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 $\sum_0^{n-1} x^i$ is reducible over $\mathbb{Z}$.*

Proof.
1. (a) $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$
   (b) $x^4 + 1 = (x^2 + 2)(x^2 + 3)$
   (c) No roots, must be product of two irreducibles of deg 2. But $a + b = 10$ and $ab = 1$ which cannot occur. **Make this pretty.**
   (d) Eisenstein $p = 2$
   (e) Eisenstein $p = 3$

(f) Consider $\mathbb{Z}[x,y]/(y-1)$. Get x^2+x+1 root must be either ± 1. Use gauss's lemma.

2. (a) Sub $x-1$ for x and that simplifies to x^4-2x+2 by Eisenstein with $p=2$ is irreducible and thus the rest of it is as well.

(b)

(c)

$\square$

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. Let R be a PID and $a, b \in R$ such that a and b are relatively prime. Then 1 is a gcd of a and b. However this means that there exists $\alpha, \beta \in R$ such that $\alpha a + \beta b = 1 \in (a)+(b)$ (Prop 8.11) implying that $(a)+(b)=1$.

Now we will show that a^i and b are relatively prime. We have the case where $i=1$ be assumption. Next assume that we have $\alpha a^i + b = 1$. Then if we square both sides we get

$$\alpha^2 a^{2i} + \beta^2 b^2 + \alpha a^i \beta b + \beta b \alpha a^i \beta b = (\alpha^2 a^{i-1})a^{i+1} + (\beta b + \alpha a^i \beta + \alpha a^i \beta)b = 1$$

which shows that a^{i+1} is relatively prime to b with the assumption that a^i is relatively prime to b. Therefore a^i is relatively prime to b where $i \in \mathbb{Z}_{>0}$. To get arbitrary powers of b just set $a := b$ and $b := a^i$ and repeat the process.

Therefore if a, b are relatively prime then $(a)+(b)=R$ and a^i, b^j are relatively prime for $i, j \in \mathbb{Z}_{>0}$. $\square$

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. 1. We proceed by induction. Suppose that $\deg f = 0$. Then $(f)=F[x]$ implies that $F[x]/(f) \cong F[x]/F[x] = \{0\}$ which shows that the order is one.

Now assume that if $\deg g \leq n$ then $F[x]/(f)$ is of order $q^{\deg g}$. Then suppose that $\deg f = n+1$. In the case where f is reducible by Proposition 9.23 we have

$$f = f_1^{n_1} \cdots f_k^{n_k}$$

where $\sum n_i = n+1$ and $n_i \leq n$ and that $F[x]/(f) \cong F[x]/(f_1^{n_1} \times \cdots \times f_k^{n_k})$ The order of $F[x]/(f_i^{n_i i})$ is q^{n_i} by our inductive hypothesis which implies that $|F[x]/(f)| = q^{n_1} \cdots q^{n_k} = q^{n+1}$.

However if f is irreducible, then $F[x]/(f)$ is the $n+1$th degree field extension and which the field with q^{n+1} elements.

Therefore if $\deg f = n$ then the order of $F[x]/(f)$ is q^n where F is the field with q elements. $\square$

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. $\square$

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. 1.

2.

$$\begin{gathered}
(1,1),(2,36),(3,18),(4,18),(5,36),(6,36),(7,12),(8,12),(9,9),(10,18),(11,12),(12,6), \\
(14,18),(15,36),(16,9),(17,18),(18,4),(20,12),(21,36),(22,18),(23,18),(24,36),(25,18), \\
(27,6),(28,36),(29,18),(30,6),(31,12),(32,36),(33,36),(34,36),(35,9),(36,18),(37,12), \\
(40,18),(41,36),(42,9),(43,18),(44,36),(45,12),(46,12),(47,36),(48,18),(49,6),(50,12), \\
(51,18),(53,18),(54,36),(55,9),(56,6),(58,12),(59,36),(60,36),(61,9),(62,18),(63,36), \\
(64,6),(66,9),(67,36),(68,3),(69,6),(70,36),(71,36),(72,36),(73,36),(74,9),(75,6), \\
(77,2),(79,18),(80,36),(81,9),(82,18),(83,12),(84,12),(85,36),(86,36),(87,3),(88,6), \\
(89,36),(90,18),(92,9),(93,36),(94,6),(96,4),(97,36),(98,36),(99,36),(100,9),(101,18), \\
(102,12),(103,6),(105,18),(106,12),(107,6),(108,18),(109,36),(110,36),(111,36), \\
(112,36),(113,6),(115,12),(116,18),(118,9),(119,36),(120,9),(121,6),(122,12),(123,36), \\
(124,36),(125,12),(126,6),(127,18),(128,36),(129,18),(131,9),(132,12),(134,6),(135,36), \\
(136,36),(137,36),(138,36),(139,9),(140,6),(141,12),(142,18),(144,3),(145,12),(146,18), \\
(147,18),(148,36),(149,36),(150,36),(151,4),(153,6),(154,36),(155,18),(157,9),(158,36), \\
(159,3),(160,6),(161,36),(162,36),(163,12),(164,12),(165,18),(166,18),(167,36), \\
(168,18),(170,2),(172,3),(173,18),(174,36),(175,36),(176,36),(177,36),(178,3),(179,6), \\
(180,36),(181,18),(183,6),(184,36),(185,18),(186,18),(187,36),(188,36),(189,12), \\
(191,3),(192,18),(193,36),(194,18),(196,9),(197,12),(198,6),(199,18),(200,36), \\
(201,12),(202,12),(203,36),(204,18),(205,18),(206,36),(207,18),(210,12),(211,18), \\
(212,18),(213,36),(214,36),(215,36),(216,12),(217,6),(218,18),(219,36),(220,6), \\
(222,18),(223,36),(224,18),(225,18),(226,36),(227,12),(229,4),(230,18),(231,18), \\
(232,36),(233,18),(235,3),(236,12),(237,9),(238,18),(239,12),(240,12),(241,36), \\
(242,36),(243,18),(244,18),(245,36),(246,2)
\end{gathered}$$

$\square$

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.

p

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. □