Corso di Algebra 2 - a.a. 2014-2015
Prova scritta del 22.2.2016

Esercizio 0.1. *Sia L/K un'estensione di Galois finita. Siano L_1, L_2 estensioni di K contenute in L, inoltre siano H_1 e H_2 i sottogruppi di $G = \mathrm{Gal}(L/K)$ corrispondenti (nella corrispondenza di Galois) rispettivamente a L_1 e L_2. Dimostrare che, dato $f \in \mathrm{Gal}(L/K)$, $f(L_1) = L_2$ se e soltanto se $fH_1f^{-1} = H_2$. Suggerimento: che relazione c'è tra $\mathrm{Gal}(L/f(L_1))$ e $\mathrm{Gal}(L/L_1)$?*

Risoluzione. Dimostriamo che

$$\mathrm{Gal}(L/f(L_1)) = f\,\mathrm{Gal}(L/L_1)f^{-1}.$$

Infatti, se $g \in \mathrm{Gal}(L/f(L_1))$, allora

$$f^{-1}gf(x) = f^{-1}f(x) = x,$$

per ogni $x \in L_1$. Cioè, $f^{-1}gf \in \mathrm{Gal}(L/L_1)$. Viceversa, prendiamo un elemento della forma fgf^{-1} con $g \in \mathrm{Gal}(L/L_1)$. Allora, per ogni $y = f(x) \in f(L_1)$ abbiamo:

$$fgf^{-1}(y) = fg(x) = f(x) = y,$$

cioè $fgf^{-1} \in \mathrm{Gal}(L/f(L_1))$, come volevamo.

Ora, supponiamo che $f(L_1) = L_2$. Allora, abbiamo che

$$H_2 = \mathrm{Gal}(L/L_2) = \mathrm{Gal}(L/f(L_1)) = f\,\mathrm{Gal}(L/L_1)f^{-1} = fH_1f^{-1}.$$

Viceversa, supponiamo che $H_2 = fH_1f^{-1}$. Allora:

$$\mathrm{Gal}(L/L_2) = f\,\mathrm{Gal}(L/L_1)f^{-1} = \mathrm{Gal}(L/f(L_1)),$$

da cui $L_2 = f(L_1)$ per la corrispondenza di Galois. □

Esercizio 0.2. *Sia $P(X) = X^4 + 2 \in \mathbb{F}_5[X]$.*

1. *Dimostrare che $P(X)$ è irriducibile.*

2. *Determinare il gruppo di Galois di $P(X)$.*

3. *Determinare il discriminante di $P(X)$ e verificare che non è un quadrato in $\mathbb{F}_5$.*

Risoluzione. 1. Si verifica subito che $P(X)$ non ha radici in $\mathbb{F}_5$. Dobbiamo mostrare che non si può fattorizzare come prodotto di due polinomi di grado 2. Supponiamo che $P(X) = (X^2 + aX + b)(X^2 + cX + d)$. Otteniamo che $c = -a$, $ad + bc = a(d - b) = 0$, $bd = 2$, $d + b - a^2 = 0$. Se $a = 0$ abbiamo $2b^{-1} = d = -b$, quindi $b^2 = 3$, ma 3 non è un quadrato in $\mathbb{F}_5$. Quindi $a \neq 0$ e allora $d = b$, ma $d = 2b^{-1}$ quindi $b^2 = 2$ che è impossibile perché nemmeno 2 è un quadrato in $\mathbb{F}_5$. Quindi P è irriducibile.

2. Poiché P è irriducibile in $\mathbb{F}_5[X]$, il suo gruppo di Galois è un sottogruppo transitivo e ciclico di S_4, quindi è isomorfo a $\mathbb{Z}/4\mathbb{Z}$.

3. Il discriminante di $P(X)$ è il determinante della matrice

$$\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}$$

che è uguale a 3 che non è un quadrato in $\mathbb{F}_5$. □

Esercizio 0.3. *Sia G un gruppo di cardinalità 104. Supponiamo inoltre che i 2-Sylow non siano ciclici e che contengano esattamente due elementi di ordine 4.*

1. *Descrivere le possibili classi di isomorfismo dei 2-Sylow.*
2. *Dimostrare che G è isomorfo al prodotto semidiretto di un 2-Sylow e di un 13-Sylow.*
3. *Sia K un 2-Sylow, H un 13-Sylow e $\phi : K \to Aut(H)$ l'omomorfismo che descrive l'azione di K su H per coniugio. Dimostrare che per ogni $g \in K$, $\phi(g)$ ha ordine minore o uguale a 2.*
4. *Descrivere tutti i possibili omomorfismi ϕ come sopra.*

Soluzione. 1. $104 = 13 \cdot 8$, quindi i 2-Sylow hanno ordine 8. I gruppi di ordine 8 non ciclici sono isomorfi o a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, o a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, o ai quaternioni, o al gruppo diedrale D_4. L'unico gruppo tra questi che ha esattamente due elementi di ordine 4 è il diedrale. Quindi ogni 2-Sylow K è isomorfo a D_4.

2. Il numero dei 13-Sylow è congruo a 1 modulo 13 e divide $|G|$, quindi esiste un unico 13-Sylow $H \cong \mathbb{Z}/13\mathbb{Z}$ che pertanto è normale in G. Sia K un 2-Sylow. Si ha $HK = KH$ per la normalità di H, quindi HK è un sottogruppo di G. Inoltre, $|H \cap K|$ deve dividere sia $|H| = 13$ che $|K| = 8$, quindi $H \cap K$ è banale. Dunque $|HK| = |H| \cdot |K| = 104$ e pertanto $G = HK$.

3. Abbiamo dmostrato che $K \cong D_4 = \langle x, y \mid x^4 = y^2 = 1,\ yxy^{-1} = x^{-1} \rangle$. Il gruppo $Aut(H) = Aut(\mathbb{Z}/13\mathbb{Z}) \cong (\mathbb{Z}/13\mathbb{Z})^*$ è abeliano.

L'ordine di $\phi(y)$ deve dividere l'ordine di y che è 2, quindi è minore o uguale a 2. L'ordine di $\phi(x)$ deve dividere l'ordine di x che è 4. Inoltre si ha: $(\phi(x))^{-1} = \phi(x^{-1}) = \phi(yxy^{-1}) = \phi(y) \circ \phi(x) \circ \phi(y^{-1}) = \phi(y) \circ \phi(x) \circ (\phi(y))^{-1} = \phi(x)$ perché $Aut(H)$ è abeliano. Quindi $\phi(x) \circ \phi(x) = Id$ e dunque anche l'ordine di $\phi(x)$ è minore o uguale a 2. Infine $\phi(x^2) = \phi(x) \circ \phi(x) = Id$, $(\phi(yx^i))^2 = \phi((yx^i)^2) = \phi(1) = Id$.

4. Sia $\phi : D_4 \to Aut(\mathbb{Z}/13\mathbb{Z}) \cong (\mathbb{Z}/13\mathbb{Z})^*$ come sopra. In $(\mathbb{Z}/13\mathbb{Z})^*$ c'è un solo elemento di ordine 2 che è $[12]$, quindi se indichiamo con z un generatore di H, per il punto tre sappiamo che si deve avere $\phi(x)(z) = z$ oppure $\phi(x)(z) = z^{12}$ e $\phi(y)(z) = z$ oppure $\phi(y)(z) = z^{12}$ e in ognuno di questi casi otteniamo un omomorfismo ben

definito perché x e y generano D_4, z genera H, $o(\phi(x))|2$ (e quindi divide 4), $o(\phi(y))|2$ e si ha sempre $\phi(x^{-1}) = \phi(yxy^{-1}) = \phi(x)$ perché in tutti i casi $\phi(x) \circ \phi(x) = Id$. Quindi ho quattro possibili omomorfismi definiti da: 1) $\phi = Id$, 2) $\phi(x)(z) = z$ e $\phi(y)(z) = z^{12}$, 3) $\phi(x)(z) = z^{12}$ e $\phi(y)(z) = z$, 4) $\phi(x)(z) = z^{12}$ e $\phi(y)(z) = z^{12}$.

$\square$