Algebra I. 12. Radice primitiva, anelli quoziente, CRT, PID. Roma, 10 dicembre 2022.

1. (a) Determinare una radice primitiva $\overline{g}$ in $\mathbf{Z}_{13}^*$.
   (b) Sia g la radice primitiva modulo 13 calcolata nella parte (a). Calcolare $m \in \mathbf{Z}$ tale che $\overline{10} = \overline{g}^m$ in $\mathbf{Z}_{13}^*$.
   (c) Stesse domande per il primo 41 invece di 13.
2. Il numero 641 è primo. Quante radici primitive ci sono in $\mathbf{Z}_{641}^*$?
3. (a) Dimostrare che la mappa $\Psi : \mathbf{Z}[X] \longrightarrow \mathbf{Z}_2$ data da $\Psi(f) = f(0) \pmod 2$ è un omomorfismo suriettivo di anelli.
   (b) Dimostrare che $\ker(\Psi)$ è l'ideale $(2, X)$ (l'ideale generato da 2 e da X).
   (c) Dimostrare che l'anello $\mathbf{Z}[X]/(2, X)$ è isomorfo a $\mathbf{Z}_2$.
4. Sia $p > 2$ un primo.
   (a) Dimostrare che l'anello $\mathbf{Z}_p[X]/(X^2 - 1)$ è isomorfo a $\mathbf{Z}_p \times \mathbf{Z}_p$.
   (b) Dimostrare che l'affermazione della parte (a) è falsa per $p = 2$.
5. Sia R un anello commutativo e sia $I \subset R$ un ideale. Dimostrare che l'applicazione
$$\{\text{ideali di } R \text{ che contengono } I\} \longrightarrow \{\text{ideali di } R/I\}$$
data da $J \mapsto \{\overline{x} \in R/I : x \in J\}$ è una biiezione ben definita.
6. (a) Sia A un dominio. Dimostrare che il gruppo $A[X]^*$ degli elementi invertibili dell'anello dei polinomi $A[X]$ consiste nei polinomi costanti non nulli ed è isomorfo al gruppo A^*.
   (b) Sia k un campo e sia $f \in k[X]$ non nullo. Dimostrare che $f = cg$ con $c \in k^*$ e $g \in k[X]$ monico.
   (c) Far vedere che l'affermazione della parte (b) è falsa per l'anello $\mathbf{Z}$ invece di k.
7. Sia k un campo. Un polinomio $f \in k[X]$ si dice irriducibile, se non è costante e se non è prodotto di due polinomi non costanti in $k[X]$.
   (a) Dimostrare che ogni polinomio di grado 1 è irriducibile.
   (b) Dimostrare che ogni polinomio in $k[X]$ è prodotto di polinomi irriducibili.
   (c) Dimostrare che $k[X]$ contiene infiniti polinomi irriducibili monici.
   (d) Sia $f \in k[X]$ irriducibile e sia $g \in k[X]$. Dimostrare che se f non divide g, allora $\mathrm{mcd}(f, g) = 1$, cioé l'ideale generato da f e g è uguale a $k[X]$.
   (e) Sia $f \in k[X]$ irriducibile e siano $g, h \in k[X]$. Dimostrare: se f divide gh, allora f divide g oppure f divide h.
   (f) Dimostrare che se f è irriducibile, allora l'anello quoziente $k[X]/(f)$ è un campo.
8. Sia R l'insieme delle successioni $(a_k)_{k=1}^{\infty}$ con $a_k \in \mathbf{Q}$, con somma e prodotto definiti come segue: $(a_k)_{k=1}^{\infty} + (b_k)_{k=1}^{\infty} = (a_k + b_k)_{k=1}^{\infty}$ e $(a_k)_{k=1}^{\infty} \cdot (b_k)_{k=1}^{\infty} = (a_k b_k)_{k=1}^{\infty}$. Sia
$$S = \{(a_k)_{k=1}^{\infty} \in R : \forall \epsilon \in \mathbf{Q}_{>0}\ \exists k \geq 1 \text{ tale che } |a_i - a_j| < \epsilon \text{ per ogni } i, j > k\}.$$
Sia
$$I = \{(a_k)_{k=1}^{\infty} \in R : \forall \epsilon \in \mathbf{Q}_{>0}\ \exists k \geq 1 \text{ tale che } |a_i| < \epsilon \text{ per ogni } i > k\}.$$
   (a) Dimostrare che R è un anello commutativo.
   (b) Dimostrare che S è un sottoanello di R.
   (c) Dimostrare che I è un ideale di S.
   (d) Chi è l'anello quoziente S/I?