CATEGORY THEORY
RING THEORY
A WORKSHEET APPROACH

PAUL L. BAILEY

Worksheet Instructions

Here is a series of definitions and problems designed with the intent to help you master the essential aspects of ring theory. If you would like to use them, I suggest that you proceed as follows.

You may assume all of your previous knowledge of sets, functions, and numbers. In particular, understand and use the propositions regarding integers, such as prime factorization and the formulas $n = mq + r$ and $xm + yn = \gcd(m, n)$. Try to use only that knowledge of group theory that seems presupposed by the problem.

Proceed directly from the definitions on the worksheet without looking in the book for further explanation or proofs. I think that all problems can be solved using the previous knowledge mentioned above, definitions given in the worksheets, and previous results that you will have shown from the worksheets. I've found that for me, after having been exposed to the subject initially, this is really the best way to learn abstract mathematics.

For some of the worksheets, you may wish to merely read the definitions and statements so that you can use them on later worksheets.

For some of the problems, you may see the proof clearly without writing it down. For other problems, it probably is a good idea to try to write a proof on paper.

The definition of ring here is slightly different from that used by some authors (e.g. Fraleigh), and we have corresponding differences in the definition of subring and homomorphism:

- Assume that all rings have a multiplicative identity, or unity;
- Assume that all subrings contain the same unity;
- Assume that all ring homomorphisms send unity to unity.

This approach simplifies some statements about the cases in which we are most interested, and is standard in algebraic geometry, where commutative ring theory plays the leading role.

Date: November 26, 2019.

Worksheet I - Rings

Definition 1. A *ring* is a set R together with a pair of binary operations

$$+ : R \times R \to R \text{ and } \cdot : R \times R \to R$$

such that
(R1) $a + b = b + a$ for every $a, b \in R$;
(R2) $(a + b) + c = a + (b + c)$ for every $a, b, c \in R$;
(R3) there exists $0 \in R$ such that $a + 0 = a$ for every $a \in R$;
(R4) for every $a \in R$ there exists $-a \in R$ such that $a + (-a) = 0$;
(R5) $(ab)c = a(bc)$ for every $a, b, c \in R$;
(R6) there exists $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for every $a \in R$;
(R7) $a(b + c) = ab + ac$ for every $a, b, c \in R$;
(R8) $(a + b)c = ac + bc$ for every $a, b, c \in R$.

Remark 1. Properties **(R1)** through **(R4)** say that R is an abelian group under addition. Properties **(R5)** and **(R6)** say that R is a monoid under multiplication. Properties **(R7)** and **(R8)** relate the two binary operations on R.

Definition 2. We say that a ring R is *commutative* if $ab = ba$ for every $a, b \in R$.

Problem 1. Let R be a ring and let $x, y \in R$ such that $x + a = a$ and $y + a = a$ for every $a \in R$.
Show that $x = y$. Thus 0 is unique. We call 0 the *additive identity*, or *zero*, of R.

Problem 2. Let R be a ring and let $x, y \in R$ such that $xa = ax = a$ and $ya = ay = a$ for every $a \in R$.
Show that $x = y$. Thus 1 is unique. We call 1 the *multiplicative identity*, or *unity*, of R.

Problem 3. Let R be a ring and let $a, b, c \in R$ such that $a + b = 0$ and $a + c = 0$.
Show that $b = c$. Thus $-a$ is unique. We call $-a$ the *additive inverse* of a.

Problem 4. Let R be a ring and let $a, b, c \in R$ and suppose that $ab = ba = 1$ and $ac = ca = 1$.
Show that $b = c$. Denote such an element by a^{-1}. Thus a^{-1} is unique if it exists. We call a^{-1} the *multiplicative inverse*, or simply the *inverse*, of a.

Remark 2. The standard rules for additive and multiplicative notation are in force.

The additive identity is denoted by 0 and the additive inverse of a is denoted $-a$. If $n \in \mathbb{Z}$, then $na = 0$ if $n = 0$, $na = a + \cdots + a$ (n times) if $n > 0$, and $na = (-a) + \cdots + (-a)$ (n times) if $n < 0$.

The multiplicative identity is denoted by 1 and the multiplicative inverse of a (if it exists) is denoted by a^{-1}. If $n \in \mathbb{N}$, then $a^n = 1$ if $n = 0$ and $a^n = a \cdot \cdots \cdot a$ (n times) if $n > 0$. If a has a multiplicative inverse and $n < 0$, then $a^n = (a^{-1})^{-n}$. The notation 0^0 is undefined. The product symbol $\cdot$ may be dropped, so that multiplication is denoted by juxtiposition.

Problem 5. Let R be a ring and let $a, b \in R$.
(a) Show that $a \cdot 0 = 0 \cdot a = 0$.
(b) Show that $(-a)b = a(-b) = -(ab)$.

Problem 6. Let R be a ring and let $a, b \in R$. Let $n \in \mathbb{N}$.
(a) Show that $n(ab) = (na)b = a(nb)$.
(b) Show that $(-n)a = -(na)$.

Remark 3. To emphasize that a certain element acts as an identity in the ring R, we may write 0_R or 1_R instead of just 0 or 1. This is useful when comparing rings.

Worksheet II - Examples of Rings

Remark 4. To show that R is a ring, you must verify that the given operations addition and multiplication are well-defined functions from $R \times R$ to R, and that they satisfy the properties **(R1)** through **(R8)**.

In practice, however, many of these steps are tedious, and only the ones in question or of interest are verified. In particular, check that the binary operations are well-defined (if this is an issue) and closed (that is, into R); specify the zero, the form of additive inverses, the unity, and the form of multiplicative inverses.

Problem 7. Let $R = \{0\}$. Define $0 + 0 = 0$ and $0 \cdot 0 = 0$.
Show that R is a ring, called the *zero ring* .

Remark 5. If R is a ring in which the additive and multiplicative identities are the same element, then R is the zero ring, because if $a \in R$, then $0 = 0 \cdot a = 1 \cdot a = a$, so $a = 0$.

Problem 8. Verify that the following are rings under their standard addition and multiplication:
(a) $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, the integers;
(b) $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}\}$, the rational numbers;
(c) $\mathbb{R}$, the real numbers;
(d) $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}$, the complex numbers.

Problem 9. Let R and S be rings. Define addition and multiplication on their cartesian product $R \times S$ coordinatewise by

- $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$;
- $(r_1, s_1) \cdot (r_2, s_2) = (r_1 s_1, r_2 s_2)$.

Verify that $R \times S$ is a ring, called the *product ring* of R and S.

Problem 10. Let X be a set and let $\mathcal{P}(X)$ be the collection of all subsets of X. Define addition and multiplication on $\mathcal{P}(X)$ by

- $A + B = A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$;
- $A \cdot B = A \cap B$.

Verify that $\mathcal{P}(X)$ is a commutative ring, called the *power set* of X.

Problem 11. Let X be a set and let R be a ring. Let $\mathcal{F}(X, R)$ denote the set of all functions from X to R. Define addition and multiplication of functions in $\mathcal{F}(X, R)$ pointwise by

- $(f + g)(x) = f(x) + g(x)$;
- $(f \cdot g)(x) = f(x)g(x)$.

Verify that $\mathcal{F}(X, R)$ is a ring, called the *ring of functions* from X to R.

Problem 12. Let A be an additive abelian group and set

$$\text{End}(A) = \{f : A \to A \mid f(a + b) = f(a) + f(b) \text{ for all } a, b \in A\}.$$

Define addition and multiplication of functions in $\text{End}(A)$ by

- $(f + g)(a) = f(a) + g(a)$;
- $(f \cdot g)(a) = f \circ g(a) = f(g(a))$.

Verify that $\text{End}(A)$ is a ring, called the *ring of endomorphisms* of A.

Worksheet III - Commutative Invertibility and Entireness

Definition 3. Let R be a commutative ring and let $a \in R$.
We say that a is *entire* if $ab = 0 \Rightarrow b = 0$ for every $b \in R$.
We say that a is *cancellable* if $ab = ac \Rightarrow b = c$ for every $b, c \in R$.
We say that a is *invertible* if there exists an element $a^{-1} \in R$ such that $aa^{-1} = 1$.

Problem 13. Let R be a commutative ring and let $a \in R$. Show that a is entire if and only if a is cancellable.

Problem 14. Let R be a commutative ring and let $a \in R$. Show that if a is invertible, then a is entire.

Definition 4. Let R be a nonzero commutative ring. Set

$$R^* = \{x \in R \mid x \text{ is invertible } \}$$

and

$$R^\bullet = \{x \in R \mid x \text{ is entire } \}.$$

Problem 15. Let R and S be nonzero commutative rings.
(a) Show that $(R \times S)^* = R^* \times S^*$.
(b) Show that $(R \times S)^\bullet = R^\bullet \times S^\bullet$.

Problem 16. Let R be a nonzero commutative ring. Show that R^* is an abelian group under multiplication.

Definition 5. Let R be a commutative ring and let $a \in R$.
We say that a is a *zero divisor* if $a \neq 0$ and there exists $b \in R \smallsetminus \{0\}$ such that $ab = 0$.

Problem 17. Let R be a commutative ring and let $a \in R$.
Show that a is a zero divisor if and only if a is a nonzero nonentire element of R.

Problem 18. Let R and S be commutative rings and let A be the set of zero divisors in $R \times S$. Show that

$$A = R \times S \smallsetminus ((R^\bullet \times S^\bullet) \cup \{(0_R, 0_S)\}).$$

Definition 6. Let R be a nonzero commutative ring.
We say that R is an *integral domain* if every nonzero element of R is entire.
We say that R is a *field* if every nonzero element of R is invertible.

Problem 19. Let R be a commutative ring. Show that if R is a field, then R is an integral domain.

Problem 20. Let R be a finite integral domain. Let $a \in R \smallsetminus \{0\}$ and define a function

$$\mu_a : R \to R \quad \text{given by } \mu_a(x) = ax.$$

(a) Show that μ_a is injective.
(b) Show that μ_a is surjective.
(c) Show that a is invertible.
(d) Conclude that R is a field.

Worksheet IV - General Invertibility and Entireness

Definition 7. Let R be a ring and let $a \in R$.
We say that a is *entire* if $ab = 0 \Rightarrow b = 0$ and $ba = 0 \Rightarrow b = 0$ for every $b \in R$.
We say that a is *cancellable* if $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$ for every $b, c \in R$.
We say that a is *invertible* if there exists an element $a^{-1} \in R$ such that $aa^{-1}a^{-1}a = 1$.

Remark 6. These definitions are compatible with our defintions in the commutative case, and supercede them.

Problem 21. Let R be a ring and let $a \in R$. Suppose that there exist $b, c \in R$ such that $ab = 1$ and $ca = 1$. Show that $b = c$, so that a is invertible.

Problem 22. Let R be a ring and let $a \in R$. Show that a is entire if and only if a is cancellable.

Problem 23. Let R be a ring and let $a \in R$. Show that if a is invertible, then a is entire.

Definition 8. Let R be a nonzero ring. Set

$$R^* = \{x \in R \mid x \text{ is invertible } \}$$

and

$$R^\bullet = \{x \in R \mid x \text{ is entire } \}.$$

Problem 24. Let R and S be nonzero rings.
(a) Show that $(R \times S)^* = R^* \times S^*$.
(b) Show that $(R \times S)^\bullet = R^\bullet \times S^\bullet$.

Problem 25. Let R be a nonzero ring. Show that R^* is a group under multiplication.

Definition 9. Let R be a ring and let $a \in R$.
We say that a is a *zero divisor* if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that $ab = 0$ or $ba = 0$.

Problem 26. Let R be a ring and let $a \in R$.
Show that a is a zero divisor if and only if a is a nonzero nonentire element of R.

Problem 27. Let R and S be rings and let A be the set of zero divisors in $R \times S$. Show that

$$A = R \times S \setminus ((R^\bullet \times S^\bullet) \cup \{(0_R, 0_S)\}.$$

Definition 10. Let R be a nonzero ring.
We say that R is a *domain* if every nonzero element of R is entire.
We say that R is a *division ring* if every nonzero element of R is invertible.

Problem 28. Let R be a ring. Show that if R is a division ring, then R is an domain.

Problem 29. Let R be a finite domain. Show that R is a division ring.

Worksheet V - Subrings

Definition 11. Let R be a ring. A *subring* of R is a subset $S \subset R$ such that
(S0) $1 \in S$;
(S1) $a, b \in S \Rightarrow a + b \in S$;
(S2) $a \in S \Rightarrow -a \in S$;
(S3) $a, b \in S \Rightarrow ab \in S$.
If S is a subring of R, we write $S \leq R$.

Remark 7. Properties **(S1)** and **(S2)** say that S is an additive subgroup of R.

Problem 30. Let R be a ring and let $S \leq R$.
Show that the restriction of $+$ and $\cdot$ to $S \times S$ induces a ring structure on S.

Problem 31. Let R be a ring. Show that $R \leq R$.

Problem 32. Let F be a field and let $R \leq F$. Show that R is an integral domain.

Problem 33. Let R be a ring and define the *center* of R to be

$$Z(R) = \{x \in R \mid xy = yx \text{ for all } y \in R\}.$$

Show that $Z(R) \leq R$.

Definition 12. A *subfield* of R is a subring $F \leq R$ such that
(F1) $a, b \in F \Rightarrow ab = ba$;
(F2) $a \in F \setminus \{0\} \Rightarrow a$ is invertible and $a^{-1} \in F$.

Problem 34. Let R be a ring and let $F \leq R$ be a subfield.
Show that the restriction of $+$ and $\cdot$ to $F \times F$ induces a field structure on F.

Definition 13. Let X be a set and let $\mathcal{C} \subset \mathcal{P}(X)$ be a collection of subsets of X. Define the *intersection* and *union* of the collection by

- $\cap\mathcal{C} = \{x \in X \mid x \in C \text{ for all } C \in \mathcal{C}\}$;
- $\cup\mathcal{C} = \{x \in X \mid x \in C \text{ for some } C \in \mathcal{C}\}$.

Problem 35. Let R be a ring and let $\mathcal{S}$ be a nonempty collection of subrings of R.
Show that $\cap\mathcal{S}$ is a subring of R.

Problem 36. Let R be a ring and let $\mathcal{S}$ be a nonempty collection of subfields of R.
Show that $\cap\mathcal{S}$ is a subfield of R.

Definition 14. Let R be a ring and let $X \subset R$. The *subring generated by* X is denoted by $\mathrm{gr}_R(X)$ and is defined to be the intersection of all subrings of R which contain X.

Problem 37. Let R be a ring and let $X \subset R$. Show that $\mathrm{gr}_R(X) \leq R$.

Problem 38. Let R be a ring and let $X, Y \subset R$. Show that if $X \subset Y$, then $\mathrm{gr}_R(X) \leq \mathrm{gr}_R(Y)$.

Problem 39. Let R be a ring and let $X, Y \subset R$. Show that $\mathrm{gr}_R(X \cap Y) \subset \mathrm{gr}_R(X) \cap \mathrm{gr}_R(Y)$.

Problem 40. Let R be a ring and let $X, Y \subset R$. Give an example where $\mathrm{gr}_R(X \cap Y) \neq \mathrm{gr}_R(X) \cap \mathrm{gr}_R(Y)$.

Definition 15. Let F be a field and let $X \subset F$. The *subfield generated by* X is denoted by $\mathrm{gf}_F(X)$ and is defined to be the intersection of all subfields of F which contain X.

Problem 41. Let F be a field and let $X, Y \subset F$. Show that $\mathrm{gf}_F(X \cap Y) \subset \mathrm{gf}_F(X) \cap \mathrm{gf}_F(Y)$.

Worksheet VI - Ring Homomorphisms

Definition 16. Let R and S be rings. A *ring homomorphism* from R to S is a function $\phi : R \to S$ such that
(H0) $\phi(1_R) = 1_S$;
(H1) $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$;
(H2) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.

A bijective ring homomorphism is called a *ring isomorphism*. If there exists a ring isomorphism from R to S we say that R and S are *isomorphic*, and write $R \cong S$.

An isomorphism from a ring onto itself is called a *ring automorphism*.

Remark 8. Property **(H1)** says that ϕ is an additive group homomorphism.

Problem 42. Let $\phi : R \to S$ be a ring homomorphism.
(a) Show that $\phi(0_R) = 0_S$.
(b) Show that $\phi(-r) = -\phi(r)$ for every $r \in R$.

Problem 43. Let $\phi : R \to S$ be a ring homomorphism with S nonzero.
Show that if $r \in R$ is invertible, then $\phi(r)$ is invertible and $\phi(r^{-1}) = \phi(r)^{-1}$.

Problem 44. Give an example of a ring homomorphism $\phi : R \to S$ such that $\phi(r) = s$ for some $r \in R$, $s \in S$, where s is invertible but r is not.

Problem 45. Let $\phi : R \to S$ be a ring isomorphism. Then $\phi^{-1} : S \to R$ is a bijective function. Show that ϕ^{-1} is a ring isomorphism.

Problem 46. Let $\phi : R \to S$ be a ring homomorphism and let $T \leq R$.
Show that $\phi(T) \leq S$.

Problem 47. Let $\phi : R \to S$ be a ring homomorphism and let $T \leq S$.
Show that $\phi^{-1}(T) \leq R$.

Problem 48. Let $\phi : R \to S$ and $\psi : S \to T$ be ring homomorphisms.
Show that $\psi \circ \phi : R \to T$ is a ring homomorphism.

Problem 49. Let $\phi : R \to S$ be a ring homomorphism and let $X \subset R$.
Show that $\phi(\mathrm{gr}_R(X)) = \mathrm{gr}_S(\phi(X))$.

Problem 50. Let E and F be a fields.
Let $\phi : E \to F$ be a ring homomorphism and let $X \subset E$.
Show that $\phi(\mathrm{gf}_E(X)) = \mathrm{gf}_F(\phi(X))$.

Problem 51. Let $\phi : R \to S$ be a ring homomorphism. Let $\phi^* : R^* \to S$ be the restriction of ϕ to R^*.
(a) Show that $\phi^* : R^* \to S^*$ is a group homomorphism.
(b) Show that if ϕ is an bijective, then ϕ^* is bijective.

Problem 52. Let $\phi : F \to S$ be a ring homomorphism, where F is a field and S is nonzero.
Show that ϕ is injective. Thus the image of F in S is a subfield of S which is isomorphic to F.

Worksheet VII - Ideals

Definition 17. Let R be a ring. An *ideal* of R is a subset $I \subset R$ such that
(I1) $a, b \in I \Rightarrow a + b \in I$;
(I2) $a \in I$ and $r \in R \Rightarrow ra, ar \in I$.
If I is an ideal of R, we write $I \lhd R$.

Remark 9. Since $-1 \in R$, properties **(I1)** and **(I2)** say that I is an additive subgroup of R.

Problem 53. Let R be a ring. Show that $\{0\} \lhd R$ and $R \lhd R$.

Definition 18. Let R be a ring and let $I \lhd R$.
We say that I is *improper* if $I = R$; otherwise I is *proper*.
We say that I is *trivial* if $I = \{0\}$; otherwise I is *nontrivial*.
We say that R is *simple* if $I \lhd R \Rightarrow I = \{0\}$ or $I = R$.

Problem 54. Let R be a ring and $I \lhd R$. Show that if I contains an invertible element, then I is improper.

Problem 55. Let R be a commutative ring. Show that R is simple if and only if R is a field.

Problem 56. Let R be a ring and let $\mathcal{I}$ be a collection of ideals of R. Show that $\cap\mathcal{I} \lhd R$.

Problem 57. Let R be a ring and let $I, J \lhd R$. Set

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

Show that $I + J \lhd R$.

Definition 19. Let $\phi : R \to S$ be a ring homomorphism. The *kernel* of ϕ is denoted by $\ker(\phi)$ and is defined to be the subset of R given by

$$\ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}.$$

Problem 58. Let $\phi : R \to S$ be a ring homomorphism.
Show that $\ker(\phi) \lhd R$.

Problem 59. Let $\phi : R \to S$ be a ring homomorphism.
Show that ϕ is injective if and only if $\ker(\phi) = \{0\}$.

Problem 60. Let $\phi : R \to S$ be a ring homomorphism and let $J \lhd S$.
Show that $\phi^{-1}(J) \lhd R$.

Problem 61. Let $\phi : R \to S$ be a surjective ring homomorphism and let $I \lhd R$.
Show that $\phi(I) \lhd R$.

Problem 62. Give an example of a nonsurjective ring homomophism $\phi : R \to S$ and an ideal $I \lhd R$ such that $\phi(I)$ is not an ideal in S.

Problem 63. Let R be a ring and let $\mathcal{I}$ be a nonempty collection of ideals in R. Show that $\cap\mathcal{I} \lhd R$.

Definition 20. Let R be a ring and let $X \subset R$. The *ideal generated by* X is denoted $\mathrm{gi}_R(X)$ or $\langle X \rangle$ and is defined to be the intersection of all ideals of R which contain X.

Problem 64. Let R be a ring and let $I, J \lhd R$. Show that $\mathrm{gi}_R(I \cup J) = I + J$.

Problem 65. Let $\phi : R \to S$ be a surjective ring homomorphism and let $X \subset R$.
Show that $\phi(\mathrm{gi}_R(X)) = \mathrm{gi}_S(\phi(X))$.

Worksheet VIII - Factor Rings

Definition 21. Let R be a ring and let $I \lhd R$. Let $x \in R$. The *coset* for x of I in R is the set

$$x + I = \{x + a \mid a \in I\}.$$

Let $x, y \in R$. We say that x and y are *congruent modulo* I, and write $x \equiv y \mod I$, if $x - y \in I$.

Problem 66. Let R be a ring and let $I \lhd R$.
(a) Show that $0 \in I$.
(b) Let $x, y \in R$. Show that $x + I = y + I \Leftrightarrow x - y \in I$.

Remark 10. Recall that the *cardinality* of a set X is denoted $|X|$ and is (loosely speaking) the number of elements in the set. To show that $|X| = |Y|$, is suffices to find a bijective function from X to Y.

Problem 67. Let R be a ring and let $I \lhd R$.
(a) Show that congruence modulo I is an equivalence relation.
(b) Show that the congruence classes modulo I are the cosets of I in R.
(c) Show that $|x + I| = |y + I|$ for every $x, y \in R$.
(d) Conclude that if R is finite, then the cardinality of R is equal to the cardinality of I times the number of cosets of I in R.

Problem 68. Let R be a ring and let $I \lhd R$. Let R/I denote the collection of cosets of I in R. Define addition and multiplication on R/I by $(x + I) + (y + I) = (x + y) + I$ and $(x + I)(y + I) = xy + I$. Show that these operations are well-defined and induce a ring structure on R/I. We call R/I a *factor ring*, or the *quotient* of R by I.

Problem 69. Let R be a ring and let $I \lhd R$. Define a function $\beta : R \to R/I$ by $\beta(x) = x + I$. Show that β is a surjective ring homomorphism whose kernel is I. We call β the *canonical* homomorphism from R to R/I.

Remark 11. Thus every kernel is an ideal and every ideal is a kernel.

Definition 22. Let R be a ring and let $r, s \in R$. Then *Lie bracket* of r and s is

$$[r, s] = rs - sr.$$

Problem 70. Let R be a ring and set

$$I = \mathrm{gi}_R(\{[r, s] \mid r, s \in R\}).$$

Show that R/I is commutative.

Problem 71. Let R be a commutative ring and set

$$I = \mathrm{gi}_R(R \setminus R^*).$$

Show that if I is a proper ideal, then R/I is a field.

Worksheet IX - Isomorphism Theorem

Problem 72. (Isomorphism Theorem)
Let $\phi : R \to S$ be a ring homomorphism and let $K = \ker(\phi)$. Let $\beta : R \to R/K$ be the canonical homomorphism. Define a function $\overline{\phi} : R/K \to S$ by $\overline{\phi}(x + K) = \phi(x)$.
(a) Show that $\overline{\phi}$ is well-defined.
(b) Show that $\overline{\phi}$ is an injective ring homomorphism.
(c) Show that $\phi = \overline{\phi} \circ \beta$.
(d) Show that if ϕ is surjective, then $\overline{\phi}$ is a ring isomorphism.

Remark 12. Thus every homomorphic image of R is isomorphic to a quotient of R, and every quotient of R is a homomorphic image of R.

Problem 73. Let R be a ring and let $I, J \lhd R$ such that $I \subset J$. Let $\beta : R \to R/I$ and $\alpha : R \to R/J$ be the canonical homomorphisms. Set $J/I = \{a + I \in R/I \mid a \in J\}$. Define $\gamma : R/I \to R/J$ by $\gamma(a + I) = a + J$.
(a) Show that γ is a well-defined surjective ring homomorphism.
(b) Show that $\alpha = \gamma \circ \beta$.
(c) Show that $J/I \lhd R/I$.
(d) Show that

$$\frac{R}{J} \cong \frac{R/I}{J/I}.$$

Problem 74. (Correspondence Theorem)
Let $\phi : R \to S$ be a surjective ring homomorphism and let $K = \ker(\phi)$. Set

$$\mathcal{I} = \{I \lhd R \mid K \subset I\} \quad \text{and} \quad \mathcal{J} = \{J \lhd S\}.$$

Define a function

$$\Phi : \mathcal{I} \to \mathcal{J} \quad \text{by} \quad \Phi(I) = \phi(I).$$

(a) Show that Φ is bijective.
(b) Show that $I_1 \subset I_2 \Leftrightarrow \Phi(I_1) \subset \Phi(I_2)$.

Remark 13. Thus the ideals in the range of a ring homomorphism correspond to the ideals in the domain which contain the kernel. This correspondence is inclusion preserving. Via the isomormorphism theorem, this is equivalent to the fact that the ideals in R which contain I correspond to the ideals in R/I.

Problem 75. (Chinese Remainder Theorem)
Let R be a commutative ring and let $I, J \lhd R$ such that $I + J = R$.
Define a function $\phi : R \to R/I \times R/J$ by $\phi(r) = (r + I, r + J)$.
(a) Show that for every $a \in R$ there exist $x, y \in R$ such that $x \equiv a \mod I$ and $y \equiv a \mod J$.
(b) Show the ϕ is a surjective homomorphism with kernel $I \cap J$.
(c) Conclude that

$$R/(I \cap J) \cong R/I \times R/J.$$

Worksheet X - Characteristic

Problem 76. Let $\mathbb{Z}$ be the set of integers and for $n \in \mathbb{Z}$, set $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$.
Show that $n\mathbb{Z} \triangleleft \mathbb{Z}$, so that $\mathbb{Z}/n\mathbb{Z}$ is a ring.

Problem 77. Let $I \triangleleft \mathbb{Z}$. Show that there exists a unique nonnegative integer $n \in \mathbb{Z}$ such that $I = n\mathbb{Z}$. We say that n *generates* I, since I is the ideal generated by the set $\{n\}$ in $\mathbb{Z}$.

Definition 23. Let n be a positive integer. Set $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. We call $\mathbb{Z}_n$ the *ring of integers modulo* n.

Problem 78. Let n be a positive integer. Show that the following conditions are equivalent.

(i) n is prime;
(ii) $\mathbb{Z}_n$ is an integral domain;
(iii) $\mathbb{Z}_n$ is a field.

Remark 14. Thus every quotient of $\mathbb{Z}$ by a nontrivial ideal is either a field or a nondomain. We will see later that this holds for every commutative ring R whose ideals are of the form aR for some $a \in R$.

Problem 79. Let R be a ring. Show that there exists a unique ring homomorphism $\phi : \mathbb{Z} \to R$.

Definition 24. Let R be a ring and let $\phi : \mathbb{Z} \to R$ be the unique ring homomorphism from $\mathbb{Z}$ to R.
The *characteristic* of R is the unique nonnegative generator of $\ker(\phi)$. Denote this integer by $\mathrm{char}(R)$.
The *characteristic subring* of R is $\phi(\mathbb{Z})$, the image of $\mathbb{Z}$ in R under ϕ. Denote this subring by $H(R)$.

Remark 15. Viewing a ring R as an additive group, let $\mathrm{ord}^+(a)$ denote the additive order of $a \in R$.

Problem 80. Let R be a ring and let $\phi : \mathbb{Z} \to R$ be the unique ring homomorphism from $\mathbb{Z}$ to R. Let $n \in \mathbb{N}$ be a positive integer. Show that the following statements are equivalent:

(i) $n = \mathrm{char}(R)$;
(ii) $n = \mathrm{ord}^+(1)$;
(iii) $na = 0$ for every $a \in R$;
(iv) $H(R) \cong \mathbb{Z}_n$.

Problem 81. Let R be a ring.
(a) Show that $H(R) = \mathrm{gr}_R(\{1\})$.
(b) Show that $H(R) \leq Z(R)$.

Problem 82. Let D be an integral domain.
(a) Show that either $\mathrm{char}(R) = 0$ or $\mathrm{char}(R) = p$ for some prime p.
(b) Show that either $H(R) \cong \mathbb{Z}$ or $H(R) \cong \mathbb{Z}_p$ for some prime p.

Problem 83. Let R be a ring and let $\phi : R \to R$ be an automorphism.
Show that $\phi(a) = a$ for every $a \in H(R)$.

Worksheet XI - Principal, Maximal, and Prime Ideals

Definition 25. Let R be a ring and let $I \lhd R$.
We say that I is a *principal ideal* if $I = \text{gi}_R(\{a\})$ for some $a \in R$.

Problem 84. Let R be a commutative ring and let $a \in R$. Let $aR = \{ax \mid x \in R\}$.
Show that aR is a principal ideal.

Problem 85. Let R be a commutative ring and let $I \lhd R$ be a principal ideal.
Show that there exists $a \in R$ such that $I = aR$.

Problem 86. Let $\phi : R \to S$ be a surjective ring homomorphism, where R is commutative.
(a) Let $a \in R$. Show that $\phi(aR) = \phi(a)S$.
(b) Conclude that the surjective homomorphic image of a principal ideal is principal.

Definition 26. A *principal ring* is a commutative ring in which all ideals are principal.

Problem 87. Let R be a principal ring.
(a) Let $I \lhd R$. Show that R/I is a principal ring.
(b) Let $\phi : R \to S$ be a surjective ring homomorphism. Show that S is a principal ring.

Definition 27. A *principal ideal domain* (pid) is an integral domain in which all ideals are principal.

Remark 16. Recall that every ideal in $\mathbb{Z}$ is generated by a unique nonnegative integer. Thus $\mathbb{Z}$ is a pid.

Definition 28. Let R be a commutative ring and let $I \lhd R$.
We say that I is *prime* if $ab \in I \Rightarrow a \in I$ or $b \in I$ for all $a, b \in R$.

Problem 88. Let R be a commutative ring.
Show that $\{0\}$ is a prime ideal if and only if R is an integral domain.

Problem 89. Let R be a commutative ring and let $I \lhd R$.
Show that I is prime if and only if R/I is an integral domain.

Definition 29. Let R be a commutative ring and let $I \lhd R$.
We say that I is *maximal* if whenever $I \subset J \lhd R$, then either $J = I$ or $J = R$.

Problem 90. Let R be a commutative ring.
Show that $\{0\}$ is maximal if and only if R is a field.

Problem 91. Let R be a commutative ring and let $I \lhd R$.
Show that I is maximal if and only if R/I is a field.
(Hint: use the Correspondence Theorem.)

Problem 92. Let R be a commutative ring and let $I \lhd R$.
Show that if I is maximal, then I is prime.

Problem 93. Let R be a pid and let $I \lhd R$ be a nontrivial proper ideal.
Show that I is maximal if and only if I is prime.

Problem 94. Let R be a pid and let $I \lhd R$ be a nontrivial proper ideal.
Show that R/I is either a field or a nondomain.

Problem 95. Let $\phi : R \to S$ be a ring homomorphism, where R is a pid.
Show that $\phi(R)$ is either a field or a nondomain.

Problem 96. Let R and S be commutative rings and let $\phi : R \to S$ be a ring homomorphism. Let $J \lhd S$.
(a) Show that if J is prime, then $\phi^{-1}(J)$ is prime.
(b) Show that if J is maximal, then $\phi^{-1}(J)$ is maximal.

Worksheet XII - Irreducible and Prime Elements

Definition 30. Let R be a commutative ring and let $a, b \in R$.
We say that a *divides* b, and write $a \mid b$, if there exists $c \in R$ such that $b = ac$. Otherwise we write $a \nmid b$.

Definition 31. Let R be a commutative ring and let $a, b \in R^\bullet$.
We say that a and b are *associates*, and write $a \sim b$, if $a \mid b$ and $b \mid a$.

Problem 97. Let R be a commutative ring and let $a, b \in R^\bullet$.
(a) Show that $a \sim b$ if and only if there exists an invertible element $u \in R$ such that $b = ua$.
(b) Show that $\sim$ is an equivalence relation on $R^\bullet$.

Problem 98. Let R be a commutative ring and let $a, b \in R^\bullet$.
(a) Show that $bR \subset aR$ if and only if $a \mid b$.
(b) Show that $bR = aR$ if and only if $a \sim b$.
(c) Show that $abR \subset aR \cap bR$.

Definition 32. Let R be a commutative ring and let $p \in R^\bullet \setminus R^*$.
We say that p is *irreducible* if whenever $p = ab$, then either a is invertible or b is invertible.
We say that p is *prime* if whenever $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Problem 99. Let R be a commutative ring and let $p, u \in R$, where u is invertible.
(a) Show that if p is irreducible, then so is up.
(b) Show that if p is prime, then so is up.

Problem 100. Let D be an integral domain and let $p \in D$.
Show that p is a prime element if and only if pD is a prime ideal.

Problem 101. Let D be a pid and let $p \in D$.
Show that pD is maximal if and only if p is irreducible.

Problem 102. Let D an integral domain and let $p \in D$.
Show that if p is prime, then p is irreducible.

Problem 103. Let D be a pid and let $p \in D$.
Show that p is prime if and only if p is irreducible.

Worksheet XIII - Common Divisors and Multiples

Definition 33. Let R be a commutative ring and let $a, b \in R^\bullet$.
We say that $d \in R^\bullet$ is a *greatest common divisor* of a and b, and write $d \vDash \gcd(a, b)$, if
(GCD1) $d \mid a$ and $d \mid b$;
(GCD2) $e \mid a$ and $e \mid b \Rightarrow e \mid d$.

Problem 104. Let D be an integral domain and let $a, b, d, e, u \in D$, where u is invertible.
(a) Show that if $d \vDash \gcd(a, b)$, then $ud \vDash \gcd(a, b)$.
(b) Show that if $d \vDash \gcd(a, b)$ and $e \vDash \gcd(a, b)$, then $d \sim e$.

Problem 105. Let D be a pid and let $a, b \in D$. Show that there exists $d \in D$ such that $d \vDash \gcd(a, b)$.

Problem 106. Let D be a pid and let $a, b \in D$. Let $d \vDash \gcd(a, b)$.
Show that there exist $x, y \in D$ such that $d = ax + by$.

Definition 34. Let R be a commutative ring and let $a, b \in R^\bullet$.
We say that $l \in R^\bullet$ is a *least common multiple* of a and b, and write $l \vDash \operatorname{lcm}(a, b)$, if
(LCM1) $a \mid l$ and $b \mid l$;
(LCM2) $a \mid m$ and $b \mid m \Rightarrow l \mid m$.

Problem 107. Let D be an integral domain and let $a, b, l, m, u \in D$, where u is invertible.
(a) Show that if $l \vDash \operatorname{lcm}(a, b)$, then $ul \vDash \operatorname{lcm}(a, b)$.
(b) Show that if $l \vDash \operatorname{lcm}(a, b)$ and $m \vDash \operatorname{lcm}(a, b)$, then $l \sim m$.

Problem 108. Let D be a pid and let $a, b \in D$. Show that there exists $l \in D$ such that $l \vDash \operatorname{lcm}(a, b)$.

Problem 109. Let D be a pid and let $a, b \in D$. Let $d \vDash \gcd(a, b)$ and $l \vDash \operatorname{lcm}(a, b)$.
Show that $ab \sim dl$.

Definition 35. Let R be a commutative ring and let $A \subset R^\bullet$.
We say that $d \in R^\bullet$ is a *greatest common divisor* of A and write $d \vDash \gcd(A)$, if
(GCD1) $d \mid a$ for every $a \in A$;
(GCD2) $e \mid a$ for every $a \in A \Rightarrow e \mid d$.

Remark 17. This is a generalization of our previous definition of gcd, and coexists with it.

Problem 110. Let D be an integral domain. Let $A \subset D$ and $d, e, u \in D$, where u is invertible.
(a) Show that if $d \vDash \gcd(A)$, then $ud \vDash \gcd(A)$.
(b) Show that if $d \vDash \gcd(A)$ and $e \vDash \gcd(A)$, then $d \sim e$.

Problem 111. Let D be a pid and let $A \subset D$. Show that there exists $d \in D$ such that $d \vDash \gcd(A)$.

Problem 112. Let D be a pid and let $A = \{a_1, \ldots, a_n\} \subset D$. Let $d \vDash \gcd(A)$.
Show that there exist $x_i \in D$ such that $d = \sum_{i=1}^{n} x_i a_i$.

Definition 36. Let R be a commutative ring and let $A \subset R^\bullet$.
We say that $l \in R^\bullet$ is a *least common multiple* of a and b, and write $l \vDash \operatorname{lcm}(a, b)$, if
(LCM1) $a \mid l$ and $b \mid l$;
(LCM2) $a \mid m$ and $b \mid m \Rightarrow l \mid m$.

Remark 18. This is a generalization of our previous definition of lcm, and coexists with it.

Problem 113. Let D be an integral domain. Let $A \subset D$ and let $l, m, u \in D$, where u is invertible.
(a) Show that if $l \vDash \operatorname{lcm}(A)$, then $ul \vDash \operatorname{lcm}(A)$.
(b) Show that if $l \vDash \operatorname{lcm}(A)$ and $m \vDash \operatorname{lcm}(A)$, then $l \sim m$.

Problem 114. Let D be a pid and let $A \subset D$. Show that there exists $l \in D$ such that $l \vDash \operatorname{lcm}(A)$.

Worksheet XIV - Noetherian Rings

Definition 37. Let R be a commutative ring.

An *ascending chain of ideals* in R is a collection of ideals $\{I_i \mid i \in \mathbb{N}\}$ such that $i < j \Rightarrow I_i \subset I_j$:

$$I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_i \subset \ldots$$

Problem 115. Let R be a ring and let $\{I_i \mid i \in \mathbb{N}\}$ be an ascending chain of ideals. Show that $\cup_{i=1}^{\infty} I_i \triangleleft R$.

Definition 38. Let R be a commutative ring and let $\{I_i \mid i \in \mathbb{N}\}$ be an ascending chain of ideals.

We say that $\{I_i \mid i \in \mathbb{N}\}$ is *eventually constant* if there exists $n \in \mathbb{N}$ such that $I_i = I_n$ for all $i \geq n$.

We say that R is *noetherian* if every ascending chain of ideals in R is eventually constant.

Problem 116. Let D be a pid. Show that D is noetherian.
(Hint: the union of an ascending chain of ideals in D is also a principal ideal.)

Problem 117. Let D be a pid and let $a \in D$. Show that only finitely many prime ideals in D contain a.
(Hint: suppose not, and construct an ascending chain of ideals in D which is not eventually constant.)

Problem 118. Let D be a pid and let $a, b \in D$. Show that there exists a unique nonnegative integer n such that b^n divides a but b^{n+1} does not.

Problem 119. Let D be a pid and let $a \in D$. Let $p_1, \ldots, p_r$ be generators for the distinct prime ideals which contain a. Show that there exist unique positive integers $n_1, \ldots, n_r$ such that

$$a \sim p_1^{n_1} \ldots p_r^{n_r}.$$

Remark 19. We were after the above result, which we will use later. The following result will not be used in later worksheets, but illuminates the nature of noetherian rings.

Definition 39. Let R be a commutative and and let $I \triangleleft R$.

We say the I is *finitely generated* if there exist $a_1, \ldots, a_n \in R$ such that $I = \langle a_1, \ldots, a_n \rangle$.

Problem 120. Let R be a commutative ring. Show that R is noetherian if and only if every ideal of R is finitely generated.

Worksheet XV - Unique Factorization Domains

Definition 40. Let R be an integral domain.

Let $a \in R$. A *complete factorization* of a is a true expression of the form

$$a = \prod_{i=1}^{r} p_i^{m_i},$$

where $p_i \in R$ are irreducible elements and $m_i \in \mathbb{Z}$ are positive integers. Such an expression is call *essentially unique* if whenever

$$a = \prod_{j=1}^{s} q_j^{n_j}$$

is another complete factorization of a, we have $r = s$ and a permutation $\sigma \in S_r$ such that $q_j \sim p_{\sigma i}$ and $n_j = m_{\sigma i}$.

We say that R is a *unique factorization domain* (ufd) if every nonzero element of R has an essentially unique complete factorization.

Problem 121. Let R be a pid. Show that R is a ufd.

Problem 122. Let R be a ufd and let $a \in R$. Show that a is prime if and only if a is irreducible.

Problem 123. Let R be a ufd and let $a, b \in R$.
(a) Show that there exists $d \in R$ such that $d \vDash \gcd(a, b)$.
(b) Show that there exists $l \in R$ such that $l \vDash \operatorname{lcm}(a, b)$.
(c) Show that $ab \sim dl$.

Problem 124. Let R be a ufd and let $a, b \in R$.
Show that $aR \cap bR = abR \Leftrightarrow 1 \vDash \gcd(a, b)$.

Definition 41. Let R be a commutative ring.

We say that R is *seminoetherian* if every ascending chain of principal ideals is eventually constant.

Problem 125. Let R be a ufd. Show that R is seminoetherian.

Fact 1. Let R be an integral domain. Then following conditions are equivalent:
(1) R is a ufd;
(2) R is seminoetherian and every irreducible element of R is prime;
(3) R is seminoetherian and every pair of nonzero elements in R has a gcd.

Worksheet XVI - Quotient Fields

Definition 42. Let D be an integral domain and let F be a field which contains D.
We say that F is a *quotient field* of D if for every $x \in F$ there exist $a, b \in D$ such that $x = ab^{-1}$.

Example 1. Clearly $\mathbb{Q}$ is a quotient field for $\mathbb{Z}$.

Problem 126. (Relabeling Lemma)
Let R and $\widetilde{S}$ be rings. Let $\phi : R \to \widetilde{S}$ be an injective ring homomorphism. Show that there exists a ring S which contains R and an isomorphism $\psi : \widetilde{S} \to S$ such that $\psi \circ \phi(a) = a$ for every $a \in R$.

Problem 127. (Existence of Quotient Fields)
Let R be a commutative ring.
(a) Show that if $a, b \in R^\bullet$, then $ab \in R^\bullet$. Also note that $1 \in R^\bullet$.
Define a relation $\div$ on $R \times R^\bullet$ by

$$(a, b) \div (c, d) \Leftrightarrow ad = bc.$$

(b) Show that $\div$ is an equivalence relation.
Denote the equivalence class of (a, b) by $[a, b]$, so that $(a, b) \div (c, d) \Leftrightarrow [a, b] = [c, d]$. Set

$$\widetilde{S} = \{[a, b] \mid a \in R \text{ and } b \in R^\bullet\}.$$

Define addition and multiplication on $\widetilde{S}$ by

$$[a, b] + [c, d] = [ad + bc, bd] \quad \text{and} \quad [a, b] \cdot [c, d] = [ac, bd].$$

(c) Show that these operations of addition and multiplication on $\widetilde{S}$ are well defined.
(d) Verify that $\widetilde{S}$ is a commutative ring.
(e) Show that the function $\phi : R \to \widetilde{S}$ given by $\phi(a) = [a, 1]$ is an injective homomorphism.
(f) Show that there exists a ring S isomorphic to $\widetilde{S}$ such that S contains R and every entire element of R is invertible in S.
(g) Show that if R is an integral domain, then S is a quotient field for R.

Problem 128. (Universal Property of Quotient Fields)
Let D be an integral domain and let F be a quotient field of D. Let E be a field containing D. Show that there exists a unique injective homomorphism $\phi : F \to E$ such that $\phi(a) = a$ for every $a \in D$.

Problem 129. Let D be an integral domain and let F be a field containing D. Suppose that for every field E containing D there exists a unique homomorphism $\phi : F \to E$ such that $\phi(a) = a$ for every $a \in D$. Show that F is a quotient field for D.

Problem 130. Let D be an integral domain and let E be a field containing D. Set

$$\mathrm{qf}_E(D) = \{x \in E \mid x = ab^{-1} \text{ for some } a, b \in D\}.$$

(a) Show that $\mathrm{qf}_E(D)$ is a field.
(b) Show that $\mathrm{qf}_E(D)$ is a quotient field for D.
(c) Show that $\mathrm{qf}_E(D) = \mathrm{gf}_E(D)$.
We call $\mathrm{qf}_E(D)$ the *quotient field of D in E*.

Problem 131. Let E be a field and let D be a subring of E. Let $F = \mathrm{qf}_E(D)$.
Let $\psi : E \to E$ be an automorphism of E such that $\psi \restriction_D = \mathrm{id}_D$. Show that $\psi \restriction_F = \mathrm{id}_F$.

Problem 132. Let D be a pid and let F be a quotient field for D. Let $x \in F$.
Show that there exist $a, b \in D$ with $1 \vDash \gcd(a, b)$ such that $ab^{-1} = x$.

Worksheet XVII - Polynomials

Definition 43. Let R be a commutative ring. A *polynomial* (in one indeterminant) over R is a sequence $f : \mathbb{N} \to R$ such that $f(n) = 0$ for all but finitely many $n \in \mathbb{N}$.

Let $R[X]$ be the set of all polynomials over R, where X is the sequence $(0, 1, 0, 0, 0, \dots)$.

Define addition and multiplication on $R[X]$ by

$$(a_i)_i + (b_i)_i = (a_i + b_i)_i;$$
$$(a_i)_i \cdot (b_i)_i = (\sum_{j+k=i} a_j b_k)_i.$$

Fact 2. Every element of $R[X]$ is of the form $f = \sum_{i=0}^{n} a_i X^i$, where $n \in \mathbb{N}$ and $a_i \in R$ for $i = 1, \dots, n$.

Moreover, $R[X]$ is a commutative ring, and R embeds in $R[X]$ via $a \mapsto (a, 0, 0, 0, \dots)$; we consider R to be a subring of $R[X]$.

Definition 44. Let R be a commutative ring and let $f = (a_i) \in R[X]$. Then *degree* of f is denoted $\deg(f)$ and is defined by $\deg(f) = \max\{n \in \mathbb{N} \mid a_i \neq 0\}$. If $f = 0$, we set $\deg(f) = -\infty$.

We call the a_i the *coefficients* of f; a_0 is called the *constant coefficient* and a_n is called the *leading coefficient*.

Problem 133. Let R be a commutative ring and let $f, g \in R[X]$.
(a) Show that $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$;
(b) Show that $\deg(fg) \leq \deg(f) + \deg(g)$;
(c) Show that if R is an integral domain, then $\deg(fg) = \deg(f) + \deg(g)$.

Problem 134. Let D be an integral domain. Show that $D[X]$ is an integral domain.

Problem 135. Let F be a field and let $f \in F[X]$. Show that f is invertible if and only if $f \in F \setminus \{0\}$.

Definition 45. Let R be a subring of a commutative ring S. Let $f \in R[X]$; then $f = \sum_{i=0}^{n} a_i X^i$. Let $s \in S$ and set $f(s) = \sum_{i=0}^{n} a_i s^i \in S$. We call $f(s)$ f *evaluated at* s. In particular, note that $R \leq R[X]$, and $f(X) = f$ in this context. If $f(s) = 0_S$, we say that s is a *zero*, or *root*, of f.

Problem 136. (Universal Property of Polynomial Rings)
Let R be a subring of a commutative ring S. Let $s \in S$ and define a function

$$\psi_s : R[X] \to S \text{ by } \psi_s(f) = f(s).$$

Show that ψ_s is a homomorphism, called the *evaluation homomorphism*.

Problem 137. (Division Algorithm for Polynomials)
Let R be a commutative ring and let $f, g \in R[X]$ such that the leading coefficient of g is invertible. Show that there exist unique polynomials $q, r \in R[X]$ with $\deg(r) < \deg(f)$ such that $f = gq + r$.
(Hint: consider the set $\{f - gq \mid q \in R[X]\} \subset R[X]$; this set contains a polynomial of minimal degree.)

Problem 138. Let R be a commutative ring. Let $f \in R[X]$ and let $a \in R$.
Show that $f(a) = 0$ if and only if $(X - a) \mid f(X)$.

Problem 139. Let R be an integral domain and let $f \in R[X]$ of degree n.
Show that f has at most n roots in R.

Worksheet XVIII - Polynomial Factorization

Remark 20. Let R be a ring contained in a commutative ring S. Let $f \in R[X]$. Since the coefficients of f lie in $R \subset S$, we may naturally view $f \in S[X]$. The primeness or irreducibility of f depends on whether we view it as an element of $R[X]$ or as an element of $S[X]$.

Problem 140. Find a ring R contained in a commutative ring S and a polynomial $f \in R[X]$ such that f is irreducible in $R[X]$ but not in $S[X]$.

Problem 141. Let F be a field and let $f \in F[X]$.
(a) Show that if $f(x)$ is irreducible, then $p(x)$ has no root in F.
(b) Show that if $\deg(f) \in \{2, 3\}$, then f is irreducible if and only if f has no roots in F.

Problem 142. (Rational Roots Theorem)
Let D be an integral domain and let F be a quotient field for D. Let $f(X) = \sum_{i=0}^{n} c_i X^i \in D[X]$ and let $z \in F$ such that $f(z) = 0$. Then there exist $a, b \in D$ with $\gcd(a, b) = 1$ such that $z = ab^{-1} \in D$.
Show that if $f(z) = 0$, then $a \mid c_0$ and $b \mid c_n$.

Problem 143. Let R be a commutative ring and let $I \triangleleft R$. Set

$$I[X] = \{f(X) = \sum_{i=0}^{n} c_i X^i \in R[X] \mid c_i \in I \text{ for } i = 0, \ldots, n\}.$$

For $a \in R$, set $\overline{a} = a + I$, and for $f = \sum_{i=0}^{n} c_i X^i \in R[X]$, set $\overline{f} = \sum_{i=0}^{n} \overline{c_i} X^i$.
Define $\phi : R[X] \to \frac{R}{I}[X]$ by $\phi(f) = \overline{f}$.
(a) Show that ϕ is a ring homomorphism.
(b) Show that $I[X] \triangleleft R[X]$.
(c) Show that $\frac{R[X]}{I[X]} \cong \frac{R}{I}[X]$.

Definition 46. Let R be a commutative ring and let $f \in R[X]$.
A *proper factorization* of f is a factorization $f = gh$, where $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$.

Problem 144. Find a ring R and a polynomial f such that f is not irreducible but has no proper factorization.

Problem 145. (Gauss's Lemma)
Let D be a pid and let $f, g, h \in D[X]$ such that $f = gh$. Let $p \in D$ be a prime element. Show that if p divides every coefficient of f, then either p divides every coefficient of g or p divides every coefficient of h.
(Hint: consider the ideal $I = \langle p \rangle$.)

Problem 146. Let D be a pid and let F be a quotient field of D. Let $f \in D[X]$.
Show that if f is irreducible in $F[X]$ if and only if f has no proper factorization in $D[X]$.
(Hint: clear denominators, then cancel prime factors.)

Worksheet XVIX - Polynomial Irreducibility Criteria

Problem 147. (Modular Irreducibility Test)
Let D be a pid and let F be a quotient field for D. Let $f = \sum_{i=0}^{n} a_i X^i \in D[X]$ and let $p \in D$ be a prime element of D. Let $\overline{D} = D/\langle p \rangle$ and let $\overline{f}$ be the reduction of f modulo $\langle p \rangle$. Suppose:
(1) p does not divide a_n;
(2) $\overline{f}$ is irreducible in $\overline{D}[X]$.
Show that f is irreducible in $F[X]$.
(Hint: suppose f reduces in $F[X]$, and show that $\overline{f}$ reduces in $\overline{D}[X]$.)

Problem 148. (Eisenstein's Criterion)
Let D be a pid and let F be a quotient field for D. Let $f = \sum_{i=0}^{n} a_i X^i \in D[X]$ and let $p \in D$ be a prime element of D. Suppose:
(1) p divides a_i for $i = 0, \ldots, n-1$;
(2) p does not divide a_n;
(3) p^2 does not divide a_0.
Show that f is irreducible in $F[X]$.
(Hint: suppose that f reduces in $F[X]$; then f reduces in $D[X]$. Write $f = gh$ where $g, h \in D[X]$, and compare the coefficients of the product to the coefficients of f.)

Problem 149. Let $p \in \mathbb{Z}$ be a prime integer and set

$$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}.$$

Show that $\Phi_p(X)$ is irreducible.
(Hint: first note that $\Phi_p(X)$ is irreducible if and only if $\Phi_p(X+1)$ is irreducible.)

Fact 3. Let $f \in \mathbb{C}[X]$ with $\deg(f) > 0$. Then there exists $z \in \mathbb{C}$ such that $f(z) = 0$.

Fact 4. Let $f \in \mathbb{C}[X]$ be irreducible. Then $\deg(f) = 1$.

Fact 5. Let $f \in \mathbb{R}[X]$ be irreducible. Then either $\deg(f) = 1$ or $\deg(f) = 2$.

Worksheet XX - Minimum Polynomials

Definition 47. Let R be a subring of a commutative ring S and let $s \in S$.
Set $R[s] = \mathrm{gr}_S(R \cup \{s\})$; this is called the ring R *extended* by s.

Problem 150. Let R be a subring of a commutative ring S.
Let $s \in S$ and let $\psi_s : R[X] \to S$ be evaluation at s. Show that $\psi_s(R[X]) = R[s]$.

Problem 151. Let F be a field. Show that $F[X]$ is a pid.
(Hint: use the division algorithm.)

Remark 21. Let F be a field; we list the facts about principal ideals and pids which we have collected and are significant for $F[X]$:

- If $\langle f \rangle = \langle g \rangle$, then $f = ug$ for some invertible element $u \in F[X]$. Since the invertible elements of $F[X]$ are the nonzero constants, we have $u \in F \smallsetminus \{0\}$.
- If $I \lhd F$ is a nonzero prime, then I is maximal;
- Every quotient of $F[X]$ by a nontrivial proper ideal is either a field or a nondomain;
- If $f \in F[X]$, then f is prime if and only if f is irreducible;
- If $f, g \in F[X]$, then there exists $d \in F[X]$ such that $d \vDash \gcd(f, g)$, and $d = af + bg$ for some $a, b \in F[X]$.

Definition 48. Let R be a commutative ring and let $f \in R[X]$ be a nonconstant polynomial.
We say that f is *monic* if the leading coefficient of f is 1.

Problem 152. Let D be an integral domain and let $f \in D[X]$ be monic. Show that there exist unique monic irreducible polynomials $g_1, \ldots, g_r \in D[X]$ such that $f = \prod_{i=1}^{r} g_i$.

Problem 153. Let F be a field and let $I \lhd F[X]$.
Show that there exists a unique monic polynomial $f \in F[X]$ such that $I = \langle f \rangle$.

Problem 154. Let F be a field and let $f, g \in F[X]$.
Show that there exists a unique monic polynomial $d \in F[X]$ such that $d \vDash \gcd(f, g)$.

Definition 49. Let F be a subfield of a field E and let $\alpha \in E$.
The unique monic polynomial which generates the kernel of ψ_α is called the *minimum polynomial* of α.

Problem 155. Let F be a subfield of a field E and let $\alpha \in E$.
Let $f \in F[X]$ be the minimum polynomial of α.
(a) Show that $F[X]/\langle f \rangle \cong F[\alpha]$.
(b) Show that $\langle f \rangle$ is a prime ideal.
(c) Show that f is either zero or is irreducible in $F[X]$.

Definition 50. Let F be a subfield of a field E and let $\alpha \in E$.
We say that α is *algebraic* over F if there exists a nonzero polynomial $f \in F[X]$ such that $f(\alpha) = 0$. Otherwise we say that α is *transcendental* over F.

Problem 156. Let F be a subfield of a field E and let $\alpha \in E \smallsetminus F$.
Let $\psi_\alpha : F[X] \to E$ be the evaluation map.
(a) Show that α is algebraic if and only if the minimum polynomial of α generates a maximal ideal.
(b) Show that if α is algebraic if and only if $F[\alpha]$ is a field.
(c) Show that α is transcendental if and only if the evaluation map ψ_α is injective.
(d) Show that if α is transcendental if and only if $F[\alpha] \cong \mathbb{F}[X]$.

Worksheet XXI - Splitting Fields

Definition 51. Let R be a commutative ring contained in a ring S and let $s_1, \ldots, s_n \in S$. Set $R[s_1, \ldots, s_n] = \mathrm{gi}_S(R \cup \{s_1, \ldots, s_n\})$; this is the ring R *extended* by $s_1, \ldots, s_n$. If $S = R[s_1, \ldots, s_n]$, we say that $s_1, \ldots, s_n$ *generated* S over R.

Definition 52. Let F be a field contained is a field E and let $f \in F[X]$.

We say that f *splits* in E if f is the product of linear factors in E:

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i), \qquad \text{where } \alpha_i \in E \text{ for } i = 1, \ldots, n.$$

We say that E is a *splitting field* for f over F if there exist $\alpha_1, \ldots, \alpha_n \in E$ such that
(SF1) $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$;
(SF2) $E = F[\alpha_1, \ldots, \alpha_n]$.

Problem 157. Let F be a field and let $f \in F[X]$ be an irreducible polynomial.
Let $\widetilde{E} = F[X]/\langle f \rangle$; we have seen that $\widetilde{E}$ is a field.
(a) Show that there exists an injective homomorphism $\phi : F \to \widetilde{E}$.
(b) Show that there exists a field E which is isomorphic to $\widetilde{E}$ and contains F.
(c) Show that there exists $\alpha \in E$ such that $f(\alpha) = 0$.
(d) Show that $E = F[\alpha]$.

Problem 158. Let F be a field and let $f \in F[X]$ be an irreducible polynomial.
Show that there exists a field E which is a splitting field for f over F.

Problem 159. Let F be a field and let $f \in F[X]$ be a nonconstant polynomial.
Show that there exists a field E which is a splitting field for f over F.

Problem 160. Let F be a field and let $f \in F[X]$ be a a nonconstant polynomial.
Let E be a field in which f splits. Show that E contains a splitting field for f over F.

Multiple Roots

Definition 53. Let F be a field and let $f \in F[X]$. We define the *derivative* of $f(X) = \sum_{i=0}^{n} a_i X^i$ to be

$$f'(X) = \sum_{i=0}^{n} i a_i X^{i-1}.$$

Problem 161. Let F be a field and let $f, g \in F[X]$.
(a) Show that $(f + g)' = f' + g'$.
(b) Show that $(fg)' = fg' + f'g$.

Problem 162. Let F be a field and let $f \in F[X]$.
(a) Show that $\deg(f') \leq \deg(f) - 1$.
(b) Show that if F has characteristic zero, then $\deg(f') = \deg(f) - 1$.
(c) Show that if F has characteristic $p > 0$, there exists a polynomial $f \in F[X]$ such that $\deg(f') < \deg(f) - 1$.

Definition 54. Let F be a field and let $f \in F[X]$. Let E be a field containing F in which f splits.

We say that $a \in E$ is a *multiple root* of f if $(X - a)^n \mid f(X)$ in $E[X]$ for some $n \in \mathbb{N}$, $n \geq 2$. The maximum such n is called the *order* of the root.

Problem 163. Let F be a field and let $a \in F$.
Show that $(X - a)^2 \mid f \Leftrightarrow (X - a) \mid f$ and $(X - a) \mid f'$.

Worksheet XXII - Finite Fields

Definition 55. Let G be a finite group.
The *exponent* of G, denoted $\exp(G)$, is defined as

$$\exp(G) = \min\{n \in \mathbb{N} \mid g^n = 1 \text{ for all } g \in G\}.$$

Fact 6. Let G be a finite group and let $n = |G|$. Then $g^n = 1$ for every $g \in G$.

Fact 7. Let G be a finite group. Then $\exp(G) \leq |G|$.

Fact 8. Let G be a finite abelian group. If $\exp(G) = |G|$, then G is cyclic.

Problem 164. Let F be a field and let G be a finite subgroup of F^*.
(a) Note that $f(X) = X^{\exp(G)} - 1$ has at most $\exp(G)$ roots in F.
(b) Note that every element of G is a root of $f(X)$.
(c) Conclude that F^* is cyclic.

Problem 165. Let G be a finite abelian group and let p be a prime integer. Suppose that $g^p = 1$ for every $g \in G$. Show that $|G| = p^k$ for some $k \in \mathbb{N}$.

Problem 166. Let F be a finite field. Show that there exists a prime integer p and a positive integer n such that $|F| = p^k$.

Problem 167. Let F be a field of cardinality p, where p is a prime integer.
Show that $F \cong \mathbb{Z}_p$. Denote this field by $\mathbb{F}_p$.

Problem 168. Let $k, p \in \mathbb{Z}$ with $k \geq 2$ and p prime.
(a) Let x be the number of monic polynomials of degree k in $\mathbb{F}_p$. Find x.
(b) Let y be the number of monic polynomials of degree less than k in $\mathbb{F}_p$. Find y.
(c) Show that $x - y = p + (p-2)y$.
(d) Conclude that there exists an irreducible polynomial of degree k over $\mathbb{F}_p$.
(e) Let $f \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree k. Show that $\mathbb{F}_p[X]/\langle f \rangle$ is a field of cardinality p^k.

Problem 169. Let R be an integral domain with finite subfields E and F of the same cardinality.
Show that $E = F$.
(Hint: Let $n = |E| = |F|$ and let $f(X) = X^n - X \in R[X]$. How many roots does f have in R? How many roots does f have in E and in F?)

Fact 9. If E and F be finite fields such that $|E| = |F|$, then $E \cong F$.

Problem 170. Let F be a finite field and let $p = \text{char}(F)$.
Define $\phi : R \to R$ by $\phi(a) = a^p$. Show that ϕ is an automorphism.

Worksheet XXIII - Vector Spaces

Definition 56. A *vector space* over a field F is a set V together with operations

$$+ : V \times V \to V \quad \text{and} \quad \cdot\, F \times V \to V,$$

respectively called addition and scalar multiplication, satisfying:
(V1) $x + y = y + x$ for all $x, y \in V$;
(V2) $x + (y + z) = (x + y) + z$ for all $x, y, z \in V$;
(V3) there exists $0_V \in V$ such that $x + 0_V = x$ for every $x \in V$;
(V4) for every $x \in V$ there exists $-x \in V$ such that $x + (-x) = 0_V$;
(V5) $1_F \cdot x = x$ for every $x \in V$;
(V6) $(ab)x = a(bx)$ for every $a, b \in F$ and $x \in V$;
(V7) $(a + b)x = ax + bx$ for every $a, b \in F$ and $x \in V$;
(V8) $a(x + y) = ax + ay$ for every $a \in F$ and $x, y \in V$.

Remark 22. Properties **(V1)** through **(V4)** say that $(V, +)$ is an additive abelian group. Let $\mathrm{End}(V)$ denote the collection of additive group homomophisms of V.

Problem 171. Let V be a vector space over a field F. Let $a \in F$ and $x \in V$.
(a) Show that $0_F \cdot x = 0_V$.
(b) Show that $a \cdot 0_V = 0_V$.
(c) Show that $(-1_F) \cdot x = -x$.

Problem 172. Let V be a vector space over a field F. Define a function $\phi : F \to \mathrm{End}(V)$ by $\phi_a(v) = av$, where ϕ_a means $\phi(a)$ for each $a \in F$. Show that ϕ is a ring homomorphism.

Problem 173. Let A be an additive abelian group and let F be a field. Let $\phi : F \to \mathrm{End}(A)$ be a ring homomorphism. Define scalar multiplication $\cdot : F \times A \to A$ by $a \cdot x = \phi_a(x)$. Show that A together with this scalar multiplication is a vector space.

Definition 57. Let V be a vector space over a field F.
A *subspace* of V is a subset $W \subset V$ such that
(W1) $x, y \in W \Rightarrow x + y \in W$;
(W2) $a \in F, x \in W \Rightarrow ax \in W$.
If W is a subspace of V, this is denoted by $W \leq V$.

Problem 174. Let V be a vector space over a field F and let $W \leq V$. Show that the restriction of $+$ and $\cdot$ to W induces a vector space structure on W.

Problem 175. Let V be a vector space over a field F and let $\mathcal{W}$ be a collection of subspaces of V. Show that $\cap\mathcal{W} \leq V$.

Definition 58. Let V be a vector space over a field F and let $X \subset V$. The subspace *generated* by x is denoted by $\mathrm{gv}_V(X)$ and is defined to be the intersection of all subspaces of V which contain X. This subspace is called the *span* of X.

Problem 176. Let V be a vector space over a field F and let $X = \{v_1, \ldots, v_n\}$. Show that

$$\mathrm{gv}_V(X) = \{\sum_{i=1}^{n} a_i v_i \mid a_i \in F\}.$$

Worksheet XXIV - Dimension

Definition 59. Let V be a vector space over a field F. Let $B \subset V$.

We say that B *spans* V is for every $x \in V$ there exist $a_1, \ldots, a_n \in F$ and $v_1, \ldots, v_n \in B$ such that $x = \sum_{i=1}^{n} a_i v_i$.

We say that B is *linearly independent* if whenever $v_1, \ldots, v_n \in B$ are distinct elements of B and $a_1, \ldots, a_n \in F$,

$$\sum_{i=1}^{n} a_i v_i = 0 \Rightarrow a_i = 0 \text{ for } i = 1, \ldots, n.$$

We say that B is a *basis* for V if B spans V and is linearly independent.

Problem 177. Let V be a vector space over a field F and let $X \subset V$ span V. Show that $V = \mathrm{gv}_V(X)$.

Problem 178. Let V be a vector space over a field F and let $X \subset V$ be linearly independent. Let $v \in X$. Show that $\mathrm{gv}_V(X \smallsetminus \{v\})$ is a proper subset of $\mathrm{gv}_V(X)$.

Problem 179. Let V be a vector space over a field F and let $X \subset V$ span V. Show that there exists a subset $B \subset X$ such that B is a basis for V.

Problem 180. Let V be a vector space over a field F and let $X \subset V$ be linearly independent. Show that there exists a subset $Y \subset V$ such that $X \cup Y$ is a basis for V.

Problem 181. Let V be a vector space over a field F. Let $A = \{v_1, \ldots, v_m\}$ and $B = \{w_1, \ldots, w_n\}$ be bases for V. Show that $m = n$.

Definition 60. Let V be a vector space over a field F. If V has a basis containing n elements, where $n \in \mathbb{N}$, we say that V is *finite dimensional*, and that n is the *dimension* of V; this is denoted by $\dim(V) = n$.

Problem 182. Let V be a vector space over a field F and let $U, W \leq V$. Set $U+W = \{u+w \mid u \in U, w \in W\}$.
(a) Show that $U + W \leq V$.
(b) Show that $\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$.

Problem 183. Let F be a field and let n be a positive integer. Let F^n denote the cartesian product of F with itself n times. Show that F^n is a vector space over F of dimension n.

Definition 61. Let V and W be a vector spaces over a field F.

A *linear transformation* from V to W is a function $f : V \to W$ such that
(L1) $f(x + y) = f(x) + f(y)$ for every $x, y \in V$;
(L2) $f(ax) = af(x)$ for every $a \in F$ and $x \in V$.

Definition 62. Let V and W be a vector spaces over a field F. Let $f : V \to W$ be a linear transformation.

The *kernel* of f is $\ker(f) = \{x \in V \mid f(x) = 0_W\}$.

Problem 184. Let V and W be a vector spaces over a field F. Let $f : V \to W$ be a linear transformation. Show that f is injective if and only if $\ker(f) = \{0_V\}$.

Problem 185. Let V and W be finite dimensional vector spaces over a field F. Let $f : V \to W$ be a linear transformation.
(a) Show that $f(V) \leq W$.
(b) Show that $\dim(V) = \dim(\ker(f)) + \dim(f(V))$.

Problem 186. Let V be a vector space over a field F. Let $\mathrm{End}_F(V)$ denote the set of all linear transformations from V into itself. Show that $\mathrm{End}_F(V)$ is a subring of $\mathrm{End}(V)$.

Problem 187. Let F be a field and let $\mathcal{M}_n(F)$ denote the set of $n \times n$ matrices over F.
Verify that $\mathcal{M}_n(F)$ is a ring under the standard definitions of matrix addition and matrix multiplication.

Problem 188. Let V be a vector space over a field F of dimension n.
Show that $\mathrm{End}_F(V) \cong \mathcal{M}_n(F)$ as rings.

Worksheet XXV - Field Extensions

Definition 63. A *field extension* E/F is a field F which is a subfield of a field E.

Problem 189. Let E/F be a field extension. Show that E is a vector space over F via ring addition and multiplication.

Definition 64. Let E/F be a field extension.

We say that E/F is *finite* if E is a finite dimensional vector space over F. The *degree* of E/F is the dimension of E as a vector space over F; this dimension is denoted by $[E : F]$.

Problem 190. Let E/F be a field extension. Show that $[E : F] = 1 \Leftrightarrow E = F$.

Problem 191. Let F be a subfield of a field E and let $\alpha \in E$ be algebraic over F. Let f be the minimum polynomial of α over F and set $n = \deg(f) > 0$.
(a) Show that $F[\alpha] = \{\sum_{i=0}^{n-1} b_i \alpha^i \mid b_i \in F\}$.
(b) Show that $\sum_{i=0}^{n-1} b_i \alpha^i = \sum_{I=1}^{n-1} c_i \alpha^i$ if and only if $b_i = c_i$ for $i = 1, \ldots, n-1$.
(c) Show that $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $F[\alpha]$ as a vector space over F.
(d) Conclude that $[F[\alpha] : F] = \deg(f)$.

Problem 192. Let E/F and K/E be finite field extensions. Show that

$$[K : F] = [K : E][E : F].$$

(Hint: let $\{v_i\} \subset E$ be a basis for E/F and let $\{w_j\} \subset K$ be a basis for K/E. Consider $\{v_i w_j\}$.)

Problem 193. Let F be a field and let $f \in F[X]$ be an irreducible polynomial of degree n. Let E be a splitting field if f over F. Show that $[E : F]$ divides $n!$.

Worksheet Exercises

Isomorphism Theorem

Problem 194. Let $C = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is continuous }\}$; note that C is a ring under pointwise addition and multiplication. Let $I = \{f \in C \mid f(0) = 0\}$. Show that I is a maximal ideal of C and that $C/I \cong \mathbb{R}$.

Problem 195. Let R be a commutative ring. For $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$, define

$$\sigma(f) = \sum_{i=0}^{n} a_i; \qquad I = \{f(X) \in R[X] : \sigma(f) = 0\}.$$

Show that I is an ideal of $R[X]$ and that $R[X]/I \cong R$.

Problem 196. Let D be a pid and let $a \in D$ be a prime element. Define a function

$$\gamma : D[X] \to D \quad \text{by} \quad \gamma(a_0 + a_1X + \cdots + a_nX^n) = a_0.$$

Set

$$I = \{f(X) \in D[X] : a \mid \gamma(f)\}.$$

Show that I is a maximal ideal of $D[X]$ and that $D[X]/I \cong D/aD$.

Problem 197. Let R be a commutative ring. Show that

$$\frac{R[X]}{\langle X^2 \rangle} \cong \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \Big| a, b \in R \right\}.$$

Problem 198. Let R be a commutative ring and let $M_1, M_2 \triangleleft R$ be distinct maximal ideals. Let $I = M_1 \cap M_2$. Show that I is an ideal of R and that R/I is not a domain.

Problem 199. Let $\phi : R \to S$ be a ring homomorphism. Let $J = \ker(\phi)$ and let $I \triangleleft R$ such that $I \subset J$. Show that there exist homomorphisms $\alpha : R \to R/I$ and $\beta : R/I \to S$ such that $\phi = \beta \circ \alpha$.

Direct Product

Problem 200. Let R and S be rings and let $A \subset R \times S$. Set

$$T = \{r \in R \mid (r, s) \in A \text{ for some } s \in S\} \quad \text{and} \quad U = \{s \in S \mid (r, s) \in A \text{ for some } r \in R\}.$$

Show that $A \leq R \times S$ if and only if $T \leq R$, $U \leq S$, and $A = T \times U$.

Problem 201. Let R and S be commutative rings. Set

$$T = \{(r, s) \in R \times S \mid s = 0\} \quad \text{and} \quad U = \{(r, s) \in R \times S \mid r = 0\}.$$

Define $p_1 : R \times S \to R$ by $p_1(r, s) = r$ and $p_2 : R \times S \to S$ by $p_2(r, s) = s$.
(a) Show that $T \triangleleft R \times S$ and $U \triangleleft R \times S$.
(b) Show that p_1 and p_2 are ring homomorphisms with $\ker(p_1) = U$ and $\ker(p_2) = T$.
(c) Show that $R \times S/T \cong S$ and $R \times S/U \cong R$.

Problem 202. Let R and S be commutative rings. Let $m = \text{char}(R)$ and $n = \text{char}(S)$.
Find $\text{char}(R \times S)$ in terms of m and n.

Polynomials

Problem 203. Let R be a commutative ring in which every nonzero element is a root of $f(X) = X^2 - 1 = 0$. Show that R is commutative.

Problem 204. Let F be a finite field of cardinality 1331.
Show that the polynomial $f(X) = X^2 + X + 1$ is irreducible over F.
(Hint: Note that $X^3 - 1 = (X - 1)(X^2 + X + 1)$ and that F^* is a group under multiplication; what are the possible orders of its elements?)

Problem 205. Let F be a finite field of cardinality 343.
Show that the polynomial $f(X) = X^5 + X^4 + X^3 + X^2 + X + 1$ splits in $F[X]$.

Problem 206. Find all square roots of -1 in $\mathbb{Z}_{101}$.

Problem 207. Let F be a finite field of cardinality 243.
Show that $\sqrt{-1}$ does not exist in F.

Problem 208. Let F be a finite field of cardinality q, and suppose that $q \equiv 3 \mod 4$.
Show that the polynomial $f(X) = X^2 + 1$ is irreducible over F.

Problem 209. Show that $\mathbb{Z}_{51}[X]/\langle X^2 - 15X - 1\rangle$ is not a field.

Problem 210. Let $R = \mathbb{Z}_3[X]$ be the ring of polynomials over $\mathbb{Z}_3$.
Find an ideal $A \triangleleft R$ such that R/A is a nondomain with six elements.

Problem 211. Find three nonisomorphic rings of cardinality four.

Problem 212. Classify each commutative ring as one of the following:

- **(F)** a field;
- **(P)** a pid which is not a field;
- **(D)** a domain which is not a pid;
- **(R)** a ring which is not a domain.

Justify your answer in each case.

- **(a)** $\mathbb{Z}[X]/I$, where $I = \langle X - 16\rangle$;
- **(b)** $\mathbb{Z}[X]/I$, where $I = \langle X^5 - 32\rangle$;
- **(c)** $\mathbb{Z}[X]/I$, where $I = \langle 17\rangle$;
- **(d)** $\mathbb{Z}[\alpha]$, where $\alpha = \frac{43}{12} \in \mathbb{Q}$;
- **(e)** $\mathbb{Q}[X]/I$, where $I = \langle X - 16\rangle$;
- **(f)** $\mathbb{Q}[X]/I$, where $I = \langle X^3 + 15X^2 + 8X + 40\rangle$;
- **(g)** $\mathbb{Q}[X]/I$, where $I = \langle X^4 + 2X^2 + 1\rangle$;
- **(h)** $\mathbb{Q}[X]/I$, where $I = \langle X^5 + 6X^4 + 10X^3 + 8X + 18\rangle$;
- **(i)** $\mathbb{Q}[\alpha]$, where $\alpha = \sqrt[3]{\sqrt{2} + 5\sqrt{6}} \in \mathbb{R}$;
- **(j)** $\mathbb{R}[X]/I$, where $I = \langle 7X^2 - 9X + 3\rangle$;
- **(k)** $\mathbb{R}[\alpha]$, where $\alpha \in \mathbb{C}$;
- **(l)** $\mathbb{C}[\alpha]$, where $E/\mathbb{C}$ is a field extension and $\alpha \in E \smallsetminus \mathbb{C}$.

Idempotents

Definition 65. Let R be a ring and let $a \in R$.
We say that a is *idempotent* if $a^2 = a$.

Problem 213. Let R be a commutative ring and let $a \in R$ be idempotent.
(a) Show that $1 - a$ is idempotent.
(b) Show that aR is a commutative ring with identity element a.
(c) Show that $R \cong aR \times (1 - a)R$ as rings.

Problem 214. Let F be a field. Find a subring of $F \times F$ which is isomorphic to $F[X]/\langle X^2 - X \rangle$.

Definition 66. Let R be a ring.
We say that R is *Boolean* if every element in R is idempotent.

Problem 215. Let R be a Boolean ring.
(a) Show that $\text{char}(R) = 2$.
(b) Show that R is commutative.

Nilpotents

Definition 67. Let R be a ring and let $a \in R$.
We say that a is *nilpotent* if there exists $n \in \mathbb{N}$ such that $a^n = 0$.
We say that R is *nilpotent free* if the only nilpotent elements of R is 0.

Problem 216. Let R be a commutative ring and set

$$I = \{a \in R \mid a \text{ is nilpotent}\}.$$

(a) Show that $I \lhd R$.
(b) Show that R/I is nilpotent free.

Definition 68. Let R be a commutative ring and let $I \lhd R$.
We say that I is *radical* if $a^n \in I \Rightarrow a \in I$, where $a \in R$ and $n \in \mathbb{N}$.
The radical of I is defined by

$$\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N}\}.$$

Problem 217. Let R be a commutative ring and let $I \lhd R$.
(a) Show that $\sqrt{I} \lhd R$.
(b) Show that $\sqrt{I} = \sqrt{\sqrt{I}}$.
(c) Show that I is a radical ideal if and only if $I = \sqrt{I}$.

Problem 218. Let R be a commutative ring and let $I \lhd R$.
Show that I is radical if and only if R/I is nilpotent free.

Problem 219. Let R be a commutative ring and let I be the intersection of all the prime ideals of R.
(a) Show that $I \lhd R$.
(b) Show that R/I is nilpotent-free.
(c) Conclude that I is a radical ideal.

Algebraic Closure

Definition 69. A field K is called *algebraically closed* if every polynomial in $K[X]$ has a root in K.

Definition 70. Let K be an algebraically closed field and let $f \in K[X]$ be an irreducible polynomial. Show that $\deg(f) = 1$.

Problem 220. Let K be an algebraically closed field.
Show that there exists a bijective correspondence between the maximal ideals of $K[X]$ and the points of K.

Problem 221. Let K be an algebraically closed field. Let E/K be a field extension and let $\alpha \in E \setminus K$.
Show that α is transcendental over K.

Fact 10. The field $\mathbb{C}$ is algebraically closed.

Problem 222. Find all ideals in the ring $\mathbb{C}[X]/\langle X^2 \rangle$ and determine if they are principal, prime, and/or maximal.

Problem 223. Find all ideals in the ring $\mathbb{C}[X, Y]/\langle X^2 \rangle$ and determine if they are principal, prime, and/or maximal.

Ring of Functions

Problem 224. Let X be a nonempty set and let F be a field. Let $A = \{f : X \to F\}$. Then A is a ring under pointwise addition and multiplication.
For $Y \subset X$, set

$$A(Y) = \{f : Y \to F\}.$$

For $Y \subset X$, set

$$E(Y) = \{f \in A \mid f(y) = 0 \text{ for all } y \in Y\}.$$

For $I \lhd A$, set

$$V(I) = \{x \in A \mid f(y) = 0 \text{ for all } f \in I\}.$$

Let $\mathcal{I}$ be the collection of ideals of A and let $\mathcal{P}$ be the collection of subsets of X.
Let $Y, Z \subset X$ and $I, J \lhd A$.
(a) Show that $E(Y) \lhd A$.
(b) Show that $Y \subset Z \Leftrightarrow E(Y) \supset E(Z)$.
(c) Show that $I \subset J \Leftrightarrow V(I) \supset V(J)$.
(d) Show that $V(I + J) = V(I) \cap V(J)$.
(e) Show that $V(I \cap J) = V(I) \cup V(J)$.
(f) Show that $E(Y \cup Z) = E(Y) \cap E(Z)$.
(g) Show that $E(Y \cap Z) = E(Y) + E(Z)$.
(h) Show that $V : \mathcal{I} \to \mathcal{P}$ is a bijective function with inverse $E : \mathcal{P} \to \mathcal{I}$.
(i) Show that A is a principal ring which is usually not a domain.
(j) Show that I is maximal if and only if $I = V(\{x\})$ for some $x \in X$.
(k) Show that if $x \in X$, then $A/E(\{x\}) \cong F$.
(l) Show that $A/E(Y) \cong A(Y)$.

Department of Mathematics, BASIS Scottsdale
Email address: paul.bailey@basised.com