Problem 1 (8.5)**.** *Let $R = \mathbb{Z}[\sqrt{-5}]$. Show that $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducibles of R and no two of which are associate in R, and that $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are two distinct factorizations of 6 into irreducibles in R. So R is not a UFD.*

Proof. □

Problem 2 (9.1)**.** *Prove that every irreducible element of a UFD is a prime.*

Proof. Let R be a UFD and $r \in R$ irreducible. Then consider $a, b \in R$ such that $r|ab$. This implies that $cr = ab$ for some $c \in R$. As R is a UFD take the factorization for both sides and we get $t_1 \cdots t_s r = p_1 \cdots p_n q_1 \cdots q_m$. As r is irreducible and factorizations are unique it must be that r is an associate of something on the right. Thus either $r|p_i$ or $r|q_j$ it then follows that $r|a$ or $r|b$ respectively which implies that r is in fact prime. □

Problem 3 (9.3)**.** *Give an example of a UFD which is not a PID.*

Proof. Consider $\mathbb{Z}[x]$. This is a UFD because $\mathbb{Z}$ is a UFD. However the ideal $\langle x^2-1, x\rangle$ cannot be generated by a single polynomial. Therefore $\mathbb{Z}[x]$ is a PID which is not a UFD. □

Problem 4 (9.4)**.**

1. *Determine whether the following polynomials are irreducible in the rings indicated and prove your assertions. For those that are reducible, determine their factorization into irreducibles.*
   (a) x^3+x+1 *in* $\mathbb{Z}_3[x]$.
   (b) x^4+1 *in* $\mathbb{Z}_5[x]$.
   (c) x^4+10x^2+1 *in* $\mathbb{Z}[x]$.
   (d) x^4-4x^3+6 *in* $\mathbb{Z}[x]$.
   (e) $x^6+30x^5-15x^3+6x-120$ *in* $\mathbb{Z}[x]$.
   (f) x^2+y^2+xy+1 *in* $\mathbb{Q}[x,y]$.
2. *Prove that the following polynomials are irreducible in* $\mathbb{Z}[x]$.
   (a) $x^4+4x^3+6x^2+2x+1$ *(Substitute $x-1$ for x).*
   (b) $\frac{(x+2)^p-2^p}{x}$ *where p is an odd prime.*
   (c) $\prod_1^n (x-i)-1$, *where $n \in \mathbb{Z}_{>0}$*
3. *Find all irreducible polynomials of degree ≤ 3 in $\mathbb{Z}_2[x]$, and the same for $\mathbb{Z}_3[x]$.*
4. *Prove that if n is composite number, then $\sum_0^{n-1} x^{n-1}$ is reducible over $\mathbb{Z}$.*

Proof. □

Problem 5 (9.5)**.** *Let R be a PID and $a, b \in R$. Prove that if a, b are relatively prime, then $(a)+(b) = R$, and a^i, b^j are relatively prime for all $i, j \in \mathbb{Z}_{>0}$.*

Proof. □

Problem 6 (9.6). *1. Let F be a finite field of order q and $f(x)$ a polynomial of degree n. Prove that the quotient ring $F[x]/(f(x))$ has q^n elements.*

2. Show that $f(x) = x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$ and that $K = \mathbb{Z}_2/(f(x))$ is a field. Find a generator of the cyclic group K^X.

Proof. □

Problem 7 (G4). *Let $G = GL(2, \mathbb{F}_p)$ be the group of invertible 2×2 matrices with entries in the finite field $\mathbb{F}_p$, where p is prime.*

1. *Show that G has order $(p^2 - 1)(p^2 - p)$.*
2. *Show that for $p = 2$ the group G is isomorphic to the symmetric group S_3.*

Proof. □

Problem 8 (G5). *Let G be the group of units of the ring $\mathbb{Z}/247\mathbb{Z}$.*

1. *Determine the order of G.*
2. *Determine the structure of G (as in the classification theorem for finitely generated abelian groups). (Hint: Use the Chinese Remainder Theorem).*

Proof. □

Problem 9 (G8). *List all abelian groups of order 8 up to isomorphism. Identify which groups on your list is isomorphic to each of the following groups of order* 8. *Justify your answer.*

1. *$(\mathbb{Z}/15\mathbb{Z})^*$ = the group of units of the ring $\mathbb{Z}/15\mathbb{Z}$.*
2. *The roots of the equation $z^8 - 1 = 0$ in $\mathbb{C}$.*
3. *$\mathbb{F}_8^+$ = the additive group of the field $\mathbb{F}_8$ with eight elements.*

Proof. □

Problem 10 (R4). *Let $\mathbb{F}$ be a field and let $R = \mathbb{F}[X, Y]$ be the ring of polynomials in X and Y with coefficients from $\mathbb{F}$.*

1. *Show that $M = \langle X + 1, Y - 2\rangle$ is a maximal ideal of R.*
2. *Show that $P = \langle X + Y + 1\rangle$ is a prime ideal of R.*
3. *Is P a maximal ideal of R. Justify your answer.*

Proof. ∎

Problem 11 (R6)**.** *Let R be a commutative ring with identity and let I and J be ideals of R.*

1. *Define*

$$(I : J) = \{r \in R | rx \in I, \forall x \in J\}$$

   Show that $(I : J)$ is an ideal of R containing I.

2. *Show that if P is a prime ideal of R and $x \notin P$, then $(P : \langle x \rangle) = P$, where $\langle x \rangle$ denotes the principal ideal generated by x.*

Proof. ∎

Problem 12 (R7)**.** *Let R be a commutative ring with identity, and let I and J be ideals of R.*

1. *Define what is meant by the sum $I + J$ and the product IJ of the ideals I and J.*

2. *If I and J are distinct maximal ideals, show that $I + J = R$ and $I \cap J = IJ$.*

Proof. ∎