Exercise Sheet. You may assume that all rings in these exercises are commutative.

1. (a) List all the divisors of zero in $\mathbb{Z}_{20}$.
   (b) Prove that every non-zero element of $\mathbb{Z}_n$ is a unit or a divisor of zero.

2. Let $R$ be a commutative ring with identity. An element $a \in R$ is called nilpotent if $a^n = 0$ for some $n \in \mathbb{Z}^+$. Show that if $a$ is nilpotent, then $1 - a$ is a unit of $R$.
   (Hint: If $a^n = 0$, consider $1 - a^n$.)

3. Let $R$ be a ring. Show that if $R \neq \{0\}$, then $R^R$ has divisors of zero.

4. (a) Show that $2X + 1$ is a unit in $\mathbb{Z}_4[X]$.
   (b) Are any non-constant polynomials in $\mathbb{Z}[X]$ units?
   (c) If $p$ is prime, are any non-constant polynomials in $\mathbb{Z}_p[X]$ units?

5. Let $R$ be a ring with identity. Suppose $I$ is an ideal of $R$ and $I \neq R$. Show that if $u$ is a unit in $R$, then $u + I$ is a unit in $R/I$. Is the converse true?

6. (a) Give an example of a ring which is not a field itself for which some factor ring is a field.
   (b) Can a factor ring of a ring with divisors of zero be an integral domain?
   (c) Can a factor ring of an integral domain have divisors of zero?

7. Let $D$ be an integral domain and $a \in D$, $a \neq 0$.
   (a) Show that the map $\theta : D \to D$ defined by $\theta(x) = ax$ is injective (one-to-one).
   (b) Use (a) to prove that every finite integral domain is a field. (Hint: If $D$ is finite the map $\theta$ is also surjective.)
8. Let $D$ be an integral domain and $a, b \in D$. Prove that if $a^m = b^m$ and $a^n = b^n$, where $m, n$ are coprime positive integers, then $a = b$.

9. Let $D$ be an integral domain.

(a) Show that if $a \in D$ and $a^2 = 1$, then $a = 1$ or $a = -1$.

(b) Prove that if $D$ contains only finitely many units, then the product of these units is $-1$.

(c) Deduce from (b) that $\prod_{1 \leq a < n \atop (a,n) = 1} a \equiv -1 \pmod{n}$.

10. Let $R$ be the set $\{0, 2, 4, 6, 8\}$ under the operations of addition and multiplication mod 10. Prove that $R$ is a field.

11. (a) [Subfield Test] Let $F$ be a field and $E \subseteq F$. Show that $E$ is a subfield of $F$ if and only if the following hold:

(i) $1 \in E$,

(ii) if $\alpha, \beta \in E$ then $\alpha - \beta \in E$ and $\alpha\beta \in E$,

(iii) if $\alpha \in E \setminus \{0\}$ then $\alpha^{-1} \in E$.

(b) Prove that $E = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.

(c) Let $I$ denote the ideal of $\mathbb{Q}[X]$ generated by the polynomial $f(X) = X^2 - 3$. Prove that the map $\varphi : E \rightarrow \mathbb{Q}[X]/I$ defined by $\varphi(a + b\sqrt{3}) = (a + bX) + I$ is an isomorphism.

12. Prove that if $F$ is a field containing $2^n$ elements, then $\text{char}(F) = 2$.

13. Let $R, S, T$ be non-trivial rings with $S \leq R$ and suppose $\{0\} \neq I \triangleleft R$. For each of the following statements, determine whether it is true or false. Give reasons for your answers.

(1) $\text{char}(R) = \text{char}(S)$.

(2) $\text{char}(R) = \text{char}(R/I)$.

14. (a) Let $R$ be a commutative ring with no divisors of zero. Prove that all non-zero elements of $R$ have the same additive order. Do not assume that $R$ has an identity. [Hint. $(na)b = (nb)a$ for all $n \in \mathbb{Z}^+$ and all $a, b \in R$.]
(b) Let $D$ be an integral domain and $I$ an ideal of $D$ with $I \neq D$. Prove that if $D$ has characteristic $= p \neq 0$, then so does $D/I$.

What if $\text{char}(D) = 0$?

15. Let $p \in \mathbb{Z}^+$ be prime. Recall that $p$ divides the binomial coefficient $\binom{p}{i}$ for each $i = 1, 2, \ldots, p - 1$.

(a) Show that if $R$ is a commutative ring with 1 and $\text{char}(R) = p$, then $(a + b)^p = a^p + b^p$ for all $a, b \in R$, and the map $\varphi : R \to R$ defined by $\varphi(a) = a^p$ is a homomorphism (called the Frobenius homomorphism).

(b) Show that if $R$ is a finite field of characteristic $p$, then $\varphi$ is an automorphism of $R$.

16. Describe the field of quotients of the integral subdomain $D = \{n + mi \mid n, m \in \mathbb{Z}\}$ of $\mathbb{C}$.

17. Let $\alpha = \sqrt[3]{2}$ be the real cube root of 2, and put $D = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}\}$.

(a) Prove that $D$ is an integral domain.

(b) *Show that the field of quotients of $D$ is $F = \{r + s\alpha + t\alpha^2 \mid r, s, t \in \mathbb{Q}\}$.

18. (a) Show that the only automorphism of the field $\mathbb{Q}$ is the identity map on $\mathbb{Q}$.

(b) *Show that the only automorphism of the field $\mathbb{R}$ is the identity map on $\mathbb{R}$.

[ Aside: The field $\mathbb{C}$ has infinitely many automorphisms! Can you imagine what they might look like?]

19. In each of the following, find the quotient and remainder when $f(X)$ is divided by $g(X)$ in $F[X]$.

(1) $f(X) = X^6 + 3X^5 + 4X^2 - 3X + 2$, $g(X) = X^2 + 2X - 3$, and $F = \mathbb{Z}_7$.

(2) $f(X) = X^5 - 2X^4 + 3X - 5$, $g(X) = 2X + 1$, and $F = \mathbb{Z}_{11}$. 

3
20. In each of the following, the polynomial \( f(X) \) can be factored into linear factors in \( F[X] \). Find this factorization.

(1) \( f(X) = X^4 + 4 \) and \( F = \mathbb{Z}_5 \).

(2) \( f(X) = 2X^3 + 3X^2 - 7X + 5 \) and \( F = \mathbb{Z}_{13} \).

21. Let \( F \) be a field. Prove that every ideal of the polynomial ring \( F[X] \) is principal. (Hint. If \( I \) is a non-zero ideal of \( F[X] \), let \( d(X) \) be a polynomial of least degree in \( I \). Imitate the proof of the corresponding result for \( \mathbb{Z} \) to show that \( I = \langle d(X) \rangle \).)

22. (a) Is there a Division Algorithm for polynomials in \( \mathbb{Z}[X] \)? That is, if \( f(X), g(X) \in \mathbb{Z}[X] \) have degrees \( \geq 1 \), do there exist \( q(X), r(X) \in \mathbb{Z}[X] \) such that \( f(X) = g(X)q(X) + r(X) \) and \( r(X) = 0 \) or \( \deg r(X) < \deg g(X) \)?

(b) The same as (a) for polynomials in \( \mathbb{Z}[X, Y] \).

23. Prove the **Rational Zeros Theorem**:

Let \( f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X] \) have degree \( \geq 1 \). If the rational number \( r/s \) (in lowest terms, i.e., \( (r, s) = 1 \)) is a zero of \( f(X) \), then \( r \mid a_0 \) and \( s \mid a_n \).

[Hint: If \( f(r/s) = 0 \), then \( a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s) + a_0 = 0 \). Multiply both sides by \( s^n \) and consider the resulting equation in \( \mathbb{Z} \).]