Problem set 1 , January 30, 2020

Let R be a ring with unity.

1. Let $R = \left\{ \cdot \begin{pmatrix} a & \bar{b} \\ 0 & c \end{pmatrix} \right\}$, where $a, c \in \mathbb{Z}$ and $b \in \mathbb{Z}/p\mathbb{Z}$ where p is a prime number.
   (a) Show that R is a ring. Is it commutative.
   (b) Let $\alpha = \left\{ \begin{pmatrix} a & \bar{p} \\ 0 & 1 \end{pmatrix} \right\}$. Determine a so that α is a left zero divisor. Is it a right zero divisor.
   (c) Let $\beta = \left\{ \begin{pmatrix} 0 & \bar{1} \\ 0 & 0 \end{pmatrix} \right\}$. Determine whether β is a left /right zero divisor. Is there an integer n so that $\beta^n = 0$.
2. Let $i^2 = j^2 = k^s = -1$ and $ij = -ji = k$.
   (a) Let $\mathbb{H} = \mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot i \oplus \mathbb{R} \cdot j \oplus \mathbb{R} \cdot k$. Show that $\mathbb{H}$ is a division ring. Determine the center of $\mathbb{H}$.
   (b) Let $R = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot i \oplus \mathbb{Z} \cdot j \oplus \mathbb{Z} \cdot k$
   Is R is a division ring. Determine the center of R. What are the units in R.
3. Consider the ring $\mathbb{C}[x; \sigma]$ where σ denotes complex conjugation on $\mathbb{C}$ and for any $a \in \mathbb{C}$, $xa = \sigma(a)x$.
   (a) Define $(\sum a_i x^i)(\sum b_j x^j) = \sum a_j \sigma^i(b_j) x^{i+j}$ and show that $\mathbb{C}[x; \sigma]$ is a ring.
   (b) Show that the center of R is $\mathbb{R}[x^2]$
   (c) Show that $R/R \cdot (x^2 + 1)$ is isomorphic to the division ring of real quartenions.
   (d) Let $\phi : R \to M_2(\mathbb{C})$ be given by $\phi(x) = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$ and $\phi(r) = \begin{pmatrix} r & 0 \\ 0 & \sigma(r) \end{pmatrix}$. Show that $\ker(\phi) = (x^4 + 1)$
4. Let D be a division ring with center R. Let $D[x]$ be the polynomial ring over D.
   (a) Show that the center of $D[x]$ is $R[x]$.
   (b) Let $a \in D \setminus R$. Show that the ideal generated by $x - a$ in $D[x]$ is the unit ideal.
   (c) Show that any ideal in $I \subset D[x]$ is of the form $D[x] \cdot (h)$ where $h \in R[x]$.

Problem set 2 , August 18, 2025

Tutorial 3- Monday 8/8/2022

We will assume that all rings have the unit element.

1. Let $U(R)$ denote the set of units in R. Show that $U(R)$ is a group with respect to multiplication. If R is an integral doman and x is a variable, then show that $U(R[x]) = U(R)$.
2. Let $n \geq 1$ be an integer. Determine $U((\mathbb{Z}/n\mathbb{Z})[x])$ and $U(\mathbb{Z}/n\mathbb{Z})$.
3. Determine the kernel and image of the map in the following cases:
   (a) Let x, y, t be variables, a, b be positive integers with $gcd(a, b) = 1$. Let $\phi : \mathbb{C}[x, y] \to \mathbb{C}[t]$ be the homomorphism given by $\phi(x) = t^a$ and $\phi(y) = t^b$.
   (b) Let x be a variable and $\phi : \mathbb{Z}[x] \to Z[i]$ be given by $\phi(r + sx) = r + si$.
   (c) Let R be a ring of characteristic p. Consider the map $\phi : R \to R$ given by $\phi(r) = r^p$. Show that ϕ is a ring homomorphism.
4. Let R be an integral domain. Let $S(R) := \{(a, b) : a, b \in R, b \neq 0\}$. Consider the relation $\sim$ on $S(R)$ give by $(a, b) \sim (c, d)$ if and only if $ad = bc$.
   (a) Show that $\sim$ is an equivalence relation.
   (b) Define $Q(R) := S(R)/\sim$. Let — denote image in $Q(R)$. Define operations on $Q(R)$ as follows:
   $$\begin{aligned} \overline{(a,b)} + \overline{(c,d)} &= \overline{(ad+bc, bd)} \\ \overline{(a,b)} \circ \overline{(c,d)} &= \overline{(ac, bd)}. \end{aligned}$$
   Show that sum and product are well defined. Show that with these operations show that $Q(R)$ is a field. What is the inverse of $\overline{(a, b)}$.
5. Let R be a subset of rationals m/n such that $n \neq 0$ and p does not divide n. Show that R is a ring.
6. Let R be a ring. Let $Z := \{a \in \mathrm{R}\}$ such that $ax = xa$ for all $x \in R$. Show that Z is a subring of R. (Z is called the center of R).
7. Show that a ring has no zero divisors if and only if right and left cancellation laws hold. i.e., if $ac = bc \implies b = c$ (similarly if $ca = ba$).
8. Let $R = \mathbb{Z}$. Determine all prime ideals in $\mathbb{Z}[x]$.

Tutorial 3- Monday 25/8/2022

We will assume that all rings are commutative and have the unit element.

1. Let $p \in \mathbb{Z}$ be a non-zero prime. Consider $R := \{a + bi + cj + dk | i^2 = j^2 = -1, ij = -ji = k\}$ be the ring of quartenions over $\mathbb{Z}/p\mathbb{Z}$.
   (a) Show that R has only finitely many elements. Determine this number.
   (b) Show that R is a ring, but not a division ring.
2. Let $R = \mathbb{C}[x, y, z]$ and $S = \mathbb{C}[t]$ where x, t, z, t are variables. Let $\phi : R \to S$ be a homomorphism given by $\phi(x) = t^3$, $\phi(y) = t^4$ and $\phi(z) = t^5$. Show that $ker(\phi) = (x^3 - yz, y^2 - xz, z^2 - x^2y)$.
3. Let $\phi : R \to R'$ be a homomorphism of R into R'. Show that $ker(\phi) := \{a \in R | \phi(a) = 0\}$ is an ideal in R.
4. 'Let R be the set of all real valued functions on $[0, 1]$ and S a subset of $[0, 1]$. Show that the set of all functions on $f \in R$ such that $f(x) = 0$ for all $x \in S$ is a maximal ideal in R.
5. Let p be a prime number, $R = \mathbb{Z}[\sqrt{p}] := \{a + b\sqrt{p} : a, b \in \mathbb{Z}]$ and $S = \mathbb{Z}/p\mathbb{Z}$. Let $\phi : R \to S$ be given by $\phi(a + b\sqrt{p}) = a + p\mathbb{Z}$.
   (a) Show that ϕ is a homomorphism.
   (b) Determine $ker(\phi)$
6. Let R be a ring. An element e is said to be idemopotent if $e^2 = e$
7. Show that $R \cong (e)R \times (1 - e)R$
   (a) Suppose $e_1, \ldots, e_n$ are idempotent elements. Assume in addition they are orthogonal, i.e., and $e_j e_j = 0$ for all $i \neq j$. Let $R_1, \ldots, R_n$ be rings with identity. Show that the following are equivalent:
      i. $R \cong R_1 \times R_2 \times \cdots R_n$
      ii. There exists orthognal idempotent elements $e_1, \ldots, e_n$ such that $e_1 + \cdots + e_n = 1_R$ and $(e_i)R \cong R_i$.
      iii. $R \cong I_1 \times I_2 \times \cdots I_n$ where $I_1, \ldots, I_n$ are ideals in R.
8. Let R be a ring and $I_1, \ldots, I_n$ ideals in R.
   (a) Suppose $I_1 + \cdots I_n = R$ and for each $1 \leq k \leq n$, $I_k \cap (I_1 + \cdots + I_{k-1} + I_{k+1} + \cdots + I_n) = 0$. The show that there is an isomorphism $R \cong I_1 \times \cdots \times I_n$.
   (b) Suppose $I_i + I_j = R$ for all $i \neq j$. If $b_1, \cdots, b_n \in R$, then show that there exists $b \in R$ such that $b \cong b_i \ mod(I_i)$ for all $i = 1, \ldots, n$.
   (c) If $I_1, \ldots, I_n$ are ideals in R, then show that there is an injective map $\phi : R/(I_1 \cap \cdots \cap I_n) \to (R/I_1) \times \cdots \times (R/I_n)$.
9. Let R be a commutative ring with 1 and S a subset or R with the property that (i) $0 \notin S$ (ii) $s_1 s_2 \in S$ implies that $s_1 s_2 \in S$. Let $a_1, a_2 \in R$ and $s_1, s_2 \in S$. Define a relation $\sim$ in $R \times S$ by $(a_1, s_1) \sim (a_2, s_2)$ if there exists $s_3 \in S$ such that $s_3(a_1 s_2 - a_2 s_1) = 0$.
   (a) Show that $\sim$ is an equivalence relation.
   (b) Let R_S denote the set of all equivalence classes and let $[a, b]$ be an element of R_S. In R_S define $[a, b] + [c, d] := [ad + bc, bd]$ and $[a, b] \cdot [c, d] = [ac, bd]$. Show that these are well defined operations.
      i. Show that the mapping $\phi : R \to R_S$ defined by $\phi(a) = [as, s]$ is a homomorphism. Determine the kernel of ϕ.
      ii. Show that $ker(\phi)$ has no element of S in it.
      iii. Let $s_1, s_2 \in S$. Show that every element of the form $[s_1, s_2]$ is invertible.
10. Let $R := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
    (a) Show that R (i) is a ring (ii) R is a field
    (b) What happens if $\mathbb{Q}$ is replaced by $\mathbb{Z}$.
11. Let R, S be rings and $\phi : R \to S$ be a homomorphism of rings.
    (a) Suppose ϕ is surjective.
       i. Show that for every ideal I in R, $\phi(I)$ is an ideal in S.
       ii. Show that if P is a prime ideal in R, then $\phi(P)$ is a prime ideal in S.
    (b) If Q is a prime ideal in S, then show that $\phi^{-1}(Q)$ is a prime ideal in R which contains $ker(\phi)$.
    (c) Descirbe all prime ideals in $R = \mathbb{Z}$. Describe all prime ideals in $S = Z[x]$.

Tutorial 3- Monday 25/8/2022

We will assume that all rings are commutative and have the unit element.

1. Let R be a Euclidean ring. Show that for any $a, b \in R$, there exists an element r such that $(r) = (a, b)$.
2. Show that $\mathbb{Z}[i]$ is a Euclidean domain.
3. Let $R = \mathbb{Z}[\sqrt{10}]$. Let $N : R \to \mathbb{Z}$ be given by $N(a + b\sqrt{10}) = a^2 - 10b^2$.
   (a) Show that $N(uv) = N(u)N(v)$ for all $u, v \in R$.
   (b) Show that $N(u) = 0$ if and only if $u = 0$.
   (c) $N(u) = 1$ if and only if u is a unit.
   (d) $4 + \sqrt{10}$, is irreducible in R but not a prime element.
4. Let $R = \mathbb{R}[x, y]$ and $S = \mathbb{R}[x, y, x/y]$. Let $I = (x^3, xy^2, y^3)$. Let $\phi : R \to S$ be the inclusion map. Prove or disprove: $I^{ec} = I$ (5 marks)
5. Find the gcd of the following elements: (i) $3 + 4i$ and $4 - 3i$ (ii) $11 + 7i$ and $18 - i$.
6. Let R be an integral domain. Suppose R is not a field. Let $U(R)$ denote the set of units in R. Show that $R \setminus \{U(R) \cup \{0\}\} \neq \emptyset$. Suppose that there exists no $y \in R \setminus \{U(R) \cup \{0\}\}$, such that for all $x \in R$, $y|(x - r)$ for some $r \in \{U(R) \cup \{0\}\}$. Show that R is not a Euclidean domain. (5 marks)
7. Show that the following rings are Euclidean domains: (i) $\mathbb{Z}[i]$ (ii) $\mathbb{Z}[\sqrt{-2}]$
8. Determine all the untis in $\mathbb{Z}[\sqrt{2}]$.
9. Show that $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a PID but not a ED.

Tutorial 4- Monday 22/9/2025

We will assume that all rings are nonzero, are commutative and have the unit element.

1. Let $= \mathbb{C}[x, y]$. Show that $(xy - 3y^2, x^2 + 4y^2 - 1, 13y^3 - y) = (y, x - 1) \cap (13y^2 - 1, x - 3y) \cap (y, x + 1)$. Which of the ideals $(y, x - 1)$, $(13y^2 - 1, x - 3y)$, $(y, x + 1)$ are maximal in R.
2. Let F be a field. Prove that the ring $F[x, x^{-1}]$ of Laruent polynomials is a PID.
3. Let $R = \mathbb{Z}[\omega]$. Let $p \neq 3$ be a prime.
   (a) Show that the polynomial $x^2 + x + 1$ has a root if and only if $p \cong 1(mod\ 4)$,
   (b) (p) is maximal ideal if and only if $p \cong 1(mod\ 3)$
   (c) p factors in R if and only if $p = a^2 + ab + b^2$ for some integers a and b.
4. Let f, g be polynomials in $\mathbb{C}[x, y]$ with no common factor. Show that the ring $R = \mathbb{C}[x, y]/(f, g)$ is a finite dimensional vector space over $\mathbb{C}$.
5. Let R be the ring of polynomials in $cos(t)$ and $sin(t)$, with real coefficients.
   (a) Show that $R \cong \mathbb{R}[x, y]/(x^2 + y^2 - 1)$.
   (b) Show that R is not a UFD.
   (c) Prove that $S = \mathbb{C}[x, y]/(x^2 + y^2 - 1)$ is a PID.
   (d) Determine the units in R and S.

Tutorial 6- Monday 13/10/2022

We will assume that all rings are nonzero, are commutative and have the unit element.

1. Let $R = \mathbb{Z}[\sqrt{-5}]$. Let $\alpha = \sqrt{-5}$. Let $\mathfrak{p}_1 = (2, 1+\alpha)$, $\mathfrak{p}_2 = (2, 1-\alpha)$, $\mathfrak{p}_3 = (3, 1+\alpha)$ and $\mathfrak{p}_4 = (3, 1-\alpha)$.
   (a) Show that $\mathfrak{p}_i$ are prime ideal for $i = 1, 2, 3, 4$. Are they maximal ideals?
   Show that 2 ,3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ are irreducible in R.
   (b) Show that $(6) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$.
   (c) Is $(6) = \mathfrak{p}_1^2 \cap \mathfrak{p}_3 \cap \mathfrak{p}_4$.
   (d) Determine which of the following ideals are prime ideals:
   (a) $(3+5\alpha)$, $(2+2\alpha)$, (b) $(4+\alpha, 1+2\alpha)$
   (e) Factor (14) into prime ideals in R.
   (f) Determine whether 11 is irreducible in R.
   (g) Let $I = (3, 1+\alpha)$. Show that I^2 is a principal ideal.
2. Let $\delta = (1+\sqrt{-19})/2$ and $R = \mathbb{Z}[\delta]$.
   (a) Show that $R \cong \mathbb{Z}[T]/(T^2 - T + 5)$.
   (b) Determine whether 2 and 3 are prime ideals in R.
   (c) Determine whether the following ideals are (i) prime ideals (ii) maximal ideal in $R[x]$:
   (a) $(7, \delta^3 x + x + 1)$ (b) $(2\delta^2 + 3)$ (c) $(\delta x + 1)$ (d) $(\delta x + 2)$ (e) $(2x\delta + 1)$ (f) $(11, 2x\delta + 1)$
3. Let $R = \mathbb{Z}[\sqrt[3]{2}]$. Is it possible to write (5) as a product of prime ideals?
4. Let $R = \mathbb{Z}[\sqrt{n}]$ where $n \geq 3$.
   (a) Which of the following are (i) irreducible (ii) prime in R?
   (a) 2, (b) $\sqrt{-n}$, (c) $1+\sqrt{-n}$
   (b) Show that R is not a UFD.
5. Let $R = \mathbb{Z}[\omega]$ where $\omega = e^{2\pi i/3}$. Let $p \neq 3$ be a prime.
   (a) Show that $x^2 + x + 1$ has a root in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \ncong 1 \bmod 3$.
   (b) Show that (p) is maximal ideal if and only if $p \cong -1 \bmod 3$.
   (c) p factors in R if and only if $p = a^2 + ab + b^2$ for some integers a and b.
6. Let $\delta = \sqrt{-3}$ and $R = \mathbb{Z}[\delta]$.
   (a) Let $I = (2, 1+\delta)$, $\overline{I} = (2, 1-\delta)$. Is $I\overline{I}$ a principal ideal.
   (b) Determine whether the ideal $(3x+1)$ is a prime ideal in R.
7. Let $\delta = \sqrt{-6}$ and $R = \mathbb{Z}[\delta]$.
   (a) Determine whether $(2, \delta)$ and $(3, \delta)$ are prime ideals.
   (b) Factor $(6)R$ into prime ideals.

Tutorial 7- Monday 27/10/2022

1. Let $R \subseteq S$ be an integral domains and let $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. Define $f'(x) = \sum_{i=i}^{n} a_i k x^{i-1}$. Let $a \in S$.
   (a) Show that a is a multiple root of f if and only if $f(a) = 0$ and $f'(a) = 0$.
   (b) Let R be a field and suppose $gcd(f, f') = 1$. Show that f has no multiple roots in S.
   (c) Let R be a field and suppose $f(x)$ is irreducible in $R[x]$ and suppose there is a root of f in S. Show that f has no multiple roots in S if and only if $f' \neq 0$.
2. Show that $1 + x + \cdots + x^{p-1} \in \mathbb{Q}[x]$ is irreducible.
3. Let p be a prime, $q = p^e$ and $r = p^{e-1}$. Show that $(x^q - 1)/(x^r - 1)$ is irreducible.
4. Let $f, g \in \mathbb{Z}[x]$. Show that f and g are relatively prime in $\mathbb{Q}[x]$ if and only if the ideal they generate in $\mathbb{Z}[x]$ contains an integer.
5. Let $R = \mathbb{Z}[x_1, x_2, x_3 x_4]$. Determine which of the following polynomials are irreducible: (i) $f = x_1^{p+1} - x_2^p$ (ii) $g = x_1 x_4 - x_2 x_3$(iii) $h = x_1^p x_2 - x_3^p$ (iv) $fh + g^p$.
6. Determine which of the following polynomials in $\mathbb{C}[x, y, z]$ are irreducible: (1) $y^5 - z^4$ (2) $z^8 + 2xy^3 - x^2yz - z^3$ (3) $2y^2z^6 + xz^7 - x^3y - 2y^2z + 3xz^2$ (4) $y^4z^5 - y^4 + 2xy^2z - x^2z^2$ (5) $2xy^4z^4 + yz^7 + 3x^2y^2 - 2x^3z - yz^2$ (6) $x^2y^4z^3 + 3y^3z^5 + 2xyz^6 - x^4 - 3y^3 + 4xyz$
7. Show that $x^p - x - c$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ if and only if it has no root in $\mathbb{Z}/p\mathbb{Z}$.

Tutorial 6- Monday 17/10/2022

Throughout $K \supset F$ is a field extension.

1. Let $F_1 \subset F_2 \subset F_3$ be fields. Show that $[F_3 : F_1] = [F_3 : F_2][F_2 : F_1]$.
2. Show that $\pi \cdot i$ is algebraic over $\mathbb{R}$. Is it algebraic over Q?
3. Show that $\sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$. Compute $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$.
4. Determine the splitting field over $\mathbb{Q}$ for the following: (a) $x^4 - 2$ (b) $x^4 + 2$.
5. Show that $[K : F]$ is prime then there are no intermediate fields between K and F.
6. Let $\alpha_1, \ldots, \alpha_n \in K$. Show that $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n)$.
7. For any subset $S \subseteq K$, let $F(S)$ denote the smallest field containing F and S. If $K_1, \ldots, K_n$ be subfields of K, then show that $K_1(K_2(\ldots K_{n-1}(K_n))) = K_1 \cdots K_n$.
8. Let $\alpha \in K$ be algebraic of odd degree. Show that $K(\alpha) = K(\alpha^2)$.
9. Let $x^n - a \in F[x]$ be irreducible and $\alpha \in K$ a root of $x^n - a$. Suppose m divides n. Determine the degree of the irreducible polynomial satisfied by α^m.
10. K is algebraic over F, L is an integral domain such that $F \subseteq L \subseteq K$. Show that L is a field.
11. Let $F = \mathbb{Q}$ and $f(x) = x^5 + 2x + 2 \in F[x]$.
    (a) Show that $f(x)$ is irreducible.
    (b) Let α be a real root of $f(x)$ and $K = \mathbb{Q}(\alpha)$ and let $\{1, \alpha, \ldots, \alpha^4\}$ be a basis of K over $\mathbb{Q}$. Express $(\alpha^2 + 2)(\alpha^3 + 3\alpha)$ in terms of the basis elements.
12. Let F be a finite field and let $f(x) \in F[x]$ be a non-constant poluynomial whose derivate is the zero polynomial. Show that $f(x)$ cannot be irreducible over F.

Tutorial 9- Monday 17/11/2025

1. Let $F = \mathbb{F}_8$. Determine all the elements of F. Find the irreducible polynomial of each of the elements.
2. Find the 13-th root of 2 in the field $\mathbb{F}_8$.
3. Factor $x^9 - x$ and $x^{27} - x$ in $\mathbb{F}_3$.
4. Factor the polynomial $x^{16} - x$ over the field's $\mathbb{F}_4$ and $\mathbb{F}_8$.
5. Let K be a finite fie ld. Prove that the product of the nonzero elements of K is -1.
6. The polynomials $f(x) = x^3 + x + 1$ and $g(x) = x^3 + x^2 + 1$ are irreducible over $\mathbb{F}_2$. Let K be the field extension obtained by adjoining a root of f , and let L be the extension obtained by adjoining a root of g. Describe explicitly an isomorphism from K to L, and determine the number of such ismorphisms.
7. Let $F = \mathbb{F}_p$.
   (a) Determine the number of monic irreducible polynomials of degree 2 in $F[x]$.
   (b) Let $f(x)$ be an irreducible polynomial of degree 2 in $F[x]$. Prove that $K = F[x]/f(x)$ is a field of order p^2, and that its elements have the form $a + b\alpha$, where a and b are in F and α is a root of $f(x)$ in K. Moreover, every such element with b=t-Q is the root of an irreducible quadratic polynomial in $F[x]$.
   (c) Show that every polynomial of degree 2 in $F[x]$ has a root in K.
   (d) Show that all the fields K constructed as above for a given prime p are isomorphic .
8. Let F be a finite fie ld, and let $f(x)$ be a non constant polynomial whose derivative is the zero polynomial. Prove that $f(x)$ can not be irreduc ible over F .
9. L e t $f(x) = ax^2 + bx + c$ with a, b, c in a ring R . Show that the ideal of the polynomial ring $R[x]$ that is generated by $f(x)$ a n d $f'(x)$ contains the discriminant, the constant polynomial $b^2 - 4ac$.
10. Let p be a prime integer , and le t $q = p^r$ and $q' = p^k$. For which values of r and k does $x^{q'}x$ divide $x^q - x$ in $\mathbb{Z}[x]$?
11. Prove that a finite subgroup of the multiplicative group of any field F is a cyc lic group .