1) Sia A un anello commutativo e siano $\mathfrak{a}$, $\mathfrak{b}, \mathfrak{c}$ ideali di A.

   a) Dimostrare che $\mathfrak{a} + \mathfrak{b} := \{x + y \colon x \in \mathfrak{a}, y \in \mathfrak{b}\}$ è l'ideale generato dall'insieme $\mathfrak{a} \cup \mathfrak{b}$.

   b) Dimostrare che l'ideale $\mathfrak{ab} := \langle xy \colon x \in \mathfrak{a}, x \in \mathfrak{b} \rangle$ è uguale al seguente insieme:

$$\left\{ \sum_{i=1}^{m} x_i y_i \colon m \in \mathbb{N},\ x_i \in \mathfrak{a},\ y_i \in \mathfrak{b} \right\}.$$

   c) Dimostrare che il prodotto di ideali è distributivo rispetto alla somma, ovvero:

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}\,.$$

   d) Dimostrare che se $\mathfrak{a} + \mathfrak{b} = (1)$ allora $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

2) Sia A un anello commutativo e sia $\mathfrak{m} \subset A$ un ideale massimale. Dimostrare che le seguenti affermazioni sono equivalenti:

   (*i*) $(A, \mathfrak{m})$ è un anello locale.

   (*ii*) Ogni elemento di $A \setminus \mathfrak{m}$ è invertibile.

   (*iii*) Ogni elemento dell'insieme $1 + \mathfrak{m} := \{1 + x \colon x \in \mathfrak{m}\}$ è invertibile.

   Inoltre si analizzi l'implicazione (*ii*) $\Rightarrow$ (*i*). È necessario assumere a priori che $\mathfrak{m}$ sia massimale?

3) Si consideri l'insieme di tutte le coppie (U, f) dove $U \subseteq \mathbb{R}$ è un intorno aperto di 0 e $f : U \to \mathbb{R}$ è continua (su U). Definiamo la seguente relazione:

$$(U, f) \sim (V, g) \Leftrightarrow \exists (W, h) \text{ t.c. } W \subseteq U \cap V,\ h = f_{|W} = g_{|W}$$

   Verificare che $\sim$ è una relazione di equivalenza. Dimostrare che l'insieme quoziente (con le opportune operazioni di somma e prodotto di funzioni) è un anello locale e descrivere esplicitamente l'unico ideale massimale. Cosa cambia se invece di considerare intorni di 0, si considerano intorni di un punto fissato $x \in \mathbb{R}$? Cosa succede se eliminiamo l'ipotesi di continuità sulle funzioni?

4) Sia A un anello commutativo.

   a) Dimostrare che l'insieme $N(A)$ degli elementi nilpotenti di A forma un ideale di A tale che $A/N(A)$ non contiene elementi nilpotenti oltre lo 0.

   b)* Dimostrare che $N(A)$ è l'intersezione di tutti gli ideali primi di A.

   c) Dimostrare che se $x \in N(A)$ allora $1 + x$ è invertibile.

5) Sia $R_m = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Z}/m\mathbb{Z} \right\}$:

   a) Dimostrare che R_m è un sottoanello di $M_2(\mathbb{Z}/m\mathbb{Z})$.

   b) Sia $m = 7$. Verificare che $I = \left\{ \begin{pmatrix} 3k & k \\ 2k & 3k \end{pmatrix} : k \in \mathbb{Z}/7\mathbb{Z} \right\}$ è un ideale di R_7. R_7 è un campo?

   c) Stabilire se R_5 è un campo.

6) Sia A un anello commutativo e sia $J(A)$ l'intersezione di tutti gli ideali massimali di A. Dimostrare che $x \in J(A)$ se e solo se $1 - xy$ è invertibile per ogni $y \in A$.

7) Sia $f : A \to B$ un omomorfismo di anelli commutativi. Sia $\mathfrak{b}$ un ideale di B e sia $\mathfrak{a}$ un ideale di A.

   a) Dimostrare che $f^{-1}(\mathfrak{b})$ è un ideale di B.

   b) Giustificare tramite un controesempio che in generale $f(\mathfrak{a})$ non è un ideale di B.

   Inoltre, dimostrare o confutare le seguenti affermazioni:

   c) Se $\mathfrak{b}$ è primo, allora $f^{-1}(\mathfrak{b})$ è primo.

   d) Se $\mathfrak{a}$ è primo, allora $\langle f(\mathfrak{a})\rangle$ è primo.

8) Dimostrare che $\mathbb{Q}$ ed $\mathbb{R}$ non sono isomorfi come campi.

9) Sia A un anello commutativo unitario tale che $x^2 = x$ per ogni $x \in A$. Dimostrare che:

   a) $2x = 0$ per ogni $x \in A$.

   b) Un ideale di A è primo se e solo se è massimale. Inoltre se $\mathfrak{m}$ è un ideale massimale allora $A/\mathfrak{m} = \mathbb{F}_2$.

10) (Teorema Cinese del resto):

a) Sia A un anello commutativo e siano $\mathfrak{a}, \mathfrak{b} \subset A$ due ideali propri e coprimi, dimostrare che $A/(\mathfrak{a} \cap \mathfrak{b}) \cong A/\mathfrak{a} \times A/\mathfrak{b}$.

b) Sia m un intero positivo e sia $m = p_1^{i_1} \dots p_n^{i_n}$ la sua fattorizzazione in numeri primi. Dimostrare che $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{i_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{i_n}\mathbb{Z}$.

c) Sia m un intero positivo come nel caso *b*), dimostrare che il sistema:

$$\begin{cases} x \equiv a_1 \pmod{p_1^{i_1}} \\ x \equiv a_2 \pmod{p_2^{i_2}} \\ \vdots \\ x \equiv a_n \pmod{p_n^{i_n}} \end{cases}$$

ammette una soluzione in $\mathbb{Z}$ che è unica modulo m.

11) Siano A e B due anelli. Dimostrare che:

   a) se A_1 e B_1 sono sottoanelli di A e B rispettivamente, allora $A_1 \times B_1$ è sottoanello di $A \times B$.

   b) se I e J sono ideali (sinistri, destri o bilateri) di A e B rispettivamente, allora anche $I \times J$ è un ideale (sinistro, destro o bilatero) di $A \times B$; se I e J sono ideali bilateri, si ha $(A \times B)/(I \times J) \cong (A/I) \times (B/J)$.

12) Sia $A_1 \times A_2$ il prodotto diretto di due anelli A_1 e A_2. Si provi che

   a) $(A_1 \times A_2, +, \cdot)$ è un anello commutativo se e solo se A_1 e A_2 sono commutativi.

   b) $U(A_1 \times A_2) = U(A_1) \times U(A_2)$.

   c) Calcolare $U(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$, $U(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z})$, $U(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z})$.

   d) Determinare gli ideali di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

   e) Sia $\mathfrak{p}$ un ideale primo di $A_1 \times A_2$. Allora $\mathfrak{p} = \mathfrak{p}_1 \times A_2$ oppure $\mathfrak{p} = A_1 \times \mathfrak{p}_2$, dove $\mathfrak{p}_i$ è un ideale primo di A_i $(i = 1, 2)$.

   f) Sia $\mathfrak{m}$ un ideale massimale di $A_1 \times A_2$. Allora $\mathfrak{m} = \mathfrak{m}_1 \times A_2$ oppure $\mathfrak{m} = A_1 \times \mathfrak{m}_2$, dove $\mathfrak{m}_i$ è un ideale massimale di A_i $(i = 1, 2)$.

g) Sia K un campo e $A = K \times K \times \cdots \times K$ (n fattori). Quali sono gli ideali primi di A? Quali sono gli ideali massimali di A?

13) Sia $A = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

a) Trovare la caratteristica di A.

b) Descrivere gli ideali di A, in particolare determinare gli ideali primi e quelli massimali. Determinare se esistono ideali non principali.

c) Determinare a quali dei seguenti anelli è isomorfo l'anello A:

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}, \quad \mathbb{Z}/60\mathbb{Z}$$

d) Descrivere quali sono gli elementi invertibili e gli elementi nilpotenti di A.

14) Nell'anello $A = \mathbb{Z}[\sqrt{2}]$ si consideri l'ideale $I = (2)$. Stabilire se l'anello quoziente A/I è un campo.

15) Nell'anello $A = \mathbb{Z}[\sqrt{5}]$, sia $I = (5)$. Studiare l'anello quoziente A/I:

a) provare che se $a \equiv 0 \bmod 5$, allora l'elemento $a + b\sqrt{5} + I$ è nilpotente;

b) provare che se $a \not\equiv 0 \bmod 5$, allora l'elemento $a + b\sqrt{5} + I$ è invertibile;

c) quali sono gli ideali di A/I?

16) Sia $A = \mathbb{Z}[\sqrt{5}]$. Per $\alpha = x + \sqrt{5}y \in A$ definiamo la norma di α con $N(\alpha) = x^2 - 5y^2$. Sia $I = \{\alpha \in A : N(\alpha) \text{ pari}\}$. Dire se I è ideale di A, e in caso affermativo, dire se I è massimale.

17) Sia A un anello commutativo; sia $f \in A[X]$ con coefficiente direttivo invertibile e di grado $n > 0$.

a) Dimostrare dato l'ideale principale $I = (f)$, esiste una biezione fra $A[X]/I$ e l'insieme delle classi laterali $I + r$ tali che $\deg(r) < n$.

b) Calcolare la cardinalità dei seguenti anelli: $\mathbb{F}_2[X]/(X^3 + X + 1)$, $\mathbb{F}_3[X]/(X^2 - 1)$, $\mathbb{F}_5[X]/(X^6 - X^2 + X - 1)$

18) Sia A un dominio. Dimostrare che $U(A) = U(A[X])$. Resta vera tale uguaglianza se A non è un dominio?

PSL

19) Sia $\varphi : A \to B$ un isomorfismo di anelli commutativi, e sia $\widetilde{\varphi} : A[X] \to B[X]$ la sua naturale estensione. Sia inoltre $f \in A[X]$; dimostrare che $A[X]/(f)$ è isomorfo a $B[X]/(\widetilde{\varphi}(f))$.

20) Dimostrare che se A è un dominio a fattorizzazione unica e $p \in A$ è un primo, allora p è un primo in $A[X]$.

21) Dimostrare che un ideale massimale di $\mathbb{Z}[X]$ non può essere principale.

22) Sia $g \in \mathbb{Z}[X]$ tale che $g = hf$ con $f \in \mathbb{Z}[X]$ primitivo e $h \in \mathbb{Q}[X]$. Dimostrare che $h \in \mathbb{Z}[X]$.

23) Sia $f : A \to B$ un omomorfismo di anelli commutativi. Dimostrare o confutare le seguenti affermazioni:

a) f è suriettiva se e solo se esiste un omomorfismo $g : B \to A$ tale che $f \circ g = \mathrm{id}$.

b) f è iniettiva se e solo se esiste un omomorfismo $h : B \to A$ tale che $h \circ f = \mathrm{id}$.

24)* Sia A un anello commutativo e si consideri l'anello dei polinomi $A[X]$. Si dimostri che un elemento $a_0 + a_1X + \dots a_nX^n \in A[X]$ è invertibile se e solo se a_0 è invertibile e inoltre a_i è nilpotente per ogni $i = 1, \dots n$.
[Oss: confrontare con l'esercizio 18.]

25) Sia A un anello commutativo e si consideri l'anello delle serie formali $A[[X]]$. Si dimostri che un elemento $a_0 + a_1X + \dots \in A[[X]]$ è invertibile se e solo se a_0 è invertibile.

26) Fattorizzare $X^p - 1$ in $\mathbb{Z}[X]$.

27) Dimostrare che $f(X, Y) = X^2 + Y^2 - 1 \in \mathbb{Q}[X, Y]$ è irriducibile in $\mathbb{Q}[X, Y]$.

28) Sia A un dominio a ideali principali (PID) e sia $a \in A$ un elemento tale che esiste un primo $p \in A$ con le seguenti proprietà $p \mid a$ e $p^2 \nmid a$. Dimistrare che $X^p + a$ è irriducibile in $A[X]$ per ogni $n > 0$.

29) Dimostrare che i seguenti polinomi sono irriducibili in $\mathbb{Q}[X]$:

$$f(X) = X^4 + 830X^3 + 1002X^2 + 213X + 71,$$
$$g(X) = X^4 + X^3 + 2X^2 + X + 4.$$

30) Dimostrare che $X^4 + X^3 + X + 1$ è irriducibile in $K[X]$, dove K è un campo qualsiasi.

31) Sia K un campo. Dimostrare che se $f \in K[X]$ e $a \in K$, allora $f(X) \equiv f(a) \mod (X - a)$.

32) Sia $f(X) = X^3 - 3X + 1$. Verificare che $f(X)$ è irriducibile in $\mathbb{Q}[X]$. Sia α una radice complessa di $f(X)$, esprimere $(2\alpha^2 - \alpha - 4)^2$ come combinazione lineare di $1, \alpha, \alpha^2$.

33) Dimostrare che due polinomi a coefficienti in $\mathbb{Z}$ sono relativamente primi in $\mathbb{Q}[X]$ se e solo se l'ideale che essi generano contiene un intero non nullo.

34) Sia K è un'estensione di un campo F, provare che $[K : F] = 1$ se e solo se $K = F$.

35) Mostrare che $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$.

36) Sia K un'estensione di un campo F tale che $[K : F] = p$ con p primo, dimostrare che non ci sono campi intermedi tra K ed F.

37) Sia K un'estensione di un campo F e sia inoltre $a \in K$ tale che $[F(a) : F]$ è un numero dispari. Mostrare che $F(a) = F(a^2)$ e dare inoltre un esempio di come ciò in generale è falso se il grado di $F(a)$ su F è pari.

38) Mostrare che $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ non sono isomorfi come campi ma sono isomorfi come spazi vettoriali su $\mathbb{Q}$.

39) Sia $\mathbb{A}$ la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{C}$. Dimostrare che $[\mathbb{A} : \mathbb{Q}] = \infty$.

40) Sia $f(X) \in F[X]$ un polinomio irriducibile di grado n, e sia K un'estensione di F con $[K : F] = m$. Se $(m, n) = 1$, mostrare che $f(X)$ è irriducibile in $K[X]$.

41) Sia $K(X)$ il campo delle funzioni razionali sul campo K e sia M un sottocampo di $K(X)$ contenente K. Provare che o $M = K$ oppure $K(X)$ ha dimensione finita su M.

42) Sia K il campo di spezzamento di un insieme S di polinomi a coefficienti in F. Sia inoltre L un campo tale che $F \subseteq L \subseteq K$; se ogni polinomio $f \in S$ si spezza in L, dimostrare che $L = K$.

43) Se $F \subseteq L \subseteq K$ sono campi, e K è il campo di spezzamento di $S \subseteq F[X]$ (su F), mostrare che K è il campo di spezzamento di S su L.

44) Costruire i seguenti campi:

   a) Un campo con 3125 elementi.

   b) Un campo infinito di caratteristica maggiore di 0.

45) Si consideri il polinomio $f(X) = X^4 + 1$.

   a) Si dimostri che f è irriducibile su $\mathbb{Q}$.

   b) Si dimostri che $K = \mathbb{Q}[X]/(f)$ è un campo. Dare inoltre una descrizione di K (generatori, grado su $\mathbb{Q}$...).

   c) Si considerino i polinomi $X^2 + 1$ e $X^2 - 2$ in $K[X]$. Dire, motivando la risposta, quale fra essi è irriducibile su K.

46) Si consideri il polinomio $X^3 - 2 \in K[X]$. Si descriva il suo campo di spezzamento (su K) quando $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}(i)$, $\mathbb{C}$.

47) Sia K un campo di caratteristica 0 e sia $f \in K[X]$ un polinomio irriducibile. Mostrare che f ha radici tutte distinte nel suo campo di spezzamento. Tale affermazione rimane vera in caratteristica p?

48) Sia K un campo e sia $f \in \mathrm{Aut}(K)$. Mostrare che f fissa punto per punto il sottocampo fondamentale di K.

Esercizi di fine corso annuale (I)

1) Si fissi $n \geq 3$. Sia $\sigma = (i_1 i_2 \dots i_k) \in S_n$. Provare che per ogni $\theta \in S_n$ si ha $\theta\sigma\theta^{-1} = (\theta i_1 \theta i_2 \dots \theta i_k)$. Dimostrare inoltre che il centro di S_n è banale.

2) Sia G un gruppo di ordine $|G| = p_1 p_2 p_3$ dove i p_i sono numeri primi tali che $p_1 < p_2 < p_3$. Dimostrare che G possiede un Sylow normale.

3) Dare un esempio esplicito di un omomorfismo iniettivo non unitario di anelli $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}$. Che succede se richiediamo che $f(1) = 1$?

4) Sia $f(X) = X^4 + qX^2 + rX + s$ un polinomio a coefficienti in un campo K. Dimostrare che possiamo scrivere

$$f(X) = (X^2 + aX + b)(X^2 + a'X + b') \in K'[X]$$

dove K' è un'estensione di K se e solo se a^2 è soluzione dell'equazione:

$$T^3 + 2qT^2 + (q^2 - 4s)T - r^2 = 0$$

5) È ben noto che e e π sono trascendenti, ma non è ancora noto se $e\pi$ ed $e + \pi$ sono trascendenti. Dimostrare che almeno uno fra $e\pi$ ed $e + \pi$ è trascendente.

Esercizi di fine corso annuale (II)

1) Sia p un primo dispari; dimostrare che se q è un primo che divide $2^p - 1$, allora $q = 2kp + 1$ con $k \in \mathbb{N}$. Dedurre una dimostrazione dell'infinità dei numeri primi.

2) Dimostare le seguenti affermazioni:

   a) Sia p un primo; un gruppo finito di ordine p^2 è abeliano.

   b) Un gruppo finito ha esattamente 3 sottogruppi se e solo se è isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$ per qulche primo p.

3) Sia $d \in \mathbb{Z}^\times \setminus (\mathbb{Z}^\times)^2$ e si consideri l'anello $R_d := \mathbb{Z}[\sqrt{d}]$.

   a) Per ogni $\alpha \in R_d$, sia $N(\alpha) = \alpha\overline{\alpha}$ (si intende il coniugio complesso). Dimostrare che α è invertibile se e solo se $N(\alpha) = \pm 1$.

   b) Si determinino gli invertibili di R_d per $d = -1$ e $d < -1$.

   c) Dimostrare che $2, 3$ e $1 \pm \sqrt{-5}$ sono irriducibili in R_{-5}.

   d) R_{-5} è un dominio a fattorizzazione unica? Argomentare.

4) Sia $f \in \mathbb{Z}[X]$ un polinomio monico e siano p e q due primi distinti. Si supponga che la seguqnte proprietà sia vera: la riduzione modulo p di f è prodotto di due polinomi irriducibili di grado d_1, d_2; la riduzione modulo q di f è prodotto di due polinomi irriducibili di grado e_1, e_2 e inoltre $\{d_1, d_2\} \neq \{e_1, e_2\}$. Dimostrare che f è irriducibile in $\mathbb{Q}$.

5) Sia Φ_m l'm-esimo polinomio ciclotomico. Dimostrare che se $m > 1$ è dispari, allora $\Phi_{2m}(X) = \Phi_m(-X)$.

Esercizi di fine corso annuale (III)

1) Siano n e a due interi positivi coprimi. Dimostrare che la mappa:

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ x &\mapsto ax \end{aligned}$$

è un automorfismo di $\mathbb{Z}/n\mathbb{Z}$. Dedurre che $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

2) Sia G un gruppo semplice di ordine n. Dimostrare che se H è un sottogruppo di G tale che $|G : H| = k > 1$, allora $k! \geq n$.

3) Dimostrare o confutare la seguente proposizione: siano I_1 e I_2 due ideali massimali di $\mathbb{Z}[\sqrt{2}]$; se $\mathbb{Z}[\sqrt{2}]/I_1 \cong \mathbb{Z}[\sqrt{2}]/I_2$ allora $I_1 = I_2$.

4) Sia F in campo di caraterristica diversa da 2.

   a) Sia E un'estensione quadratica di F e sia

   $$S(E) := \{a \in F^\times : a \text{ e un quadrato in } E^\times\}.$$

   Dimostrare che $S(E)$ è un sottogruppo di $F^\times$ contenente $(F^\times)^2$.

   b) Siano E ed E' due estensioni quadratiche di F. Dimostrare che esiste un isomorfismo $f : E \to E'$ che fissa F se e solo se $S(E) = S(E')$.

   c) Dimostrare che esiste un insieme infinito di campi $\{E_i\}_i$ con le seguenti proprietà: E_i è estensione quadratica di $\mathbb{Q}$ ed inoltre E_i non è isomorfo a E_j per $i \neq j$

   d) Sia p un primo dispari. Dimostrare che a meno di isomorfismo c'è un solo campo di ordine p^2.

Esercizi di fine corso annuale (IV)

1) Dimostrare o confutare le seguenti affermazioni:

   a) Se x e y sono elementi di un gruppo tali che $x^2 = 1$ e $y^3 = 1$ allora $(xy)^6 = 1$.

   b) I seguenti elementi di S_7 sono coniugati:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}.$$

   c) L'unico sottogruppo di A_5 che contiene (123) è A_5 stesso.

2) Sia G un gruppo finito che possiede un solo p-Sylow per ogni primo p che divide $|G|$. Dimostrare che G è il prodotto diretto dei suoi p-Sylow.

3) Si consideri il primo $p = 11213$. Dimostrare le seguenti affermazioni:

   a) Trovare un ideale massimale I di $\mathbb{Z}[i]$ che contiene p.

   b) Trovare tutti gli irriducibili di $\mathbb{Z}[i]$ che dividono p in $\mathbb{Z}[i]$.

   c) Sia I l'ideale trovato in *a*). Dimostrare che $\mathbb{Z}[i]/I$ è isomorfo a $\mathbb{F}_p$.

   [*Sugg:* $11213 = 82^2 + 67^2$.]

4) Si costruisca un campo di spezzamento di $X^5 - 2$ su $\mathbb{Q}$. Si denoti tale campo con E; determinare il grado di E su $\mathbb{Q}$.

5) Sia F un campo di caratteristica p. Dimostrare che se $X^p - X - a$ è riducibile su F, allora si spezza su F in fattori distinti.