Algebra 1

Esercizio 1. Trovare tutte le soluzioni intere dell'equazione $x^2 + y^2 = 10^z - 1$.

Risoluzione: Se $z < 0$, $10^z - 1 < 0$, ma la somma di due quadrati è ≥ 0. Dunque $z \geq 0$.

Se $z > 1$ $10^z \equiv 0 \bmod 4$ dunque $10^z - 1 \equiv 3 \bmod 4$.

Ora questo implica che se una soluzione c'è o x è pari e y è dispari o viceversa. Supponiamo $x = 2h$. Abbiamo due casi:

$y = 4k + 1$ ma allora $x^2 + y^2 = 4(h^2 + k^2 + k) + 1$ non è congruo a 3 modulo 4,

$y = 4k + 3$ ma allora $x^2 + y^2 = 4(h^2 + k^2 + k + 4) + 1$ non è congruo a 3 modulo 4.

Rimangono i casi $z = 0$ e $z = 1$.

Se $z = 0$ l'equazione diventa $x^2 + y^2 = 0$ che ha la sola soluzione $(0, 0)$ dunque l'equazione originale ha la soluzione $(0, 0, 0)$.

Se $z = 1$ l'equazione diventa $x^2 + y^2 = 9$ e le uniche soluzioni sono $(\pm 3, 0, 1)$, $(0, \pm 3, 1)$.

Esercizio 2. Sia $\mathbb{F}_2$ il campo con 2 elementi. Sia G l'insieme delle applicazioni $g : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ della forma $g(v) = Av + w$ con $A \in Gl(2, \mathbb{F}_2)$xt e $w \in \mathbb{F}_2^2$. Dimoostrare che

1. G ` un gruppo rispetto alla composizione.
2. G è isomorfo al gruppo S_4 delle permutazioni su un insieme con 4 elementi.

Risoluzione: La prima è una verifica immediata. In effetti se $g_{A,w}(v) = Av + w$ e $g_{B,u}(v) = Bv + u$, $g_{B,u}g_{A,w}(v) = g_{B,u}(Av + w) = BA(v) + (Bw + u) = g_{BA,Bw+u}$. Inoltre $g_{I,0}$ è l'identità e $g_{A,w}^{-1} = g_{A^{-1},-A^{-1}w}$.

Per la seconda notiamo che G agisce su $\mathbb{F}_2^2$ dunque è un sottogruppo di S_4. Inoltre $|G| = |Gl(2, \mathbb{F}_2)||\mathbb{F}_2^2| = 6 \times 4 = 24 = |S_4|$.

Esercizio 3. Sia G un gruppo di ordine $2^4 5^6$. Dimostrare che G non è semplice.

Risoluzione: Sia n_5 il numero di 5 Sylow. Allora n_5 divide 16 ed congruo a 1 modulo 5. Dunque o $n_5 = 1$ e l'unico 5-Sylow è normale oppure $n_5 = 16$ e si ha un omomorfismo $f : G \to S_{16}$. Se G fosse semplice f sarebbe iniettivo e $|G|$ divide 16! in particolare 5^6 divide 16!, assurdo.

Esercizio 4. Siano A Dimostrare che ogni ideale di A è primo se e solo se $I^2 = I$ per ogni ideale di A e se I, J sono ideali di A o $I \subset J$ o $J \subset I$.

Risoluzione: Sia $I \subset A$ un ideale. Allora sia I che I^2 sono ideali primi, $I^2 \subset I$. Se ci fosse un $a \in I \setminus I^2$ $a^2 \in I^2$ e I^2 non sarebbe primo. Dunque $I = I^2$. Siano ora I e J due ideali I, J e $IJ \subset I \cap J$ sono primi. Supponiamo esistano $a \in I \setminus J$ e $b \in J \setminus I$. $ab \in IJ$ dunque o $a \in IJ$ dunque $a \in J$ assurdo o $b \in IJ$ dunque $b \in I$ assurdo. Dunque o $I \subset J$ o $J \subset I$.

Viceversa sia I ideale di A. Supponiamo non sia primo. esistono $a, b \in A \setminus I$ con $ab \in I$, allora e $J_1 = (a)$ $J_2 = (b)$ chiaramente I non contiene J_1 e neanche J_2. Inoltre possiamo assumere $J_1 \subset J_2$ e $I \subset J_1 \subset J_2$. Ma ora $I \supset (ab) = J_1 J_2 \supset J_1^2 = J_1$ il che implica $a \in I$ assurdo.

Esercizio 5. Si consideri il polinomio $x^2 + 1 \in \mathbb{F}_p[x]$, con $\mathbb{F}_p$ il campo con p elementi, p primo. Si determini per quali p, $\mathbb{F}_p[x]/(X^2 + 1)$ è isomorfo come anello a $\mathbb{F}_p \times \mathbb{F}_p$.

Risoluzione: L'anello $\mathbb{F}_p \times \mathbb{F}_p$ ha divisori di zero visto che $(1, 0)(0, 1) = (0, 0)$. e non ha nilpotenti dato che $(a, b)^h = (a^h, b^h) = (0, 0)$, allora $a^h = b^h = 0$ ovvero $a = b = 0$. La prima proprietà ci dice che il polinomio $x^2 + 1$ è riducibile in $\mathbb{F}_p[x]$, la seconda che ha radici distinte. Ora $x^2 + 1$ è riducibile se e solo se esiste $a \in \mathbb{F}_p$ con $a^2 = -1$, la seconda che $a \neq -a$ ovvero che $-1 \neq 1$. Le due condizioni sono chiaramente soddisfatte se e solo se $p \equiv 1 \bmod 4$.

Esercizio 6. Sia $p(x) = x^8 - 3x^4 - 4 \in \mathbb{Q}[x]$.

1. Determinare il campo di spezzamento K di $p(x)$ su $\mathbb{Q}$.
2. Determinare il gruppo di Galois di $p(x)$.
3. Descrivere il reticolo dei campi intermedi dell'estensione $K/\mathbb{Q}$.

Risoluzione:$x^8 - 3x^4 - 4 = (x^2 - 2)(x^2 + 2)(x^4 + 1)$

Il polinomio $x^4 + 1$ ha le 4 radici $(\sqrt{2}/2)(\pm 1 \pm i)$. Il polinomio $x^2 - 2$ ha radici $\pm\sqrt{2}$. Il polinomio $x^2 + 2$ ha radici $\pm i\sqrt{2}$.

Dunque il campo di spezzamento K del nostro polinomio è $K = \mathbb{Q}(i, \sqrt{2})$. Esso ha grado 4 e almeno 3 sottocampi di grado 2, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(i\sqrt{2})$. Il gruppo di Galois contiene almeno 3 elementi distinti di ordine 2. È dunque il gruppo di Klein $\mathbb{Z}/2 \times \mathbb{Z}/2$.

K ha 5 sottocampi.
$\mathbb{Q}$ di grado 1.
$\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$ di grado 2.
K di grado 4.

Per l'esame da 9 crediti

Esercizio 7. Sia p un primo. Determinare il numero dei sottogruppi di $\mathbb{Z}/p \times \mathbb{Z}/p$.

Risoluzione: $\mathbb{Z}/p \times \mathbb{Z}/p$ è uno spazio vettoriale di dimensione 2 sul campo primo $\mathbb{Z}/p$.

I suoi sottogruppi sono i suoi sotto spazi. Dunque possono avere dimensione 0,1,2

Dimensione 0. $\{0\}$.

Dimensione 1. Si tratta di un sottogruppo che consiste dei multipli di un elemento non nullo in $\mathbb{Z}/p \times \mathbb{Z}/p$. Ci sono $p^2 - 1$ elementi non nulli e nel sottogruppo generato da uno di essi $p - 1$ elementi non nulli. Dunque ci sono $(p^2 - 1)/(p - 1) = p + 1$ sottospazi di dimensione 1.

Dimensione 2. $\mathbb{Z}/p \times \mathbb{Z}/p$.

Conclusione: $\mathbb{Z}/p \times \mathbb{Z}/p$. ha $p + 3$ sottogruppi.