Teoria di Galois 1 - Tutorato IV

Gruppi di Galois, campi ciclotomici, campi finiti

Venerdì 29 Aprile 2005

Esercizio 1. Si calcoli il gruppo di Galois (cioè il numero di elementi e la struttura) di ciascuno dei seguenti polinomi:

a. $x^4 + 2x^3 + 15x^2 + 14x + 73$;

b. $x^4 + 8x^3 + 26x^2 + 24x + 28$;

c. $x^4 - 354x^2 + 29929$;

d. $x^4 - 11x^3 + 41x^2 - 61x + 30$;

e. $x^4 + 8x^3 + 14x^2 - 8x - 23$;

f. $x^4 - 13x^3 + 64x^2 - 142x + 121$;

g. $x^4 + x^3 + 2x^2 + 4x + 2$

h. $x^4 + 25x^2 + 5$;

i. $x^4 + 3x^3 + 3$

l. $x^4 + x^3 + 4x^2 + 3x + 3$;

m. $x^4 + 60x^3 + 99x^2 + 60x + 1$

n. $x^4 - 356x^2 + 29584$;

o. $x^4 + 8x + 12$;

Esercizio 2. Si elenchino i sottogruppi transitivi di S_4 descrivendone gli elementi come permutazioni.

Esercizio 3. Descrivere gli elementi del gruppo di Galois del polinomio $x^5 - 2$ mostrando che ha 20 elementi.

Esercizio 4. Dimostrare che il gruppo di Galois de polinomio (che si può assumere irriducibile) $x^5 + x^4 + x^3 + 2x^2 + 3x + 4$ non ha 20 elementi né 10 mostrando che contiene un 3 ciclo. (*Pensare al numero primo* 2)

Esercizio 5. In ciascuno dei seguenti casi si calcoli il campo di spezzamento e il numero di campi intermedi tra il campo base e il campo di spezzamento.

a. $(x^4 + x^2 + x + 1)(x^3 + x + 1) \in \mathbb{F}_2[x]$;

b. $(x^3 + x + 1)(x^6 + x + 1) \in \mathbb{F}_3[x]$;

c. $(x^4 + x^2 + 1)(x^3 + x + 1)(x^3 + 1) \in \mathbb{F}_5[x]$;

d. $(x^4 + x^2 + 1)(x^3 + x + 1)(x^3 + 1) \in \mathbb{F}_7[7]$.

Esercizio 6. Mostrare che se f è un polinomio irriducibile di grado tre a coefficienti in un campo F, G_f è di tipo A_3 se e solo se F_f non contiene sottocampi quadratici.

Esercizio 7. Calcolare una fomula per il discriminante di $X^n + aX + b$.

Esercizio 8. Si calcoli il gruppo di Galois di $y^5 - 3y^2 + 1$.

Esercizio 9. Mostrare che $\Phi_{p^r}(x) = \Phi_p(x^{p^{r-1}})$ e dedurne una formula per il discriminante di $\Phi_{p^r}(x)$.

Esercizio 10. Sia $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$ il polinomio ciclotomico. Mostrare che

$$\operatorname{disc} \Phi_p(x) = (-1)^{(p-1)/2} p^{p-2}.$$

Esercizio 11. Mostrare che se n è dispari, allora $\Psi_{2n}(x) = \Psi_n(-x)$ e che

$$\Psi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

dove μ è la funzione di Möbius.

Esercizio 12. L'obbiettivo di questo esercizio è di scoprire per passi successivi del seguente:
Teorema. *Dato un gruppo* **abeliano** G*, esiste sempre* $f \in \mathbb{Q}[x]$ *tale che* $G \cong G_f$.

i. Il famoso Teorema di Dirichlet per primi in progressione aritmentica afferma (tra l'altro) che per ogni intero m, esiste sempre un numero primo congruente a 1 modulo m. Dedurne che esiste un polinomio a coefficienti razionali il cui gruppo di Galois è isomorfo al gruppo ciclico $\mathbb{Z}/m\mathbb{Z}$;

Suggerimento: cercare tra i sottocampi di un opportuno campo ciclotomico.

ii. Dimostrare f e g sono polinomi $\in \mathbb{Q}[x]$ con campi di spezzamento *linearmente disgiunti* (i.e. $\mathbb{Q}_f \cap \mathbb{Q}_f = \mathbb{Q}$) allora $G_{fg} \cong G_f \times G_f$.

Suggerimento: Utilizzare la proprietà che $\operatorname{Gal}(E_1E_2/F) \cong \{(\sigma_1, \sigma_2) \in \operatorname{Gal}(E_1/F) \times \operatorname{Gal}(E_2/F) \mid \sigma_1|_{E_1 \cap E_2} = \sigma_2|_{E_1 \cap E_2}\}$.

iii. Dedurre il teorema dal Teorema di classificazione dei gruppi abeliani finiti che dice che ogni gruppo abeliano è il prodotto di gruppi ciclici con ordini coprimi.