WORKSHEET 1.1: RINGS, HOMOMORPHISMS, AND QUOTIENTS

A *ring* $(R,+,\cdot)$ is an abelian group $(R,+,0_R)$ together with a multiplication $\cdot$ and an element $1_R \in R$ satisfying the following axioms:

(i) (Identity) $1_R \cdot a = a \cdot 1_R = a$ for all $a \in R$,

(ii) (Associativity) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$,

(iii) (Left Distributivity) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$, and

(iv) (Right Distributivity) $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

We call 1_R the *multiplicative identity*. We generally write ab for $a \cdot b$, and we will write 1 and 0 for 1_R and 0_R when the the underlying ring is clear from context. A ring is *commutative* if $ab = ba$ for all $a, b \in R$.

Throughout this course, all rings have a multiplicative identity, but need not be commutative. In particular, matrix rings will be just as important to us as the ring of integers, or polynomial rings. The *zero ring* is the unique ring with a single element which satisfies $1 = 0$. An element $u \in R$ is a *unit* if there is an element $v \in R$ such that $uv = vu = 1$. In this case we say that v is the *multiplicative inverse* of u, which we generally denote by u^{-1}. We write $R^\times$ for the set of units of R. A *field* is a commutative ring with $1 \neq 0$ in which every nonzero element is a unit. The letter $\mathbb{K}$ will denote a field throughout these worksheets.

The goal of this worksheet is to introduce three related ways of studying rings: their elements, their homomorphisms, and their ideals. You already know a number of examples, including $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and matrix rings. The definitions let us discuss the features these examples share, while retaining differences such as whether multiplication is commutative or whether nonzero elements can be inverted. We begin with some calculations that illustrate these differences.

---

1. **Basic Ring Identities.** Throughout this question let R be a ring.

   (a) Starting from the axioms, prove the following:

   (i) If 1 and $1'$ both satisfy the identity axiom then $1 = 1'$. Hint: evaluate $1 \cdot 1'$ in two different ways.

   (ii) If 0 and $0'$ both satisfy the property of being additive identities then $0 = 0'$.

   (iii) If $a + b = 0$ and $a + c = 0$ then $b = c$.

   Hence for any ring the additive and multiplicative identity elements are unique, and for any element $a \in R$ there is a unique additive inverse, which we generally denote $-a$.

(b) Starting from the axioms, prove the following identities:

(i) $a0 = 0a = 0$ for all $a \in R$,

(ii) $(-a)b = -(ab) = a(-b)$ for all $a, b \in R$.

(c) If $1 = 0$, explain why the ring must have only one element.

(d) Suppose $vu = 1$ and $uw = 1$. Compute $v(uw)$ and $(vu)w$ and conclude $v = w$. Deduce that u is a unit and that its inverse is unique, so that the notation u^{-1} is justified. Deduce also that $(u^{-1})^{-1} = u$.

(e) Prove that $R^\times$ is a group under multiplication, with $(uv)^{-1} = v^{-1}u^{-1}$.

2. **First Examples of Rings.**

(a) For a positive integer n, use the familiar additive quotient group $\mathbb{Z}/n\mathbb{Z}$ and define $\overline{a}\,\overline{b} = \overline{ab}$. Check that this does not depend on the chosen representatives. What is the identity?

(b) Characterize the units in the following rings:

(i) $\mathbb{Z}$ (iv) $\mathbb{K}$ (vii) $\mathbb{Z}/4\mathbb{Z}$

(ii) $\mathbb{C}$ (v) $\mathbb{Z}/12\mathbb{Z}$ (viii) $\mathbb{Z}/2\mathbb{Z}$

(iii) $\mathbb{R}$ (vi) $\mathbb{Z}/30\mathbb{Z}$ (ix) $\mathbb{Z}/n\mathbb{Z}$

(c) An non-zero element $a \in R$ is a *zero-divisor* if there exists a non-zero element $b \in R$ such that $ab = ba = 0$. Characterize the zero divisors in all of the rings from part (a).

(d) Let $\mathrm{Mat}_n(\mathbb{K})$ denote the set of $n \times n$ matrices over $\mathbb{K}$. Prove that $\mathrm{Mat}_n(\mathbb{K})$ is a ring under normal matrix addition and multiplication. What are the identity elements.

(e) For integers $1 \le i, j \le n$ let $E_{i,j}$ denote the $n \times n$ matrix whose (i, j)-th entry is 1 and all other entries are zero. Compute $E_{12}E_{21}$ and $E_{21}E_{12}$. What does this show about the ring $\mathrm{Mat}_n(\mathbb{K})$.

(f) Explain why the units of $M_2(k)$ are precisely the invertible matrices. Compare "nonzero" and "invertible" in $M_2(k)$ and in k.

(g) Give an example of two elements $u, v \in \mathrm{Mat}_2(\mathbb{R})$ showing that in general $(uv)^{-1} = u^{-1}v^{-1}$ can fail.

(h) Let R be a ring and $\mathrm{Mat}_n(R)$ denote the set of $n \times n$ matrices whose entries are elements in R. Define a notion of matrix multiplciation and matrix addition for elements of $\mathrm{Mat}_n(R)$ that agrees with our normal matrix operations when $R = \mathbb{K}$. Is $\mathrm{Mat}_n(R)$ a ring?

If R is a ring the *polynomial ring* with coefficients in R is the set $R[x]$ consists of finite formal sums $a_0 + a_1x + \cdots + a_dx^d$ with coefficients in R. Addition is coefficient-wise, and multiplication is obtained by distributing, using $x^i x^j = x^{i+j}$, and collecting coefficients of the same power of x. We can regard elements of R as constant polynomials: their addition and multiplication in $R[x]$ agree with the original operations on R. The word "formal" means that equality is determined by the coefficients. This is slightly different from thinking of a polynomial as a function on R. Given an element $a \in R$, we can substitute a for x to obtain a value $f(a) \in R$, but the polynomial f and the value $f(a)$ are different objects. Over some fields, even two different polynomials can define the same function. We will see an example below and then return to substitution when we discuss ring homomorphisms.

For a nonzero polynomial f, its *degree*, denoted $\deg(f)$, is the largest exponent with nonzero coefficient. That coefficient is called the *leading coefficient*. Looking at leading coefficients is often a useful way to understand multiplication without expanding every term of a product.

---

3. **Polynomial Rings.**

   (a) Compute $(a + bx)(c + dx)$ in $\mathbb{K}[x]$. Identify the coefficient of x^j in the product of two general polynomials.

   (b) By looking at leading coefficients, prove $\deg(fg) = \deg(f) + \deg(g)$ for nonzero $f, g \in \mathbb{K}[x]$. Explain why the same argument works in $\mathbb{Z}[x]$.

   (c) Determine the units of $\mathbb{K}[x]$. In particular, can you divide by x in this ring?

   (d) Let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Evaluate $x^2 - x$ at both elements of $\mathbb{F}_2$. Is $x^2 - x$ the zero polynomial? Explain the difference between equality of polynomials and equality of the functions they define on a field.

A *ring homomorphism* is a function $\phi : R \to S$ atisfying the following conditions for all $a, b \in R$:

(i) $\phi(a + b) = \phi(a) + \phi(b)$.

(ii) $\phi(ab) = \phi(a)\phi(b)$.

(iii) $\phi(1_R) = 1_S$.

The first condition says that a ring homomorphism is a homomorphism of the underlying additive groups. In particular, a ring homomorphism preserves 0 and additive inverses. The second condition ensures that a ring homomorphism respects the multiplicative structure of both rings. Finally, the last condition ensures that all ring homomorphism preserve the multiplicative identity. Condition (iii) does not follow from the others, and some others do not make this assumption in their definition of ring homomorphims.

An ring homomorphism $\phi : R \to S$ is a *ring isomorphism* if it has an inverse $\phi^{-1} : S \to R$, which is also a ring homomorphism. Just as with groups, the condition of a ring homomorphism being a ring isomorphism is essentially a set theoretic one: a ring homomorphism $\phi : R \to S$ is an isomorphism if and only if ϕ is a bijective. You will check this equivalence shortly. We say that two rings R and S are isomorphic, and write $R \cong S$, if there exists an isomorphism between them. An isomorphism allows us to identify two rings which are essentially the same up relabeling the

As with group homomorphisms, a ring homomorphism comes with two very important subsets; its *kernel* and its *image*:

$$\ker(\phi) := \{a \in R \mid \phi(a) = 0_S\} \subset R \qquad \text{and} \qquad \operatorname{img}(\phi) := \{\phi(a) \mid a \in R\} \subset S.$$

Notice that a map is surjective exactly when its image is the whole target, while its kernel measures its failure to be injective.

A *subring* of R is a subset $T \subset R$ that is a ring under the inherited operations and contains 1_R. The image of a ring homomorphism is a subring of its target. The kernel has a different closure property, which will lead us shortly to the notion ideals.

---

4. **Examples and Properties of Ring Homomorphisms.** Throughout this exercise let R be a ring.

   (a) Prove that a ring homomorphism preserves 0, negatives, and units. If u is a unit, what must $\phi(u)^{-1}$ be?

   (b) Show that there is exactly one ring homomorphism $\phi : \mathbb{Z} \to R$. Write down a concrete description of this homomorphism when $R = \mathbb{Z}, \mathbb{Q}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}$, and $\mathrm{Mat}_2(\mathbb{R})$.

   (c) For each of the following examples determine whether a ring homomorphism exists, and if it does, whether it is unique:

   $$\mathbb{Z}/6\mathbb{Z} \xrightarrow{\mathbb{Z}} /3\mathbb{Z}, \qquad \mathbb{Z}/3\mathbb{Z} \xrightarrow{\mathbb{Z}} /6\mathbb{Z}, \qquad \mathbb{Z}/4\mathbb{Z} \xrightarrow{\mathbb{Z}} /4\mathbb{Z},$$

   Hint: Start by deciding where $\overline{1}$ would have to go, and then use an additive relation it satisfies.

   (d) For $a \in R$, the *evaluation at a homomorphism* is given by $\mathrm{ev}_a : R[x] \to R$ by $f \mapsto f(a)$. Carefully check that ev_a is a surjective ring homomorphism.

   (e) Let $\phi : R \to S$ be a ring homomorphism. Prove that $\operatorname{img}(\phi) \subset S$ is a subring of S.

   (f) Let $\phi : R \to S$ be a ring homomorphism. Prove the following:

      (i) Prove that ϕ is surjective if and only if $\operatorname{img}(\phi) = S$.

      (ii) Prove that ϕ is injective if and only of $\ker(\phi) = \{0\}$.

      (iii) Prove that ϕ is an isomorphism if and only if ϕ is bijective.

We would now like to describe the subsets of a ring that can occur as kernels. The kernel of a ring homomorphism is an additive subgroup, but it satisfies more than closure under addition. If $\phi(a) = 0$, then $\phi(ra) = \phi(r)\phi(a) = 0$ and $\phi(ar) = \phi(a)\phi(r) = 0$ for every $r \in R$. Thus multiplying an element of the kernel by an arbitrary ring element, on either side, keeps us in the kernel. A *two-sided ideal* $I \subset R$ is an additive subgroup such that $ra \in I$ and $ar \in I$ for all $r \in R$ and $a \in I$. A *left ideal* requires only the condition $ra \in I$. A *right ideal* requires only that $ra \in I$.

Unless we say otherwise, *ideal* will always mean two-sided ideal. In a commutative ring this distinction disappears, however, in arbitrary rings it is very important. For example, we will see an example of a left ideal in a matrix ring that is not a two-sided ideal. Note also that an ideal need not be a subring under our convention: a proper ideal does not contain 1_R.

For elements $a_1, \ldots, a_t$ in a commutative ring R, we write

$$\langle a_1, \ldots, a_t \rangle \coloneqq \left\{ r_1 a_1 + \cdots + r_t a_t \;\middle|\; r_i \in R \right\},$$

which is the ideal *generated* by $a_1, \ldots, a_t$. More generally, if we do not assume R is commutative the ideal *generated* by elements $a_1, \ldots, a_t \in R$ is

$$\langle a_1, \ldots, a_t \rangle \coloneqq \left\{ r_1 a_1 s_1 + \cdots + r_t a_t s_t \;\middle|\; r_i, s_i \in R \right\},$$

It is worth thinking for a moment, why these two definitions agree. In both situations we say that an ideal $I \subset R$ is a *principal ideal* if and only if there exists $a \in R$ such that $I = \langle a \rangle$, i.e., I is generated by a single element. More intrinsically, the ideal generated by $a_1, \ldots, a_t \in R$ is the smallest ideal of R containing all of the a_i simultaneously.

---

5. **Properties & Examples of Ideals.** Throughout this exercise let R be a ring.

   (a) Let $I, J \subset R$ be ideals. Prove that $I \cap J$ is an ideal.

   (b) Give an example to show that if $I, J \subset R$ are ideals then $I \cup J$ need not be an ideal.

   (c) Let $I, J \subset R$ be idea. Prove that *ideal sum* of I and J defined below is an ideal:

   $$I + J \coloneqq \left\{ a + b \;\middle|\; a \in I,\, b \in J \right\}.$$

   (d) Let $a_1, \ldots, a_t \in R$. Prove $\langle a_1, \ldots, a_t \rangle \subset R$ is a two-side idea.

   (e) Let $a_1, \ldots, a_t \in R$. Prove that $\langle a_1, \ldots, a_t \rangle$ is the smallest ideal of R containing $a_1, \ldots, a_t$, i.e.,

   $$\langle a_1, \ldots, a_t \rangle = \bigcap_{\substack{J \subset R \\ a_1, \ldots, a_t \in J}} .$$

(f) Let $I \subset R$ be an ideal. Prove that $I = R$ if and only if I contains a unit. Deduce that the only ideals of a field $\mathbb{K}$ are $\{0\}$ and $\mathbb{K}$ itself.

(g) Explicitly describe the ideals $\langle n \rangle \subset \mathbb{Z}$ and $\langle x^2 \rangle \subset \mathbb{K}[x]$. Which polynomials occur in the second example, and is x one of them?

(h) Let $L \subset \mathrm{Mat}_2(\mathbb{K})$ denote the set of matrices whose second column is zero. Prove that L is a left ideal. Compute $E_{11}E_{12}$ and use it to show that L is not a right ideal, and hence not a two-sided ideal.

6. **Ideals and Homomorphisms.** Throughout this exercise let $\phi : R \to S$ be a ring homomorphism.

(a) Prove that $\ker(\phi)$ is a two-sided ideal of R.

(b) Prove that if $J \subset S$ be an ideal then $\phi^{-1}(J)$ is an ideal. Explain why part (a) is the special case when $J = \langle 0 \rangle$.

(c) Consider the inclusion $\psi : \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$ given by $1 \mapsto 1$ and the ideal $\langle 2 \rangle \subset \mathbb{Z}$. Show that $\psi(\langle 2 \rangle) \subset \mathbb{Z}[x]$ is not an ideal. Hence the image of an ideal need not be an idea.

(d) Prove that if ϕ is surjective then $\phi(I) \subset S$ is an ideal for all ideals $I \subset R$.

Let $I \subset R$ be a two-sided ideal. Since I is an additive subgroup and the additive group of R is abelian, we can form the quotient group R/I. Its elements are cosets $r + I$, and $r + I = s + I$ if and only if $r - s \in I$. Addition is given by $(r + I) + (s + I) = (r + s) + I$. To obtain a *quotient ring*, we define multiplication by

$$(r + I)(s + I) = rs + I.$$

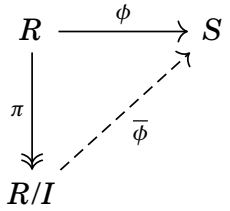
The fact that I is a two-sided ideal guarantees that this formula is well defined. Together with the identity $1_R + I$, it makes R/I a ring! From group theory we know that a quotient group R/I comes with a special group homomorphism we call the *quotient map*

$$R \xrightarrow{\pi} R/I \qquad\qquad r \longmapsto r + I \ .$$

The map π is surjective and the kernel of π, as a group homomorphism, is precisely I. However, multiplication on R/I was defined precisely so that $\pi(r)\pi(s) = (r + I)(s + I) = rs + I = \pi(rs)$, and $\pi(1_R) = 1_R + I$. Hence π is actually a surjective ring homomorphism with kernel I. Notice that this really came down to the right definition of R/I. Consequently, every ideal occurs as the kernel of a ring homomorphism, and by Problem 5 these are the only subsets which do.

One way to think of R/I is as the ring obtained when we imposing the equations $a = 0$ for all $a \in I$. For example, in $\mathbb{Z}/n\mathbb{Z}$ we are imposing the equation $n = 0$, which forces integers differing by a multiple of n to represent the same element. More generally, a ring homomorphism $\phi : R \to S$ which sends every element of I to zero determines a unique ring homomorphism $\overline{\phi} : R/I \to S$ such that $\overline{\phi} \circ \pi = \phi$ where π is the quotient

homomorphism. We often express this relationship by drawing a *commutative diagram*



In particular, homomorphisms out of R/I can be describe entirely in terms of homomorphisms out of R, namely those which kill I. This is what is often called the universal property of quotient rings. We will prove the construction and this property together in the following exercise, and return to the general language of universal properties next week.

---

7. **Construction and Properties of Quotient Rings.** Throughout this exercise let I be a two-sided ideal of a ring R.

   (a) Suppose $r' = r + a$ and $s' = s + b$ with $a, b \in I$. Expand $r's' - rs$ and prove that it lies in I. Conclude that the proposed multiplication on R/I is well defined.

   (b) Write down the formulas for addition, multiplication, and the identity element in R/I. Verify associativity and both distributive laws by computing with representatives. Why is R/I still a ring when $I = R$, which ring is it?

   (c) Prove that $\pi : R \to R/I$, $r \mapsto r + I$, is a surjective ring homomorphism with $\ker(\pi) = I$.

   (d) Return to the left ideal $L \subset \mathrm{Mat}_2(\mathbb{K})$ from Problem 5. We have $E_{11} + L = 0 + L$. Multiply these two representatives on the right by E_{12} and compare the resulting cosets. Explain why the proposed multiplication on $\mathrm{Mat}_2(\mathbb{K})/L$ is not well defined, and which hypothesis of part (a) has been lost.

   (e) Suppose $\phi : R \to S$ is a ring homomorphism with $I \subset \ker(\phi)$. Prove that $\overline{\phi}(r + I) = \phi(r)$ is a well-defined ring homomorphism $R/I \to S$, and that it is the unique one satisfying $\overline{\phi} \circ \pi = \phi$. Explain in words why a homomorphism out of R/I is the same thing as a homomorphism out of R which sends I to zero.

The construction of quotient rings also clarifies the relationship between the kernel and the image of a ring homomorphism. A ring homomorphism $\phi \to S$ respects the relation $r + I = r' + I$ precisely when it sends every element of I to zero. Whenever $I \subseteq \ker(\phi)$, we can therefore define a ring homomorphism

$$\overline{\phi}/I \longrightarrow S, \qquad r + I \longmapsto \phi(r).$$

Thus ϕ can be computed in two steps: first pass to the quotient, and then apply $\overline{\phi}$. Taking $I = \ker(\phi)$ gives a particularly useful description. Two elements of R have the same image exactly when their difference

lies in $\ker(\phi)$, so passing to this quotient identifies exactly the elements that ϕ identifies. The induced map is therefore injective, and its image is $\mathrm{img}(\phi)$.

Theorem 1 (First Isomorphism Theorem for Rings)**.** *Let $\phi \to S$ be a ring homomorphism. Then the map*

$$\overline{\phi}/\ker(\phi) \longrightarrow \mathrm{img}(\phi), \qquad r + \ker(\phi) \longmapsto \phi(r),$$

is an isomorphism of rings. In particular, there is a commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\quad\phi\quad} & S \\ {\scriptstyle\pi}\downarrow & & \uparrow \\ R/\ker(\phi) & \xrightarrow[\sim]{\ \overline{\phi}\ } & \mathrm{img}(\phi) \end{array}$$

Every ring homomorphism can therefore be understood as a quotient map followed by an isomorphism and an inclusion. If ϕ is surjective, then $\mathrm{img}(\phi) = S$, and the theorem gives $R/\ker(\phi) \cong S$. This provides our standard method for recognizing a quotient ring: construct a surjective homomorphism onto a ring we already understand, and then compute its kernel.

---

8. **First Isomorphism Theorem and Evaluation Maps.**

   (a) Use Problem 7 to construct the displayed map. Why is $\mathrm{img}(\phi)$ a ring, and why is its multiplicative identity the correct one?

   (b) Prove that the displayed map is surjective onto $\mathrm{img}(\phi)$, and that if two cosets have the same image then they are equal. Combine this with Problem 4 to finish the proof of the theorem.

   (c) Apply the theorem to the reduction homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Identify the kernel and describe the induced isomorphism explicitly. What does it do to the coset of 1?

   (d) For $a \in \mathbb{K}$, prove that $\ker(\mathrm{ev}_a) = \langle x - a \rangle$. One inclusion is immediate. For the other, first factor $x^j - a^j$ as $(x-a)(x^{j-1} + x^{j-2}a + \cdots + a^{j-1})$ and then apply this to $f(x) - f(a)$.

   (e) Deduce that $\mathbb{K}[x]/\langle x - a \rangle \cong \mathbb{K}$, and write the isomorphism down explicitly. What does the class of x become? Explain why this quotient is a genuinely different construction from the polynomial ring $\mathbb{K}[x]$ itself.

For the evaluation homomorphism $\mathrm{ev}_a : \mathbb{K}[x] \to \mathbb{K}$, the kernel $\langle x - a \rangle$ imposes the relation $x = a$, and the resulting quotient is therefore isomorphic to $\mathbb{K}$. We can use the same construction to impose a polynomial relation with a rather different effect. Consider the ring:

$$\mathbb{K}[\varepsilon] := \mathbb{K}[x]/\langle x^2 \rangle$$

where $\epsilon = x + \langle x^2 \rangle$. This ring is called the ring of *dual numbers* over $\mathbb{K}$. The relation imposed by the quotient is $\varepsilon^2 = 0$. It does not impose $\varepsilon = 0$, since the polynomial x is not a multiple of x^2. The distinction is what makes the example useful: it gives us a very simple commutative ring containing a nonzero element whose square is zero.

An element $a \in R$ of a ring is *nilpotent* if $a^m = 0$ for some integer $m \geq 1$. Recall from Problem 2 that a nonzero element a is a zero divisor if $ab = ba = 0$ for some nonzero $b \in R$. Hence a nonzero nilpotent element is always a zero divisor, however, the converse is not true. Neither phenomenon can occur in a field, as you saw when you computed the units of $\mathbb{K}$.

Every element of $\mathbb{K}[\varepsilon]$ can be expressed using only the classes of 1 and x, because every higher power of x already lies in $\langle x^2 \rangle$. In the following exercise we will show that this expression is unique, use it to describe the operations in $\mathbb{K}[\varepsilon]$, and determine which elements are units. We will revisit the same example as a module in the next worksheet.

---

9. **Computations with the Dual Numbers.** Throughout this exercise let $\mathbb{K}[\varepsilon] = \mathbb{K}[x]/\langle x^2 \rangle$ and $\varepsilon = x + \langle x^2 \rangle$.

   (a) Prove that every element of $\mathbb{K}[\varepsilon]$ can be written uniquely as $a + b\varepsilon$ with $a, b \in \mathbb{K}$. Hint: for uniqueness, use your description of $\langle x^2 \rangle$ from Problem 5. Deduce that $\varepsilon \neq 0$ and $\varepsilon^2 = 0$.

   (b) Derive formulas for addition and multiplication in these coordinates. Compute $(1 + \varepsilon)^2$, and say what happens when $\mathbb{K} = \mathbb{F}_2$.

   (c) Suppose $(a + b\varepsilon)(c + d\varepsilon) = 1$ and compare coefficients. Prove that $a + b\varepsilon$ is a unit if and only if $a \neq 0$, and compute its inverse when it exists. Describe $\mathbb{K}[\varepsilon]^\times$.

   (d) Determine all nilpotent elements and all nonzero zero divisors of $\mathbb{K}[\varepsilon]$. For the nilpotents, begin by considering the constant coefficient of a power. For the zero divisors, use your description of $A^\times$.

   (e) Construct the homomorphism $\mathbb{K}[\varepsilon] \to \mathbb{K}$ sending $a + b\varepsilon$ to a. Compute its kernel and identify the resulting quotient using the first isomorphism theorem.

   (f) More generally, prove that for $m \geq 2$ every class in $\mathbb{K}[x]/\langle x^m \rangle$ has a unique representative $a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$. Exhibit a nonzero nilpotent element. Which parts of your argument for $m = 2$ still work, and which need modification?

So far we have used homomorphisms to compare two different rings. It is equally useful to consider the homomorphisms from a ring to itself, since these record the internal symmetries of that ring. A *ring automorphism* of R is a ring isomorphism $\phi : R \to R$, and we write $\mathrm{Aut}(R)$ for the set of all automorphisms of R. The identity map Id_R is an automorphism, a composition of two automorphisms is again an automorphism, and the inverse of an automorphism is one by definition. Hence $\mathrm{Aut}(R)$ is a group under

composition, exactly as for groups and vector spaces. An automorphism is a relabeling of the elements of R which preserves every feature expressible in terms of $+$, $\cdot$, and 1. Units are sent to units, nilpotents to nilpotents, zero divisors to zero divisors, and ideals to ideals.

Every ring comes with one systematic supply of automorphisms. The *center* of a ring R is

$$Z(R) \coloneqq \{z \in R \mid zr = rz \text{ for all } r \in R\}.$$

Notice that R is commutative if and only if $Z(R) = R$. For a unit $u \in R^\times$, conjugation $\gamma_u(r) = uru^{-1}$ is an automorphism of R, and automorphisms of this form are called *inner*. In a commutative ring every inner automorphism is the identity, so for rings such as $\mathbb{Z}$ or $\mathbb{K}[x]$ the interesting automorphisms must come from elsewhere; typically they come from substitution, as in the polynomial case where x may be replaced by $ax + b$.

Frequently we want to compare automorphisms relative to a subring which we regard as fixed. If $T \subset R$ is a subring, we write $\mathrm{Aut}_T(R)$ for the subgroup of automorphisms which fix every element of T. Complex conjugation is an element of $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$, and the ring $\mathbb{K}[x]$ is most naturally studied through $\mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x])$. This relative point of view is the starting point for Galois theory, which is major focus of Math 111.

---

10. **Automorphisms of Rings.** Throughout this exercise let R be a ring.

    (a) Prove that $\mathrm{Aut}(R)$ is a group under composition. Prove that any $\phi \in \mathrm{Aut}(R)$ restricts to a group automorphism of $R^\times$, and that ϕ carries nilpotent elements to nilpotent elements and zero divisors to zero divisors.

    (b) Prove that $\phi(I)$ is an ideal for every ideal $I \subset R$ and every $\phi \in \mathrm{Aut}(R)$, and that $I \mapsto \phi(I)$ is a bijection from the set of ideals of R to itself. Hint: use Problem 5.

    (c) Prove that $\mathrm{Aut}(\mathbb{Z})$ and $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ are both trivial. Hint: use the uniqueness statement of Problem 4. Prove also that $\mathrm{Aut}(\mathbb{Q})$ is trivial, by first showing that any automorphism fixes $\mathbb{Z}$ pointwise.

    (d) For $u \in R^\times$ define $\gamma_u(r) = uru^{-1}$. Prove that $\gamma_u \in \mathrm{Aut}(R)$ and that $u \mapsto \gamma_u$ is a group homomorphism $R^\times \to \mathrm{Aut}(R)$. Prove that its kernel is $Z(R) \cap R^\times$, and deduce that every inner automorphism is trivial precisely when R is commutative.

    (e) Let $a \in \mathbb{K}^\times$ and $b \in \mathbb{K}$. Adapting your argument from Problem 4, show that $f(x) \mapsto f(ax + b)$ is a ring homomorphism $\mathbb{K}[x] \to \mathbb{K}[x]$ fixing $\mathbb{K}$ pointwise, and exhibit its inverse. Conversely, suppose $\phi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x])$. Using the degree formula of Problem 3, prove that $\deg(\phi(x)) = 1$, and conclude that $\mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x])$ consists exactly of these substitutions.

    (f) Prove that complex conjugation is an automorphism of $\mathbb{C}$ fixing $\mathbb{R}$ pointwise. Prove that $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ has exactly two elements. Hint: such a ϕ is determined by $\phi(i)$, and $\phi(i)^2 = -1$.

(g) Let A be the ring of dual numbers. Prove that any $\phi \in \mathrm{Aut}_{\mathbb{K}}(A)$ satisfies $\phi(\varepsilon) = b\varepsilon$ for some $b \in \mathbb{K}^\times$, and that every such b arises. Hint: use your classification of the nilpotents and units from Problem 9. Deduce that $\mathrm{Aut}_{\mathbb{K}}(A) \cong \mathbb{K}^\times$.

(h) Prove that $\gamma_u = \gamma_v$ in $\mathrm{Aut}(\mathrm{Mat}_n(\mathbb{K}))$ if and only if u and v differ by a nonzero scalar matrix, so that the inner automorphisms of $\mathrm{Mat}_n(\mathbb{K})$ form a copy of $\mathrm{GL}_n(\mathbb{K})/\mathbb{K}^\times$. It is a theorem of Skolem and Noether that these are in fact all of the automorphisms of $\mathrm{Mat}_n(\mathbb{K})$; we will not prove this, but it is worth comparing with parts (e) and (g), where the automorphism groups were visibly not inner.

The ideals $\langle n\rangle \subset \mathbb{Z}$ and $\langle x-a\rangle, \langle x^2\rangle \subset \mathbb{K}[x]$ are all principal. The definition of a generated ideal allows several generators, and it is natural to ask whether they can always be replaced by a single one. This is not the case in general, even for familiar commutative rings. We will prove that the ideal $\langle 2, x\rangle \subset \mathbb{Z}[x]$ is not principal. The argument uses only the degree of a product and the constant coefficient of a polynomial, so it does not require any general theory of factorization.

---

11. **A Nonprincipal Ideal in $\mathbb{Z}[x]$.** Throughout this exercise let $I = \langle 2, x\rangle \subset \mathbb{Z}[x]$.

(a) Prove that I consists exactly of the polynomials with even constant coefficient. For the harder inclusion, separate the constant term of a polynomial from all of the terms involving x.

(b) Define $\theta : \mathbb{Z}[x] \to \mathbb{F}_2$ by $\theta(f) = \overline{f(0)}$. Prove that θ is a surjective ring homomorphism with $\ker(\theta) = I$. Using Problem 8, deduce that $\mathbb{Z}[x]/I \cong \mathbb{F}_2$ and in particular that $I \neq \mathbb{Z}[x]$.

(c) Suppose for contradiction that $I = \langle d\rangle$ for some $d \in \mathbb{Z}[x]$. Since $2 \in I$, there is a polynomial h with $2 = dh$. Use Problem 3 to show that d must be a nonzero constant integer.

(d) Since $x \in I$, we may also write $x = dq$ for some $q \in \mathbb{Z}[x]$. Compare the coefficients of x on both sides. What does this force d to be?

(e) Explain why the conclusion of (d) contradicts (b), and conclude that I is not principal. Where exactly did the argument use both of the generators?

We finish by introducing several additional examples. Some extend constructions we have already met, such as polynomial rings and matrix rings; others produce a ring from a group or from a collection of operators. These examples will recur as the course develops. At this stage we will focus on their operations and on a few distinguishing properties.

- *Formal power series.* A formal power series is like a polynomial, except that it may have infinitely many nonzero coefficients. The ring $R[[t]]$ consists of expressions

$$\sum_{j \geq 0} a_j t^j = a_0 + a_1 t + a_2 t^2 + \cdots$$

for $a_j \in R$. We add and multiply using the same rules as for polynomials. For example, the product of $a_0 + a_1 t + a_2 t^2 + \cdots$ and $b_0 + b_1 t + b_2 t^2 + \cdots$ begins

$$a_0 b_0 + (a_0 b_1 + a_1 b_0) t + (a_0 b_2 + a_1 b_1 + a_2 b_0) t^2 + \cdots.$$

In general, the coefficient of t^n is $\sum_{i=0}^{n} a_i b_{n-i}$. Although the series can be infinite, computing any one coefficient requires only finitely many operations in R. The word "formal" means that we work with the coefficients without assigning a value to t or asking whether the series converges. Two formal power series are equal exactly when all their corresponding coefficients agree.

- *Endomorphism rings.* An *endomorphism* is a homomorphism from an object to itself. If $(B, +)$ is an abelian group, the set of its endomorphisms is denoted $\mathrm{End}_{\mathbb{Z}}(B)$. We make this set into a ring by defining

$$(f + g)(b) = f(b) + g(b), \qquad (fg)(b) = f(g(b)).$$

Thus addition means adding the outputs, while multiplication means applying g first and then f. The zero element is the map sending every element to 0, and the multiplicative identity is the identity map Id_B. Similarly, the linear maps from a vector space V to itself form a ring $\mathrm{End}_{\mathbb{K}}(V)$. If V has dimension n, choosing a basis represents these maps by $n \times n$ matrices, with addition and composition corresponding to matrix addition and multiplication.

- *Upper-triangular matrices.* A 2×2 matrix is *upper triangular* if its lower-left entry is zero. These matrices form a subring of $\mathrm{Mat}_2(\mathbb{K})$: adding, subtracting, or multiplying two of them again gives an upper-triangular matrix, and the identity matrix is upper triangular. In particular,

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix}.$$

This ring is not commutative. For example, if

$$P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

then $PN = N$ but $NP = 0$.

- *Group rings.* Let G be a group. For each $g \in G$, introduce a formal symbol z_g. The group algebra $\mathbb{K}[G]$ consists of formal sums

$$\sum_{g \in G} a_g z_g, \qquad a_g \in \mathbb{K},$$

in which only finitely many coefficients are nonzero. Here z_g are formal symbols. We add by collecting coefficients of the same symbol, and multiply by distributing and using the rule

$$z_g z_h = z_{gh}.$$

Thus multiplication of the symbols records multiplication in the group. Two sums are equal exactly when the coefficient of each symbol agrees. The multiplicative identity is z_e, where e is the identity of G. We define $\mathbb{Z}[G]$ analogously.

- *The Weyl algebra.* Suppose $\mathbb{K}$ has characteristic zero, meaning that $n \cdot 1_{\mathbb{K}} \neq 0$ for every positive integer n. Let $\mathrm{End}_{\mathbb{K}}(\mathbb{K}[t])$ denote the ring of $\mathbb{K}$-linear maps $\mathbb{K}[t] \to \mathbb{K}[t]$, where addition is pointwise and multiplication is composition. Consider the following two $\mathbb{K}$-linear endomorphisms

$$\begin{array}{ccc} \mathbb{K}[t] & \xrightarrow{\;X\;} & \mathbb{K}[t] \\ f & \longmapsto & tf \end{array} \qquad\qquad \begin{array}{ccc} \mathbb{K}[t] & \xrightarrow{\;\partial\;} & \mathbb{K}[t] \\ f & \longmapsto & f' \end{array}$$

  where f' is the formal derivative of f. The first Weyl algebra $A_1(\mathbb{K})$ is the subring of $\mathrm{End}_{\mathbb{K}}(\mathbb{K}[t])$ generated by X, ∂, and the scalar multiples $c \cdot \mathrm{Id}$ of the identity operator. That is elements of $A_1(\mathbb{K})$ are the finite sums of composites of copies of X and ∂, scaled by elements of $\mathbb{K}$.

  Since the product is composition, the operator on the right acts first. So ∂X means "multiply by t, then differentiate," while $X\partial$ means "differentiate, then multiply by t." By the product rule these differ:

$$(\partial X)(f) = (tf)' = f + tf', \qquad (X\partial)(f) = tf'.$$

  Subtracting, $(\partial X - X\partial)(f) = f$ for every $p \in \mathbb{K}[t]$, that is $\partial X - X\partial = \mathrm{Id}$. Since $\mathrm{Id} \neq 0$, we get $\partial X \neq X\partial$, so $A_1(\mathbb{K})$ is not commutative.

---

12. **Power Series, Endomorphisms, and Other Ring Constructions.**

(a) In $\mathbb{K}[[t]]$, prove that $f = \sum a_j t^j$ can be a unit only if $a_0 \neq 0$. When $a_0 \neq 0$, look for $g = \sum b_j t^j$ with $fg = 1$ by solving first for b_0 and then recursively for b_n. Use this to characterize $\mathbb{K}[[t]]^\times$. Compare the inverse of $1 - t$ here with the behavior of $1 - t$ in $\mathbb{K}[t]$, which you determined in Problem 3.

(b) Check that pointwise addition and composition make $\mathrm{End}_{\mathbb{Z}}(B)$ a ring.

(c) Verify that the upper-triangular matrices form a subring of $\mathrm{Mat}_2(\mathbb{K})$ containing the identity. Exhibit two of them which do not commute.

(d) In $\mathbb{K}[S_3]$, compute $\big((12) + (23)\big)^2$, using right-to-left composition of permutations. Explain why this ring is noncommutative over every field, including in characteristic two.

(e) Evaluate $(\partial X - X\partial)(t^j)$ for every $j \geq 0$ and deduce that $\partial X - X\partial = 1$ in $A_1(\mathbb{K})$. Explain why the 1 here denotes an identity operator rather than a constant polynomial.

(f) Determine the units of the ring of upper-triangular matrices in $\mathrm{Mat}_2(\mathbb{K})$, and show that this ring has nonzero nilpotent elements. Compare with your answer for the dual numbers in Problem 9.
