Esercizi di riepilogo: Teoria degli anelli e dei campi.

1. Sia A un anello commutativo con unità. Supponiamo che $\forall a \in A$ esista $n \in \mathbb{N}$, $n > 1$ (dipendente da a) tale che $a^n = a$. Dimostrare che un ideale I di A è primo $\iff$ è massimale.

2. Sia $\varphi : A \longrightarrow A'$ un omomorfismo di anelli. Sia P' un ideale primo di A' e sia $\varphi^{-1}(P') = \{\, a \in A \,:\, \varphi(a) \in P' \,\}$.
Dimostrare che $\varphi^{-1}(P')$ è un ideale primo di A.
Se P' è massimale è sempre vero che $\varphi^{-1}(P')$ è massimale in A ?

3. Sia $\mathbb{Z}[i]$ l'anello degli *interi di Gauss*. Sia $I \neq 0$ un ideale di $\mathbb{Z}[i]$. Dimostrare che $\mathbb{Z}[i]/I$ ha cardinalità finita.

4. Sia $M(\mathbb{N}, \mathbb{Z}) = \{\, f \,:\, \mathbb{N} \longrightarrow \mathbb{Z} \,\}$ l'insieme delle funzioni da $\mathbb{N}$ in $\mathbb{Z}$ con le operazioni indotte da $\mathbb{Z}$, cioè

$$(f+g)(n) = f(n) + g(n) \qquad\qquad (fg)(n) = f(n)g(n) \quad \forall n \in \mathbb{N}\,.$$

a) Dimostrare che $M(\mathbb{N}, \mathbb{Z})$ è un anello commutativo con unità.

b) Dimostrare che $M(\mathbb{N}, \mathbb{Z})$ non è un dominio di integrità.

c) Descrivere gli insiemi dei divisori di zero e degli elementi invertibili di $M(\mathbb{N}, \mathbb{Z})$. Dimostrare che nessuno dei due è un ideale di $M(\mathbb{N}, \mathbb{Z})$.

d) Per ogni sottoinsieme X di $\mathbb{N}$ definiamo

$$I(X) = \{\, f \in M(\mathbb{N}, \mathbb{Z}) \,:\, f(x) = 0 \ \forall x \in X \,\}\,.$$

Dimostrare che $I(X)$ è un ideale di $M(\mathbb{N}, \mathbb{Z})$.

e) Dimostrare che se $I(X)$ è primo allora X ha al più un elemento.

f) $I(\{0\})$ è primo ? $I(\{0\})$ è massimale ?

5. Sia $M(\mathbb{N}, \mathbb{R})$ definito in maniera analoga ad $M(\mathbb{N}, \mathbb{Z})$ dell'esercizio precedente. Rispondere alle stesse domande **a**)$, \ldots,$ **f**) dell'esercizio precedente per l'insieme $M(\mathbb{N}, \mathbb{R})$, verificando inoltre che ogni elemento di $M(\mathbb{N}, \mathbb{R})$ o è un divisore dello zero o è invertibile.

6. Sia

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathcal{M}(2, \mathbb{Q}) \right\}\,.$$

a) Dimostrare che A è un anello commutativo con unità.

b) Trovare A^* e l'insieme dei divisori dello zero.

c) Dimostrare che $A \simeq \mathbb{Q}[X]/(X^2)$.

7. Sia
$$A = \mathbb{Q}[X]/(X^5 - 2X^4 + X^3 + 2X^2 - 4X + 2) .$$

a) Trovare l'ideale dei nilpotenti di A. È un ideale primo ?

b) Trovare l'insieme dei divisori dello zero e dimostrare che non è un ideale.

8. Sia $P(X) = X^4 + 3X + 1 \in \mathbb{Q}[X]$.

a) Dimostrare che $A = \mathbb{Q}[X]/(P)$ è un campo.

b) Sia α una radice di P. Trovare l'inverso di $\alpha^2 + 1$ in $\mathbb{Q}(\alpha)$.

9. Sia $P(X) = X^4 + 3X + 1$.

a) Rispondere alle stesse domande dell'esercizio precedente considerando P come polinomio in $\mathbb{F}_2[X]$.

b) Dimostrare che $\mathbb{F}_3[X]/(P)$ e $\mathbb{F}_5[X]/(P)$ non sono campi.

10. Sia $S = \{\, P(X) \in \mathbb{Q}[X] \;:\; P(0) \neq 0 \text{ e } P(1) \neq 0 \,\}$.

a) Dimostrare che S è un sistema moltiplicativo.

b) Trovare gli ideali primi di $S^{-1}\mathbb{Q}[X]$.

11. Sia $P(X) = X^2 + 2$.

a) Dimostrare che $\mathbb{F}_7[X]/(P)$ è un campo.

b) Sia α una radice di P. Calcolare l'ordine di $\alpha + 1$ in $(\mathbb{F}_7(\alpha))^*$.

c) Calcolare l'inverso di $\alpha + 1$ in $\mathbb{F}_7(\alpha)$.

d) Rispondere alle domande **b)** e **c)** per altri elementi $a + \alpha b \in (\mathbb{F}_7(\alpha))^*$ scelti a piacere.

e) Per quali $a \in \mathbb{F}_7$ l'anello $\mathbb{F}_7[X]/(X^2 - a)$ è un campo ?

12. Sia $\zeta_n = e^{\frac{2\pi i}{n}}$ $(n \geq 1)$ una radice primitiva n-esima dell'unità e sia $\Phi_n(X)$ il suo polinomio minimo in $\mathbb{Q}(X)$.

a) Scrivere $\Phi_1(X)$, $\Phi_2(X)$, $\Phi_3(X)$ e $\Phi_4(X)$.

b) Calcolare $\Phi_p(X)$ per ogni primo p.

c) Dimostrare che

$$\prod_{d|n} \Phi_d(X) \quad \text{divide} \quad X^n - 1 \ .$$

d) Dimostrare che $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ dove ϕ e la *phi* di Eulero. (Sugg. induzione)

13. Sia K un campo, sia H un sottogruppo di $Aut(K)$ (gli automorfismi di K) e sia F un sottocampo di K.

a) Sia $K^H = \{\, \alpha \in K \ : \ \sigma(\alpha) = \alpha \ \forall \sigma \in H \,\}$. Dimostrare che K^H è un sottocampo di K.

b) Sia $G_F = \{\sigma \in Aut(K) \ : \ \sigma(\alpha) = \alpha \ \forall \alpha \in F\}$. Dimostrare che $G_F < Aut(K)$.