Algebra 1
Prova scritta del 6 settembre 2019
Soluzioni

Esercizio 1. Trovare tutte le soluzioni intere del sistema

$$\begin{cases} x = 1472^{3452} & \mod 20 \\ x = 219^{45} & \mod 23 \end{cases}$$

Soluzione: Per il teorema cinese del resto, il sistema equivale al sistema

$$\begin{cases} x = 1472^{3452} & \mod 4 \\ x = 1472^{3452} & \mod 5 \\ x = 219^{45} & \mod 23 \end{cases}$$

Ora 1472 e 3452 sono multipll di 4, $45 = 2 \times 22 + 1$ e $219 = 9 \times 23 + 12$. Dunque il sistema è equivalente a

$$\begin{cases} x = 0 & \mod 4 \\ x = 1 & \mod 5 \\ x = 12 & \mod 23 \end{cases}$$

La soluzione generale del sistema dato dalle prime due equazioni è $16+20y$, $y \in \mathbb{Z}$. Sostituendo dobbiamo dunque risolvere

$$3y = 4 \qquad \mod 23$$

ovvero

$$y = 9 \qquad \mod 23$$

e quindi

$$x = 16 + 20(9 + 23z) = 196 + 460z.$$

Esercizio 2.

1. Determinare tutti gli omomorfismi $C_{15} \to C_{18}$.
2. Sia G è un gruppo finito di ordine dispari. Dimostrare che ogni elemento è un quadrato.
3. Sia G è un gruppo finito di ordine pari. Dimostrare che esiste un elemento di ordine due.

Soluzione:

1. Notiamo che $MCD(15, 18) = 3$ e dunque per il teorema di Lagrange l'immagine di un omomorfismo

   $$\phi : C_{15} \to C_{18}$$

   è contenuta nell'unico sottogruppo H di C_{18} con tre elementi. Ora se $C_{15} = \langle x \rangle$ e $C_{18} = \langle y \rangle$, $H = \langle y^6 \rangle$ e necessariamente dato che ϕ è determinato da $\phi(x)$ ci sono 3 tali omomorfismi univocamente definiti da

   $$\phi(x) = y^6, \quad \phi(x) = y^{12}, \quad \phi(x) = y^{18} = e$$

   L'immagine di un tale ϕ è H nei primi due casi, il sottogruppo identità nel terzo.

2. Sia $|G|$ dispari. Se $g \in G$, allora $o(g) = 2h + 1$ è dispari e il sottogruppo $H =< g >$ ha ordine $2h + 1$. Allora $g^{2h+1} = g^{2h} g = e$. Quindi

   $$g = g^{-2h} = (g^{-h})^2.$$

3. Se $|G| = 2m$ è pari, G contiene almeno un elemento g diverso dall'identità e $o(g) = 2^r h$ con h dispari e $r \geq 1$. Prendiamo $x = g^{2^{r-1}h}$. $x \neq e$ e

$$x^2 = (g^{2^{r-1}h})^2 = g^{2^r}h = e.$$

Esercizio 3. Dimostrare che esiste a meno di isomorfismo un unico gruppo di ordine 3149.

Soluzione: $|G| = 3149$. $3149 = 47 \times 67$ Allora per il Teoremi di Sylow G contiene un sottogruppo normale H ciclico di ordine 67. L'azione di G su H per coniugio induce un omomorfismo $s : G/H \to Aut(H)$.

Ora $|Aut(H)| = 67 - 1 = 66$, mentre $|G/H| = 37$. Ma $MCD(66, 37) = 1$. Dunque s è l'omorfismo triviale e il gruppo G è abeliano e quindi ciclico in quanto prodotto di due sottogruppi ciclici di ordine coprimo.

Esercizio 4. Determinare gli ideali di $\mathbb{Z}[i]$ che contengono 30.

Soluzione: In $\mathbb{Z}$, $30 = 2 \times 3 \times 5$. Ora $(2) = (1+i)^2$, 3 è un intro di Gauss primo e $5 = (1+2i)(1-2i)$. Quindi in $\mathbb{Z}[i]$ un ideale contiene 30 se e solo se

$$I = ((1+i)^a 3^b (1+2i)^c (1-2i)^d)$$

con $a \leq 2$, $b, c, d \leq 1$.

Esercizio 5. Si consideri l'ideale generato I dai polinomi $x^3+8x^2+15x+6$, $x^4+6x^3+4x^2+6x+3. \in \mathbb{Q}[x]$. Dimostrare che $\mathbb{Q}[x]/I$ è un campo.

Soluzione: Calcolando

$$x^4 + 6x^3 + 4x^2 + 6x + 3 = (x-2)(x^3 + 8x^2 + 15x + 6) + 5(x^2 + 6x + 3)$$

e

$$x^3 + 8x^2 + 15x + 6 = (x+2)(x^2 + 6x + 3).$$

Dunque

$$x^2 + 6x + 3 = MCD(x^4 + 6x^3 + 4x^2 + 6x + 3, x^3 + 8x^2 + 15x + 6)$$

e

$$I = (x^2 + 6x + 3).$$

Dato che per il criterio di Eisenstein $x^2 + 6x + 3$ è irriducibile, I è massimale e $\mathbb{Q}[x]/I$ è un campo.

Esercizio 6. Si considerino i polinomi razionali $f_1 = x^3 + 3x + 1$ e $f_2 = x^3 - 3x + 1$. Per $i = 1, 2$, sia $K_i \supset \mathbb{Q}$ il campo di spezzamento di f_i. Si determini

1. $[K_i : \mathbb{Q}]$
2. Il gruppo di Galois $\mathrm{Gal}(f_i)$.
3. Il numero dei campi intermedi $K_i \supset L \supset \mathbb{Q}$ e il loro grado come estensioni di $\mathbb{Q}$.

Soluzione: I due polinomi sono entrambi irriducibili in quanto se fossero riducibili avrebbero una radice intera necessariamente uguale a ± 1 ma si verifica che 1 e -1 non sono radici di f_i. Ne segue che $\mathrm{Gal}(f_i)$ è un sottogruppo del gruppo S_3 delle permutazioni delle radici di f_i di ordine 3 o 6.

Cominciamo col caso di f_1. La derivata $f_1' = 3x^2 + 3$ è sempre positiva dunque f_1 è crescente e ha una sola radice reale e due radici complesse coniugate. Il coniugio da un elemento di $\mathrm{Gal}(f_1)$ di ordine 2. Ne segue che $\mathrm{Gal}(f_1) = S_3$. Dunque $[K : \mathbb{Q}] = 6$ e ci sono oltre a K e a $\mathbb{Q}$, tre campi intermedi di grado 3.

Passiamo al caso di f_2. Poniamo $x = y^2 - 2$. Allora sostituendo il nostro polinomio diventa

$$(y^2-2)^3-3(y^2-2)+1 = y^6-6y^4+12y^2-8-3y^2+6+1 = y^6-6y^4+9y^2-1 = (y^3-3y+1)(y^3-3y-1).$$

Ne segue che se $f_2(\alpha) = 0$ anche $f(\alpha^2 - 2) = 0$ e $K = \mathbb{Q}(\alpha)$. Quindi $[K : \mathbb{Q}] = 3$ e $\mathrm{Gal}(f_2) = C_3$. In particolare i soli campi intermedi sono K e $\mathbb{Q}$.

Alternativamente si verifica che il discriminante di f_2 è 9, un quadrato. Dunque $[K : \mathbb{Q}] = 3$ e $\mathrm{Gal}(f_2) = C_3$.