Primo compito

Esercizio 1. Siano a, b, c, m interi non-negativi e $d := mcd(c, m)$. Provare che

$$ac \equiv bc \mod m \iff a \equiv b \mod k,$$

dove $m = kd$.

Sia $c = \alpha d$. Supponiamo $a \equiv b \mod k$; allora $a-b = rk$, quindi $(a-b)c = rck = rk\alpha d = r\alpha m$ e dunque $ac \equiv bc \mod m$.

Viceversa se $ac \equiv bc \mod m$, allora $a \equiv b \mod \frac{m}{mcd(m,c)}$. Ma $\frac{m}{mcd(m,c)} = \frac{m}{d} = k$, come volevasi.

Esercizio 2. Determinare al variare del parametro intero positivo k la risolubilità del sistema di congruenze

$$\begin{cases} x \equiv k \mod 14 \\ 6x \equiv 1 \mod 35 \end{cases}$$

Risolvere il sistema per i valori di k determinati precedentemente.

Moltiplicando la seconda equazione per 6 e usando il fatto che $36 = 35+1$, il sistema può riscriversi

$$\begin{cases} x \equiv k \mod 2 \\ x \equiv k \mod 7 \\ x \equiv 6 \mod 7 \\ x \equiv 6 \mod 5 \end{cases}$$

Dunque è necessario che $k \equiv 6 \mod 7$. In tale ipotesi il sistema si riduce a

$$\begin{cases} x \equiv k \mod 2 \\ x \equiv 6 \mod 7 \\ x \equiv 6 \mod 5 \end{cases}$$

che è un sistema cinese che ammette sempre soluzione unica $\mod 70$. Con i soliti metodi si trova la soluzione $x = 35k + 6 \mod 70$. In definitiva si ottengono le soluzioni $6, 41$.

Esercizio 3. Dimostrare che un gruppo di ordine 80 non è semplice.

Sia n_p il numero dei p-Sylow di G. Osserviamo che $80 = 2^4 \cdot 5$. Dai teoremi di Sylow $n_5 \equiv 1 \mod 5$ e $n_5|16$. Queste considerazioni implicano $n_5 = 1$, e il 5-Sylow è normale, o $n_5 = 16$. In quest'ultimo caso, dal momento che due 5-Sylow si intersecano banalmente e hanno ciascuno quattro

elementi di ordine 5*, deduciamo che* G *ha* 64 *elementi di ordine* 5*. I rimanenti* 16 *elementi costituiscono il* 2*-Sylow, che è unico e quindi normale.*

Esercizio 4. Sia A anello commutativo unitario e J ideale di A. Provare che $\sqrt{J} = \{x \in A \mid \exists n \in \mathbb{N} : x^n \in J\}$ è un ideale contenuto nell'intersezione di tutti gli ideali primi contenenti J.

Mostriamo che $\sqrt{J}$ *è un ideale: se* $x, y \in \sqrt{J}$*, allora esistono* n, m *tali che* $x^n \in J, y^m \in J$*. Ma allora*

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k} \in J$$

perché ogni termine a secondo membro appartiene a J*, dato che uno dei due esponenti è maggiore uguale a* $\min(n, m)$*. Infine, se* $a \in A$*,* $(ax)^n = a^n x^n \in J$*.*

Sia $x \in \sqrt{J}$ *e* P *un ideale primo contenente* J*. Dobbiamo dimostrare che* $x \in P$*. Per definizione esiste* n *tale che* $x^n \in J \subset P$*; scegliamo tale* n *minimo. Se* $n = 1$ *abbiamo concluso; altrimenti* $x^n = xx^{n-1} \in P, x \notin P, x^{n-1} \notin P$ *contro la primalità di* P*.*

Esercizio 5. Determinare il campo di spezzamento K_i del polinomio $f(x) = x^4 - 5$ su $F_1 = \mathbb{Q}$ e su $F_2 = \mathbb{Z}_3$. Determinare poi $Gal(K_i/F_i), i = 1, 2$.

In $K_1[x]$ *risulta* $f(x) = (x - \sqrt[4]{5})(x + \sqrt[4]{5}))(x - i\sqrt[4]{5}))(x + i\sqrt[4]{5}))$*, pertanto* $K_1 = \mathbb{Q}(\sqrt[4]{5}, i)$ *e* $[K_1 : F_1] = 8$*. Essendo un sottogruppo transitivo di* S_4 *di ordine* 8*,* $Gal(K_1/F_1)$ *è necessariamente il gruppo diedrale* D_4*.*

In $F_2[x]$ *risulta* $f(x) = (x^2 + x - 1)(x^2 - x - 1)$*. Entrambi i fattori di* $f(x)$ *sono irriducibili su* $\mathbb{Z}_3$ *(hanno grado 2 e non hanno radici). Il campo si spezzamento di* f *si ottiene da* F_2 *aggiungendo una qualsiasi radice, ed è quindi il campo* $\mathbb{F}_9$ *con nove elementi. Corrispondentemente* $Gal(K_2/F_2)$ *è ciclico di ordine* 2*.*

Esercizio 6. Sia p un numero primo. Si consideri l'anello quoziente $\mathbb{Z}_p[x]/(x^2+1)$. Per quali p esso è un campo ?

Se $p = 2$*, allora* $x^2 + 1 = (x+1)^2$ *e il quoziente ha divisori di zero. Sia* p *un primo dispari; dobbiamo stabilire quando* $x^2 + 1$ *non ha radici in* $\mathbb{Z}_p[x]$*. Consideriamo il gruppo moltiplicativo* $\mathbb{Z}_p^\times$*. Se* $x \in \mathbb{Z}_p^\times$ *verifica* $x^2 = -1$*, allora* $x^4 = 1$*; dunque* x *ha ordine* 4 *e quindi* $4|p - 1 = |\mathbb{Z}_p^\times|$*. Pertanto, se* $p \equiv 3 \mod 4$ *il polinomio* $x^2 + 1$ *è irriducibile. Se invece* $p \equiv 1 \mod 4$*, allora il gruppo* $|\mathbb{Z}_p^\times|$ *è ciclico di ordine* $p - 1 = 4h$ *e dunque contiene un elemento di ordine 4.*