)$, quindi $\varphi_{hg} = \varphi_h \circ \varphi_g$.

   (b) È chiaro che $C(P) \subset N(P)$. Inoltre $g \in \ker \varphi \iff \varphi_g(x) = x$ per ogni $x \in P \iff gxg^{-1} = x$ per ogni $x \in P \iff gx = xg$ per ogni $x \in P \iff g \in C(P)$.

   (c) $C(P)$ contiene P perché P è abeliano. Quindi per passaggio al quoziente φ induce un omomorfismo $\psi : N(P)/P \to \mathrm{Aut}(P)$. Dato che P è un p-sottogruppo di Sylow di G, l'ordine di $N(P)/P$ è un prodotto di primi diversi da p e quindi, per ipotesi, maggiori di p. L'ordine di $\psi(N(P)/P) = \varphi(N(P))$ divide l'ordine di $N(P)/P$ e quindi anch'esso è un prodotto di primi maggiori di p.

   (d) Se $\#(P) = p^h$, il gruppo $\mathrm{Aut}(P)$ ha ordine $p^{h-1}(p-1)$ e quindi tutti i fattori primi di $\#(\mathrm{Aut}(P))$ sono minori o uguali a p. Ne segue che l'ordine di $\mathrm{Aut}(P)$ e quello di $\varphi(N(P))$ sono primi fra loro, e quindi che $\varphi(N(P)) = \{1\}$, cioè che $N(P) = \ker \varphi = C(P)$.