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. The only units of R will be elements $a + b\sqrt{-5}$ wherein $\frac{1}{a^2+5b^2} \in \mathbb{Z}$. However this will not happen for any elements except ± 1. Therefore $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are not associates.

- The norm of 2 is 4. Since the norm is multiplicative if $xy = 2$ then the product of their norms must be 4. Since we're throwing out associates we must have $N(x) = N(y) = 2$. However this cannot occur in R. Therefore 2 is irreducible.
- As above the norm of 3 is 9. For the same reasoning for $xy = 3$ to hold we must have $N(x) = N(y) = 3$ but this cannot happen in R. Therefore 3 is irreducible.
- The norm of $1+\sqrt{-5}$ is 6. As such if $xy = 1+\sqrt{-5}$ holds we must have $N(x) = 2$ and $N(y) = 3$ or vice versa. However no such elements exist. Therefore $1+\sqrt{-5}$ is irreducible.
- The norm of $1-\sqrt{-5}$ is 6. As such if $xy = 1-\sqrt{-5}$ holds we must have $N(x) = 2$ and $N(y) = 3$ or vice versa. However no such elements exist. Therefore $1-\sqrt{-5}$ is irreducible.

Using this we have $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ which are two distinct factorizations of 6 in R which implies that R is not a UFD. □

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) The polynomial has no roots. As such it must be the product of two degree two irreducibles. However the only way this could occur is if $a + b = 10$ and $ab = 1$ which cannot happen with integers. Thus $x^4 + 10x^2 + 1$ is irreducible.

(d) This polynomial is irreducible by Eisenstein's Criterion with $p = 1$.

(e) This polynomial is irreducible by Eisenstein's Criterion with $p = 3$.

(f) First consider the polynomial in $\mathbb{Z}[x, y]/(y-1)$. Then the polynomial we get is x^2+x+1. The roots of the original are then forced to be ± 1 for x. However this is not the case and as such by Gauss' Lemma the polynomial is irreducible.
Consider $\mathbb{Z}[x, y]/(y - 1)$. Get $x^2 + x + 1$ root must be either ± 1. Use Gauss' lemma.

2. (a) Substitute $x - 1$ for x in the polynomial and it simplifies to $x^4 - 2x + 2$. Then it is irreducible by Eisenstein's Criterion with $p = 2$.

(b) First we simplify the polynomial

$$\begin{aligned}\frac{(x+2)^p - 2^p}{x} &= \frac{\sum_0^p \binom{p}{i} x^i 2^{p-i} - 2^p}{x} \\ &= \frac{\sum_1^p \binom{p}{i} x^i 2^{p-i}}{x} \\ &= \sum_0^{p-1} \binom{p}{i+1} x^i 2^{p-(i+1)}\end{aligned}$$

Now since p is prime we can use Eisenstein's Criterion with $p = 2$ to get that the polynomial is irreducible.

(c) From $\prod_1^n (x-i) - 1$ we can deduce that $a_n = 1$ and $a_0 = (-1)^n n! - 1$. This implies that a_0 will be prime and as such the polynomial will irreducible.

3. For $\mathbb{Z}_2[x]$ we have

$$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1$$

For $\mathbb{Z}_3[y]$ we have

$$y, y+1, y+2, 2y, 2y+1, 2y+2, y^2+1, y^2+y+2, y^2+2y+2, 2y^2+2, 2y^2+y+1,$$

$$2y^2+2y+1, y^3+2y+1, y^3+2y+2, y^3+y^2+2, y^3+y^2+y+2, y^3+y^2+2y+1, y^3+2y^2+1,$$

$$y^3+2y^2+y+1, y^3+2y^2+2y+2, 2y^3+y+1, 2y^3+y+2, 2y^3+y^2+2, 2y^3+y^2+y+1, 2y^3+y^2+2y+2,$$

$$2y^3+2y^2+1, 2y^3+2y^2+y+2, 2y^3+2y^2+2y+1$$

4. If $n = ab$ is composite we can rewrite it as

$$\begin{aligned}\sum_{0}^{n-1} x^i &= \frac{x^{ab}-1}{x-1} \\ &= \frac{x^a-1)(x^{ab-a)}+\cdots+1)}{x-1} \\ &= (x^{a-1}+\cdots+1)(x^{ab-a}+\cdots+1)\end{aligned}$$

which implies that f is reducible.

$\square$

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.

2. We listed f as an irreducible above. This implies K is a degree 3 field extension. The generator is x.

$$x, x^2, x+1, x^2+x, x^2+x+1, x^2+1, 1$$

$\square$

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. 1. For the first column there are p^2 possibilities to choose. However both values cannot be zero so we end up with $p^2 - 1$ choices for the first column. For the second column there are also p^2 choices but we must avoid the p multiples of the first column. As such there are $p^2 - p$ choices for the second column and as such the order of G is $(p^2-1)(p^2-p)$.

2. The order of G is 6. The only groups of order 6 are $\mathbb{Z}_6$ and S_3. However we have

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

which implies that G is not abelian. Therefore $G \cong S_3$.

$\square$

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. The order of G is $\varphi(247) = \varphi(13 \cdot 19) = (12)(18) = 216$.

2. By the Chinese Remainder Theorem we have that $\mathbb{Z}_{247} \cong \mathbb{Z}_{13} \times \mathbb{Z}_{19}$. This implies that $\mathbb{Z}_{247}^X = (\mathbb{Z}_{13} \times \mathbb{Z}_{19})^X$. For each component is 2. Thus the largest order in $\mathbb{Z}_{247}^X$ is $\mathrm{lcm}(12, 18) = 36$. By the structure theorem for finite abelian groups there the only possible structure for $\mathbb{Z}_{247}$ is $\mathbb{Z}_{36} \oplus \mathbb{Z}_6$.

$\square$

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. By the structure theorem for finite abelian groups there are three possibilities for groups of order 8. They are

$$\mathbb{Z}_8, \mathbb{Z}_2 \oplus \mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

1. The elements of $\mathbb{Z}_{15}^X$ are $\{1, 2, 4, 7, 8, 11, 13, 14\}$. The orders respectively are $1, 4, 2, 4, 4, 2, 4, 2$ which implies that the structure of the group is $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.
2. The group of roots is generated by $e^{\frac{\pi i}{4}}$. As such the structure is $\mathbb{Z}_8$.
3. The field with 8 elements has characteristic two. As such all elements in the additive group will have order 2. Therefore the structure is $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

$\square$

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.

1. In $F[x, y]/\langle x + 1, y - 2\rangle$ we have that $x + 1 = 0$ and $y - 2 = 0$ which implies that $x = -1$ and $y = 2$ in the quotient. As such any polynomial can be reduced to an element in F and as such the quotient is a field. Therefore $\langle x + 1, y - 2\rangle$ is a maximal ideal.
2. As above in $F[x, y]/P$ we get the relation that $X + Y + 1 = 0$. Since $F[x, y]$ is an integral domain the only way to get zero divisors in $F[x, y]/P$ would be if there are two nonzero polynomials that multiplied to $X + Y + 1$. However this cannot happen because the degree of $X + Y + 1 = 0$. Therefore the quotient $F[x, y]/P$ is an integral domain and as such P is a prime ideal.
3. It is not a maximal ideal. Note that $X \notin P$ which means that $\langle X, X + Y + 1\rangle = \langle X, Y + 1\rangle$ is an distinct ideal containing P. However this ideal is not all of $F[x, y]$. Therefore P is not maximal.

$\square$

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.

1. Let $f \in I$. Then $fg \in I$ for all $g \in J$ as I is an ideal. Therefore $I \subseteq I : J$.
2. We know that $P \subseteq P : \langle x\rangle$ by the previous part of the problem. Let $f \in P : \langle x\rangle$. Then $fx \in P$ however since P is prime and $x \notin P$ it follows that $f \in P$ and as such $P : \langle x\rangle \subseteq P$.

   Therefore $P = P : \langle x\rangle$ when P is prime and $x \notin P$.

$\square$

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.

1. For a commutative ring we have

$$I + J = \{f + g | f \in I, g \in J\}$$

and

$$IJ = \{fg | f \in I, g \in J\}$$

2. Since $I \subseteq I + J$, I, J are distinct, and I is maximal it follows that $I + J = R$.

Next we'll show that $I \cap J = IJ$. Let $fg \in IJ$ where $f \in I$ and $g \in J$. Then $fg \in I$ and $fg \in J$ which implies that $fg \in I \cap J$ and as such $IJ \subseteq I \cap J$.

Now suppose that $f \in I \cap J$. Then since I, J are maximal there exists $g \in I$ and $h \in J$ such that $1 = g + h$. Multiply by f to get $f = fg + fh$. We know that $fg \in IJ$ since $f \in J$ and $g \in I$. We also have that $fh \in IJ$ as $f \in I$ and $h \in J$. This implies that $fg + fh = f \in IJ$ and as such $I \cap J \subseteq IJ$.

Therefore $I \cap J = IJ$ and $I + J = R$.

□