Problem 1 (7.14). *1. Let R be a commutative ring with $1 \neq 0$ and $I_1, \ldots, I_n$ pairwise comaximal ideals of R. Prove that*

$$(R/(I_1 \ldots I_n))^X \cong (R/I_1)^X \times \ldots \times (R/I_n)^X$$

as groups.

2. *Let m, n be relatively prime positive integers. Prove that*

$$(\mathbb{Z}_{mn})^X \cong (\mathbb{Z}_m)^X \times (\mathbb{Z}_n)^X$$

as groups.

3. *Solve the system of congruences:*

$$\begin{aligned} x &\equiv 2 \mod 9 \\ x &\equiv 3 \mod 5 \\ x &\equiv 1 \mod 7 \\ x &\equiv 5 \mod 11 \end{aligned}$$

Proof. 1. By the Chinese Remainder Theorem we know that

$$(R/(I_1 \ldots I_n)) \cong (R/I_1) \times \ldots \times (R/I_n)$$

as rings. As such there is an isomorphism $\varphi : R \to S$ and since ring isomorphisms send units to units we have a bijection $\varphi|_{R^X} : R^X \to S^X$. However since φ is an isomorphism it will send identity to identity and preserve multiplication.

Thus $\varphi|_{R^X}$ is a group homomorphism and

$$(R/(I_1 \ldots I_n))^X \cong (R/I_1)^X \times \ldots \times (R/I_n)^X$$

are isomorphic as groups.

2. From a prior homework we have that $(n)(m) = (nm)$. Therefore $\mathbb{Z}_{mn} \cong \mathbb{Z}/m\mathbb{Z}n\mathbb{Z}$ in addition to $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$. Finally note that since $\gcd(n, m) = 1$ there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha a + \beta b = 1$ and therefore $(n) + (m) = \mathbb{Z}$. Thus we can apply part 1 of this problem to get that

$$\mathbb{Z}_{mn}^X \cong \mathbb{Z}_m^X \times \mathbb{Z}_n^X$$

3. $x \cong 533 \mod 3465$

$\square$

Problem 2 (8.1). *Prove that the division algorithm holds for any polynomial ring over a field.*

Proof. Let $f, g \in k[x]$ where k is a field. We will prove the division algorithm holds via induction over the degree of f.

Let $\deg(f) = 0$. Then $f = 0 \cdot g + f$ and since $\deg(f) = 0 < \deg(g)$ this is a valid choice for the division algorithm.

Assume that the division algorithm holds for polynomials $f \in k[x]$ when $\deg(f) = n$. Then given $g \in k[x]$ we have $f = qg + r$ where $\deg(g) > \deg(r)$. However we can form any given a polynomial $f' = \sum_0^{n+1} a_i x^i$ let $f := \sum_0^n a_{i+1} x^i + a_0$. Then $f' = x \cdot f + a_0$. Apply the division algorithm to f and we get

$$f' = x(qg + r) = (q \cdot x)g + x \cdot r$$

which shows that the division algorithm holds for $\deg = k + 1$ if we assume it for $\deg = k$.

Therefore the division algorithm holds for any polynomial ring over a field. $\square$

Problem 3 (8.2). *1. Prove that $a|b$ iff $b \in (a)$ iff $(b) \subseteq (a)$.*

2. If $a|b$ and $a|c$, prove that $a|(bx+cy)$ for all $x, y \in R$.

3. Suppose $b \neq 0$. If $a|b$ and $b|c$, then $a|c$.

4. If d is a greatest common divisor of a, b then du is also a greatest common divisor of a, b for any unit u of R.

Proof. 1. Suppose that $a|b$. Then there exists a c such that $ac = b$ which implies that $b \in (a)$.

Next suppose that $b \in (a)$ and let $d \in (b)$. Then $d = fb$. However $b = ca$ since $b \in (a)$ and as such $d = fca \in (a)$.

Finally suppose that $(b) \subseteq (a)$. Then $b \in (a)$ which implies that $b = ca$ for some c. This is the definition of $a|b$.

Therefore $a|b$ iff $b \in (a)$ iff $(b) \subseteq (a)$.

2. Suppose that $a|b$ and that $a|c$. Then there exist $\beta, \gamma \in R$ such that $a\beta = b$ and $a\gamma = c$. If we have $(bx + cy)$ we can substitute b, c to get

$$bx + cy = a\beta x + a\gamma c = a(\beta x + \gamma y)$$

which implies that $a|(bx + cy)$.

Therefore if $a|b$ and $a|c$ then $a|(bx + cy)$ for all $x, y \in R$.

3. Suppose that $a|b$ and $b|c$. Then there exist $\alpha, \beta \in R$ such that $\alpha a = b$ and $\beta b = c$. Thus $\beta\alpha a = c$ and therefore $a|c$.

4. Let d be a greatest common divisor of a, b. Then $d|a$, $d|b$ and if $d'|a, b$ then $d|d'$. Consider ud where u is a unit. Then du divides a, b as $\alpha d = a$ and $\beta d = b$ which implies that $\alpha u^{-1}(ud) = a$ and $\beta u^{-1}(ud) = b$. Thus $ud|a$ and $ud|b$. Now suppose that $f|a$ and $f|b$. Then $f|d$ which implies that $\gamma f = d$. It then follows that $u\gamma f = ud$ and thus $f|ud$.

Therefore ud is a greatest common divisor of a and b.

□

Problem 4 (8.3). *An element p in an integral domain R is prime if, and only if, $p|ab$ implies $p|a$ or $p|b$ for any $a, b \in R$.*

Proof. Let $p \in R$ be prime. Suppose that $p|ab$. Then $\alpha p = ab$ which implies that $ab \in (p)$. However since p is prime, (p) is a prime ideal. This means that either $a \in (p)$, in which case $p|a$, or $b \in (p)$ with $p|b$.

Otherwise suppose that when $p|ab$ then $p|a$ or $p|b$. Let $ab \in (p)$. Then $p|ab$ which implies that $p|a$, in which case $a \in (p)$, or $p|b$ and $b \in (p)$ which shows that (p) is prime.

Therefore an element p in an integral domain R is prime if, and only if, $p|ab$ implies that $p|a$ or $p|b$ for any $a, b \in R$. □

Problem 5 (8.4). *Let R be a UFD and $a, b \in R \setminus \{0\}$. Then a, b has a greatest common divisor in R. If a, b are relatively prime and $a|bc$ for some $c \in R$, then $a|c$.*

Proof. Let $a, b \in R \setminus \{0\}$. Since R is a UFD we have unique factorizations $a = p_1 \cdots p_s$ and $b = q_1 \cdots q_t$ which are unique up to associates and permutations. Define $f : R \to \mathbb{N}$ by $f(r)$ as the minimum number of occurrences of r in the factorization of a or b up to associates. Then define $d := \prod_{r \in \{p_i, q_i\}/\text{associates}} r^{f(r)}$. We know that $d|a$ and $d|b$ since d contains only factors of a and b. Moreover if $d'|a$ and $d'|b$ then $d'|d$ as d was defined to contain as many factors as possible while still dividing a, b. Thus d is a gcd of a, b.

Therefore if $a, b \in R \setminus \{0\}$ and R is a UFD, then a, b have a greatest common divisor. □

Problem 6 (G1)**.** *Let H be a normal subgroup of a group G, and let K be a subgroup of H.*

1. *Give an example of this situation where K is not a normal subgroup of G.*
2. *Prove that if the normal subgroup H is cyclic, then K is normal in G.*

Proof.

1. Consider S_5 and A_5. We know that $A_5 \trianglelefteq S_5$ however the subgroup $\langle (1\ 2\ 3) \rangle$ is not normal in S_5.
2. Since $H = \langle h \rangle$ is cyclic we know that $K = \langle h^a \rangle$ as well. Thus if we consider $ghg^{-1} = h^k \in H$. Then if we raise both sides to the power ap we get $(ghg^{-1})^{ap} = gh^{ap}g^{-1} = h^{(kp)a} \in K$.

   Therefore $K \trianglelefteq G$.

□

Problem 7 (G2)**.** *Prove that every finite group of order at least three has a nontrivial automorphism.*

Proof. Suppose that G is abelian. Then the map $a \mapsto a^{-1}$ is an automorphism.

Otherwise if G is not abelian then exists $gh \neq hg$. Then the map $f \mapsto gfg^{-1}$ will be an automorphism that is not trivial.

Therefore every finite group of order at least three has a non-trivial automorphism. □

Problem 8 (R1)**.** *Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\}$.*

1. *Why is R an integral domain?*
2. *What are the units in R?*
3. *Is the element 2 irreducible in R?*
4. *If $x, y \in R$, and $2|xy$, does it follow that 2 divides either x or y? Justify your answer.*

Proof.

1. Note that $\sqrt{-3} = i\sqrt{3}$. As such R is a subring of $\mathbb{C}$ which is a field. As such R cannot contain any zero divisors.
2. The units of R will be the elements $a + b\sqrt{-3}$ such that $a^2 + 3b^2 = \pm 1$. The negative case cannot happen and any nonzero value for b will make it too large. Therefore the only units of R are ± 1.
3. Since the norm is multiplicative if $rs = 2$ then $4 = N(r)N(s) = (ac)^2 + 3b^2c^2 + 3a^2d^2 + 9b^2d^2$. There are three was this can be fulfilled up to swapping r and s. Either $r = 2$ and $s = \pm 1$ or $r = (1 + \sqrt{3})$, $s = 1$. However the latter doesn't fulfill $rs = 2$ so we can discard it. Therefore 2 is irreducible in R

4. The number 2 is not prime in R as $2|(4 = (1+\sqrt{-3})(1-\sqrt{-3}))$ however $2 \nmid (1 \pm \sqrt{-3})$.

$\square$

Problem 9 (R2). *1. Give an example of an integral domain with exactly 9 elements.*

2. Is there an integral domain with exactly 10 elements? Justify your answer.

Proof. 1. $\mathbb{Z}_3[\sqrt{2}]$

2. When a ring is finite it is an integral domain if and only if it is a field. However fields must have prime power order and since 10 is not a prime power there cannot exist a field, and thus an integral domain, of order 10.

$\square$

Problem 10 (R3). *Let*

$$F = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} |a, b \in \mathbb{Q} \right\}$$

1. Prove that F is a field under the usual matrix operations of addition and multiplication.

2. Prove that F is isomorphic to the field $\mathbb{Q}(\sqrt{2})$.

Proof. 1. First we will show that F is closed under matrix addition and multiplication. Let

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}, \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} \in F$$

Then

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} + \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 2(b+d) & a+c \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} ac+2bd & bc+ad \\ 2(bc+ad) & ac+2bd \end{pmatrix}$$

Therefore F is a subring of $M_2(\mathbb{Q})$ and the only thing left to check is that all nonzero elements are units.

Suppose that we have an element $x \in F$ such that a, b are not both zero. Then $\det(x) \neq 0$ as that would require $a^2 - 2b^2 = 0$ which cannot happen in the rationals. Therefore x does indeed have an inverse.

2. Define $\varphi : F \to \mathbb{Q}(\sqrt{2})$ as

$$\varphi \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = a + b\sqrt{2}$$

Then we can define an inverse $\psi : \mathbb{Q}(\sqrt{2}) \to F$ as

$$\psi(a + b\sqrt{2}) = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$$

Clearly φ and ψ are inverses and as such φ is a bijection.

To show that φ is a ring homomorphism note that in part 1 of the problem the top two lines coincide with the values of the rational part and the $\sqrt{2}$ part of addition and multiplication respectively. Therefore φ is a ring isomorphism and as such $F \cong \mathbb{Q}(\sqrt{2})$.

$\square$