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 ring 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: March 1, 1997.

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.

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 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.

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 $X, Y \subset R$. Show that $\mathrm{gr}_R(X \cap Y) = \mathrm{gr}_R(X) \cap \mathrm{gr}_R(Y)$.

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

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
(H1) $\phi(1_R) = 1_S$;
(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 39. 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 40. 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 41. 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 42. 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 43. Let $\phi : R \to S$ be a ring homomorphism and let $T \leq R$.
Show that $\phi(T) \leq S$.

Problem 44. Let $\phi : R \to S$ be a ring homomorphism and let $T \leq S$.
Show that $\phi^{-1}(T) \leq R$.

Problem 45. 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 46. 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 47. 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 48. 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 49. 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 50. 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 51. Let R be a ring and $I \lhd R$. Show that if I contains an invertible element, then I is improper.

Problem 52. Let R be a commutative ring. Show that R is simple if and only if R is a field.

Problem 53. Let R be a ring and let $\mathcal{I}$ be a collection of ideals of R. Show that $\cap\mathcal{I} \lhd R$.

Problem 54. 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 55. Let $\phi : R \to S$ be a ring homomorphism.
Show that $\ker(\phi) \lhd R$.

Problem 56. Let $\phi : R \to S$ be a ring homomorphism.
Show that ϕ is injective if and only if $\ker(\phi) = \{0\}$.

Problem 57. Let $\phi : R \to S$ be a ring homomorphism and let $J \lhd S$.
Show that $\phi^{-1}(J) \lhd R$.

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

Problem 59. 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 60. 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 61. Let R be a ring and let $I, J \lhd R$. Show that $\mathrm{gi}_R(I \cup J) = I + J$.

Problem 62. 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 63. 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 64. 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 65. 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 66. 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 67. 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 68. Let R be a commutative ring and set

$$I = \mathrm{gi}_R(R \smallsetminus R^\bullet).$$

Show that if I is a proper ideal, then R/I is an integral domain.

Problem 69. Let R be a commutative ring and set

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

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

Worksheet IX - Isomorphism Theorem

Problem 70. (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 71. 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 72. (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 73. (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 74. 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 75. 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 76. 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 77. 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 $H(R)$.

Notation 1. Viewing a ring R as an additive group, let $\mathrm{ord}^+(a)$ denote the additive order of $a \in R$.

Problem 78. Let R be a ring and let $\phi : \mathbb{Z} \to R$ be the unique ring homomoprhism 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 79. Let R be a ring.
(a) Show that $H(R) = \mathrm{gr}_R(\{1\})$.
(b) Show that $H(R) \leq Z(R)$.

Problem 80. 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 81. 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 82. 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 83. 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 84. 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 85. 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 15. 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 86. Let R be a commutative ring.
Show that $\{0\}$ is a prime ideal if and only if R is an integral domain.

Problem 87. 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 88. Let R be a commutative ring.
Show that $\{0\}$ is maximal if and only if R is a field.

Problem 89. 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 90. Let R be a commutative ring and let $I \lhd R$.
Show that if I is maximal, then I is prime.

Problem 91. 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 92. 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 93. 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 94. 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.

Department of Mathematics, University of California, Irvine
E-mail address: pbailey@math.uci.edu