Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2010/2011
AL210 - Algebra 2: Gruppi, Anelli e Campi
Prof. F. Pappalardi
Tutorato 12 - Gennaio 2011
Tutore: Matteo Acclavio
www.matematica3.com

Esercizio 1.
Sia R un anello commutativo ed unitario. Siano I, J due suoi ideali.
Sia $I+J := \{x+y \text{ con } x \in I, y \in J\}$. Sia $\phi : R \longrightarrow R/I \times R/J$, l'applicazione definita come $\phi(r) := (r+I, r+J)$ per ogni $r \in R$.

- Si dimostri che $I + J$ è un ideale di R.
- Si dimostri che ϕ è un omomorfismo unitario di anelli.
- Si dimostri che ϕ è suriettivo se e solo se $I + J = R$.
- Si dimostri che il nucleo di ϕ è $I \cap J$.
- Nel caso $R = \mathbb{Z}$, $I = 5\mathbb{Z}$, $J = 12\mathbb{Z}$, si dimostri che $\mathbb{Z}/60\mathbb{Z} = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

Esercizio 2.

(a) Quali elementi del campo $\mathbb{Z}_7$ sono quadrati perfetti? (Cioè quali elementi $q \in \mathbb{Z}_7$ sono tali che l'equazione $X^2 = q$ ha soluzione in $\mathbb{Z}_7$?).

(b) Dedurre da **(a)** per quali valori $a \in \mathbb{Z}_7$ si ha che $\mathbb{Z}_7[X]/(X^2 + a)$ è un campo;

(c) Determinare l'inverso del generico elemento di $\mathbb{Z}_7[X]/(X^2 + 4)$;

(d) Determinare i divisori dello zero in $\mathbb{Z}_7[X]/(X^2 + 3)$.

Esercizio 3.
Sia A l'insieme dei numeri complessi del tipo $a + ib\sqrt{5}$, con $a, b \in \mathbb{Z}$.

- Provare che A è un sottoanello di $\mathbb{C}$.
- Stabilire se A è un sottocampo di $\mathbb{C}$.
- Provare che $I = \{a + ib\sqrt{5} \mid a, b \in 2\mathbb{Z}\}$ è un ideale di A, ma non è un ideale primo di A.
- Provare che $J = \{a + ib\sqrt{5} \mid a \in 5\mathbb{Z}\}$ è un ideale massimale di A.

Esercizio 4.
Sia A anello commutativo unitario che ammette (per ogni suo elemento non nullo) una fattorizzazione in irriducibili, le seguenti sono equivalenti

(a) la fattorizzazione è essenzialemente unica (a meno dell'ordine dei fattori e di invertibili)

(b) $\forall a, b \in A \; \exists MCD(a, b)$

(c) $p \in A, p \; irriducibile \Rightarrow p \; primo$