1. RINGS

A ring is \((R, +, \cdot)\), consisting of a set \(R\) and two binary operations
\[+: R \times R \to R, \quad \cdot: R \times R \to R,\]
called “addition” and “multiplication”,
- \((R, +)\) is an additive group,
- \((R, \cdot)\) is a monoid, and
- multiplication distributes over addition:
  \[a(b + c) = (ab) + (ac), \quad (a + b)c = (ac) + (bc).\]

The identity for \(+\) is conventionally called 0, and the inverse of \(a\) under \(+\) is called \(-a\). The identity for \(\cdot\) is called 1.

1.1. Remark. There is an “associativity” issue when you have two different binary operations: in principle, you can interpret “\(a + b \cdot c\)” as meaning either:
\[(a + b) \cdot c \quad \text{or} \quad a + (b \cdot c).\]

We all know the solution: multiplication is always assumed to have precedence over addition, so we read this as \(a + (b \cdot c)\).

1.2. Remark. A ring without identity is one in which \((R, \cdot)\) is merely assumed to be a semi-group, i.e., there is no multiplicative identity. (Some people call this a rng.) In many introductory textbooks, “ring” is defined to mean what we are calling a “ring without identity”. Which is odd, since such textbooks have few or no examples of rings without identity, and for the most part, “ring” means the definition I am using for most mathematicians.

A ring is said to be commutative if multiplication is commutative: \(ab = ba\) for all \(a, b \in R\).

Basic examples of rings include:
- The real numbers \(\mathbb{R}\) (which is commutative).
- The integers \(\mathbb{Z}\) (commutative).
- The integers modulo \(n\): \(\mathbb{Z}/n\) (commutative).
- The ring \(R = M_{n \times n}(\mathbb{R})\) of \(n \times n\)-matrices over \(\mathbb{R}\). Not commutative if \(n \geq 2\).

1.3. Example. For any set \(X\) and ring \(R\), let \(S := \mathcal{F}(X, R) = \{f: X \to R\}\) be the set of all functions. Then \(S\) is a ring, with operations given by “pointwise” addition and multiplication:
\[(f + g)(x) := f(x) + g(x), \quad (fg)(x) := f(x)g(x).\]
(Exercise: check that this is a ring.) For instance, the set \(\mathcal{F}(\mathbb{R}, \mathbb{R})\) of real valued functions on \(\mathbb{R}\) is a ring.

If \(S\) is a ring, a multiplicative inverse of an element \(a \in S\) is an element \(b \in S\) such that
\[ab = 1 = ba.\]
Clearly not all elements of a ring can have a multiplicative inverse. For instance, \(0 \in \mathbb{R}\) has none.
1.4. Exercise. If $a \in S$ has a multiplicative inverse, then this inverse is unique. (Same as the proof for inverses in groups.)

We write $S^\times \subseteq S$ for the set of elements which have multiplicative inverses.

1.5. Exercise. $(S^\times, \cdot)$ is a group.

Examples: $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{Z}^\times = \{\pm 1\}$, $(\mathbb{Z}/n)^\times = \Phi(n)$, $M_{n \times n}(\mathbb{R})^\times = GL_n(\mathbb{R})$.

We say that a ring $S$ is a division ring if $S^\times = S \setminus \{0\}$, i.e., every non-zero element has a multiplicative inverse, and 0 does not have one.

A commutative division ring is called a field. For instance, $\mathbb{R}$ is a field. Also $\mathbb{Z}/p$ is a field when $p$ is prime.

Let’s carefully construct some more examples of rings.

2. Complex numbers and quaternions

We define a ring $\mathbb{C}$ as follows.

• The set of $\mathbb{C}$ is $\mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}$.

• Addition is defined by

$$(a, b) + (a', b') := (a + a', b + b').$$

• Multiplication is defined by

$$(a, b)(a', b') := (aa' - bb', ab' + ba').$$

2.1. Proposition. $\mathbb{C}$ is a field.

Proof sketch. The operations of $+$ and $\cdot$ are certainly well-defined. To show that $\mathbb{C}$ is a ring we need to check the following.

(1) $(\mathbb{C}, +)$ is an abelian group. In fact we have already done this: as a group $(\mathbb{C}, +)$ is the product group of $(\mathbb{R}, +)$ with itself. (Or: it is the same as the additive group of the vector space $\mathbb{R}^2$.)

(2) $(\mathbb{C}, \cdot)$ is a monoid. We need to check:

• Multiplication is associative. This is a little tedious, but here we go:

$$(a, b)(a', b')(a'', b'') = (aa' - bb', ab' + ba')(a'', b'') = (aa'a'' - bb'a'' - ab'b'' - ba'b'', aa'b'' - bb'b'' + ab'a'' + ba'a''),$$

$$(a, b)(a', b')(a'', b'') = (a, b)(a'a'' - b'b'', a'b'' + b'a'') = (aa'a'' - ab'b'' - ba'b'' - bb'a'', aa'b'' + ab'a'' + ba'a'' - bb'b''),$$

which are the same.

• There is a multiplicative unit, which I’ll call 1. In fact, if 1 = (1, 0), we check that

$$(1, 0)(a, b) = (a, b) = (a, b)(1, 0).$$
(3) The distributive law:
\[(a,b)((a',b') + (a'',b'')) = (a,b)(a' + a'', b' + b'')\]
\[= (aa' + aa'' - bb' - bb'', ab' + ab'' + ba' + ba'')\]
\[= (aa' - bb', ab' + ba') + (aa'' - bb'', ab'' + ba'')\]
\[= (a,b)(a',b') + (a,b)(a'',b''),\]
\[((a,b) + (a',b'))(a'',b'') = (a + a', b + b')(a'',b'')\]
\[= (aa'' + a'a'' - bb'' - b'b'', ab'' + a'b'' + ba'' + b'a'')\]
\[= (aa'' - bb'', ab'' + ba'') + (a'a'' - b'b'', a'b'' + b'a'')\]
\[= (a,b)(a'',b'') + (a',b')(a'',b'').\]

It is clear from the formula that multiplication is commutative:
\[(a,b)(a',b') = (aa' - bb', ab' + ba') = (a'a - b'b, b'a + a'b) = (a',b')(a,b).\]

To show that \(\mathbb{C}\) is a field, we have to produce a multiplicative inverse for each \((a,b)\) which is not equal to \((0,0)\). (Clearly \((0,0)\) can have no multiplicative inverse, since \((0,0)(a,b) = (0,0) \neq (1,0)\).)

In fact, given \(x = (a,b)\), define
\[y := \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right).\]

This is well defined since \(a^2 + b^2 > 0\) if \((a,b) \neq (0,0)\). Now check that \(xy = (1,0)\). (Exercise.) □

In practice we identify a real number \(a \in \mathbb{R}\) with the element \((a,0) \in \mathbb{C}\), and we write \(i := (0,1)\), so that we write
\[a + bi\]
instead of \((a,b)\).

Of course \(i^2 = -1\). This is the field of complex numbers.

William Hamilton (early 1800s) was one of the first people to realize that complex numbers could be described in this way, as ordered pairs of real numbers plus two binary operations. He worked for many years to do some thing similar for ordered triples of real numbers, but could not. Eventually he discovered that he could if he used ordered 4-tuples. This is the ring of quaternions, denoted \(\mathbb{H}\). (Setting this up is left as exercises.)

The quaternions are a non-associative ring with the property that the non-zero elements are exactly the ones with multiplicative inverses. Thus \(\mathbb{H}\) is a division ring.

3. Basic facts

Here are some basic facts about rings.

- The additive identity 0 is unique. (Because it is the additive identity in a group.)
- The multiplicative identity 1 is unique. (By the same proof we used for a group.)
- For any \(a \in S\), we have that
  \[0a = 0 = a0.\]

Proof: 0 + 0 = 0, so by the distributive law
\[0a = (0 + 0)a = 0a + 0a.\]

By cancellation in the additive group we get \(0 = 0a\). A similar proof shows \(a0 = 0\).

- Let \(-1\) be the additive inverse of 1. Then we always have the formula
  \[(-1)a = -a = a(-1),\]
where \(\text{"-a" is the additive inverse of } a\). Proof:
\[a + (-1)a = (1)a + (-1)a = (1 + (-1))a = 0a = 0,\]
where we use the distributive law in the second step.
• It is possible for a ring to have $1 = -1$, which implies $a = -a$ for all $a \in S$. For instance $S = \mathbb{Z}/2$.
• It is possible for a ring to have $1 = 0$. The set $S = \{0\}$ with one element has exactly one binary operation, which we use as the definition of both $+$ and $\cdot$, so $0 + 0 = 00 = 0$. Check that this is a ring, with $1 = 0$.

Exercise: if $S$ is a ring with $1 = 0$, then $S$ has only one element.

It is not generally the case that $a \neq 0$ and $b \neq 0$ implies $ab \neq 0$.

3.1. Example. In $S = M_{2 \times 2}(\mathbb{R})$, there exist non-zero matrices $A, B$ such that $AB = 0$.

3.2. Example. In $\mathbb{Z}/4$, we have $[2][2] = [0]$.

We say that a commutative ring $S$ is a \textbf{domain} if the set $S \setminus \{0\}$ is a monoid with respect to multiplication. Equivalently, $S$ is a domain if $1 \neq 0$ and $ab = 0$ implies either $a = 0$ or $b = 0$.

Examples of domains include all fields, and also the integers $\mathbb{Z}$.

4. Subrings

A \textbf{subring} of a ring $R$ is a subset $S \subseteq R$ such that (i) the $+$ and $\cdot$ operations restrict to $S$, and make $S$ a ring in its own right, and (ii) $R$ and $S$ have the same multiplicative identity.

Here is the subring criterion.

4.1. Proposition. A subset $S \subseteq R$ of a ring is a subring if and only if

\begin{enumerate}
\item $x, y \in S$ implies $x + y \in S$, i.e., $S$ is closed under addition,
\item $x \in S$ implies $-x \in S$,
\item $x, y \in S$ implies $xy \in S$,
\item $1 \in S$, where $1$ denotes the multiplicative identity in $R$.
\end{enumerate}

Proof. Note that by (4) $S$ is non-empty. Therefore together with (1) and (2) we see that $(S, +)$ is a subgroup of $(R, +)$. Property (3) implies that multiplication is a binary operation on $S$. It is straightforward to check the remaining properties (that multiplication is associative, that $1$ is a multiplicative identity, the distributive law) on $S$, because they hold in $R$. \hfill \Box

4.2. Example. The integers $\mathbb{Z}$ are a subring of $\mathbb{R}$.

4.3. Example. The rational numbers $\mathbb{Q}$ are a subring of $\mathbb{R}$.

4.4. Example. The inclusion $2\mathbb{Z} \subset \mathbb{Z}$ is not a subring. Although closed under the operations the subset does not have a multiplicative identity.

4.5. Example. Let $S \subset M_{2 \times 2}(\mathbb{R})$ be the subset consisting of $2 \times 2$ real matrices of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad a, b \in \mathbb{R}.$$ 

We can check that $S$ is a \textbf{subring} of the ring of matrices. (Verify this.)

4.6. Example. Let $T = \{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \}$. This is a subset of the ring $S = M_{2 \times 2}(\mathbb{R})$, which is closed under $+$ and $\cdot$, and in fact as such it is a ring in its own right: its multiplicative identity is $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

However, we will not consider it as a subring, because the multiplicative identity of $T$ is not the same as the one for $S = M_{2 \times 2}(\mathbb{R})$, which is the identity matrix. (Note: other sources may differ here, and will consider $T$ a subring. I won’t however.)

Compare with groups, where if $H \subseteq G$ is a subset closed under multiplication, and $H$ has an identity element for its product, then the identity element of $H$ must be the same as that for $G$.

(The proof of this used the existence of inverses in groups.) Rings are just different.

4.7. Example. The set $C(\mathbb{R}, \mathbb{R})$ of \textbf{continuous} functions $f : \mathbb{R} \to \mathbb{R}$ is a subring of $\mathcal{F}(\mathbb{R}, \mathbb{R})$, commutative with identity. This is because of the fact that sums and products of continuous functions are continuous; it has identity because constant functions are continuous.
5. Polynomials

Let $S$ be any ring. A sequence in $S$ is a function

$$a : \mathbb{Z}_{\geq 0} \to S.$$ 

I’ll use the notation $a_n \in S$ for the value of this function at $n$, i.e., I’m thinking of $a$ as an infinite sequence.

We define a new ring $P(S)$ as follows.

- Elements of $P(S)$ are sequences $a : \mathbb{Z}_{\geq 0} \to S$ for which there exists $N \in \mathbb{Z}_{\geq 0}$ such that $a_k = 0$ for all $k > N$. I.e., after finitely many terms the sequence is constant at 0.
- Addition is defined by the “pointwise addition” rule:

$$ (a + b)_n := a_n + b_n. $$

- Multiplication is defined by the rule:

$$ (ab)_n := \sum_{i=0}^{n} a_i b_{n-i} = a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1} + a_0 b_n. $$

E.g., $(ab)_0 = a_0 b_0$, $(ab)_1 = a_1 b_0 + a_0 b_1$, $(ab)_2 = a_2 b_0 + a_1 b_1 + a_0 b_2$, etc.

We need to make sure these operations are well-defined, because of the requirement that sequences in $P(S)$ are eventually 0. For instance, given $a, b \in P(S)$ let $N$ be such that $a_k = b_k = 0$ for all $k > N$. Then clearly $(a + b)_k = 0$ for $k > N$, while $(ab)_k = 0$ for $k > 2N$.

5.1. Exercise (Tedious). With this structure $P(S)$ is a ring. I’ll just note some features of this:

- The additive identity is the zero sequence: $0_n = 0$ for all $n$.
- The multiplicative identity is the sequence 1 defined by $1_0 = 1$, $1_k = 0$ for $k > 0$.
- If $S$ is commutative, so is $P(S)$.
- Associativity of multiplication is the hardest part to prove, but is is not too bad if you are good at multiple summations:

$$ ((ab)c)_n = \sum_{i=0}^{n} (ab)_i c_{n-i} $$

$$ = \sum_{i=0}^{n} \sum_{j=0}^{i} a_j b_{i-j} c_{n-i}, $$

$$ (a(bc))_n = \sum_{k=0}^{n} a_k (bc)_{n-k} $$

$$ = \sum_{k=0}^{n} \sum_{\ell}^{n-k} a_k b_\ell c_{n-k-\ell}. $$

These work out to the same thing, once you reindex the sums (so that $k = j$ and $\ell = i - j$, whence $n - k - \ell = n - i$). You will actually understand this better by working it out for small values of $n$, like 1 or 2 or 3.

Let $X \in P(S)$ denote the sequence defined by

$$ X_1 = 1, \quad X_k = 0 \text{ if } k \neq 1. $$

If we multiply $X$ by itself a bunch of times, we get $X^n$, which is the sequence with $(X^n)_n = 1$ and $(X^n)_k = 0$ if $k \neq 0$. Given $c \in S$, we use the same symbol $c$ to denote the sequence: $c_0 = c$, $c_k = 0$ if $k > 0$. With this notation we can write any $a \in P(S)$ as the expression

$$ a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$
assuming \( a_k = 0 \) for \( k > n \). We often choose to denote such an expression as “\( f(X) \)”, instead of as “\( a \)”.

In other words, \( P(S) \) is the ring of polynomials in one unknown with coefficients in \( S \).

**Warning.** Polynomials are not defined as functions, and they are not the same thing as functions. I’ll talk about this later.

Another notation for \( P(S) \) is \( S[X] \). (This is convenient when we want to name the “variable”.)

5.2. Exercise (On PS 9). If \( D \) is a domain, then \( D[X] \) is a domain.

This is also important because we can iterate the construction. Thus we may consider \( P(P(S)) \), aka \( (S[X])[Y] \). Elements \( f \) in this ring are expressions

\[
 f = g_0 + g_1 Y + g_2 Y^2 + \cdots + g_n Y^n,
\]

where each \( g_k \in S[X] \), so are expressions

\[
 g_k = a_{0k} + a_{1k} X + a_{2k} X^2 + \cdots + a_{2m} X^m
\]

with \( a_{ij} \in S \). Using the distributive law, we can always rewrite this as

\[
 f = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} X^i Y^j.
\]

We write \( S[X,Y] \) for \( (S[X])[Y] \), and call it the ring of polynomials in two variables. As we will see soon, the order of the variables isn’t really important: \( (S[X])[Y] \) and \( (S[Y])[X] \) are the “same” ring (really, they are canonically isomorphic).

You can go on to define \( S[X,Y,Z] \), etc.

6. CENTER OF A RING

Given a ring \( S \) let

\[
 \text{Cent}(S) := \{ a \in S \mid ab = ba \text{ for all } b \in S \},
\]

called the **center** of \( S \).

6.1. Exercise (On PS 9?). The set \( R = \text{Cent}(S) \) is a subring of \( S \). As a ring \( R \) is commutative.

Note that if \( S \) is commutative, then \( \text{Center}(S) = S \).

6.2. Example. The center of the quaternion algebra \( \mathbb{H} \) is the subset \( \mathbb{R} \mathbf{1} = \{ \lambda \mathbf{1} \mid \lambda \in \mathbb{R} \} \) of scalar quaternions. It’s straightforward to check that scalar quaternions are in the center. To see these are the only ones, check commutativity with \( i \), \( j \), and \( k \). For instance, commutativity with \( i \) gives

\[
 (a \mathbf{1} + bi + cj + dk) i = -b \mathbf{1} + ai + dk - cj,
\]

\[
 i (a \mathbf{1} + bi + cj + dk) = -b \mathbf{1} + ai - dk + ck,
\]

which means that if \( x = a \mathbf{1} + bi + cj + dk \) is in the center then \( c = 0 = d \). Checking commutativity with \( j \) gives \( b = 0 \).

6.3. Exercise (On PS 9). Let \( S = M_{n \times n}(F) \) where \( F \) is a field (e.g., \( F = \mathbb{R} \)). Then

\[
 \text{Center}(S) = \{ \lambda \mathbf{I} \mid \lambda \in F \},
\]

the set of diagonal matrices. Thus \( \text{Center}(S) \approx F \).
7. Homomorphisms and isomorphisms of rings

Let $R$ and $S$ be rings. A homomorphism $\phi: R \to S$ is a function such that

- $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$,
- $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$, and
- $\phi(1) = 1$.

Note: in groups we did not need a condition (3), because it was true anyway. This is because it was implied by the property that a homomorphism preserve products, which was because elements of groups always have inverses.

Easy fact: if $\phi$ is a homomorphism, then we also have:

$$\phi(0) = 0, \quad \phi(-a) = -\phi(a),$$

since $\phi$ is also a homomorphism of groups $(R, +) \to (S, +)$. We also have the following.

7.1. Proposition. If $a$ has a multiplicative inverse, then so does $\phi(a)$, with $\phi(a)^{-1} = \phi(a^{-1})$.

Proof. Just verify that $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1) = 1$ and $\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(1) = 1$.

7.2. Example. Let $R$ be a ring. There is a unique homomorphism of abelian groups $\phi: \mathbb{Z} \to R$ which sends the generator $1$ of $\mathbb{Z}$ to $1 \in R$. Thus, $\phi(0) = 0$ (since $0$s are identity elements for additive groups); we have $\phi(-1) = -1$ since homomorphisms take inverses to inverses; if $m > 0$, we have

$$\phi(m) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = m \cdot 1.$$  

Similarly, $\phi(-m) = -m \cdot 1$.

7.3. Remark. In practice, for any ring $S$ we usually just write the integer $m$ to also denote the element in $S$ given by $m1$ as above. This can be a little confusing. For instance, it is possible to have a non-zero integer $n$ whose image in $S$ is $0$.

7.4. Example. Consider the projection map $\phi: \mathbb{Z} \to \mathbb{Z}/n$, defined by $\phi(x) := [x]_n$. This is a ring homomorphism.

An isomorphism of rings is a homomorphism which is a bijection. You can show that the inverse map is also a bijection.

7.5. Proposition. If $\phi: R \to S$ is a homomorphism of rings, then $\phi(R)$ is a subring of $S$. If $\phi$ is injective then it defines an isomorphism between $R$ and $\phi(S)$.

8. Automorphisms of rings

An automorphism of a ring is an isomorphism $\phi: R \to R$ from the ring to itself. The set $\text{Aut}(R)$ of automorphisms is a group under composition.

Warning. This group of ring automorphisms of $R$ is not the same thing as the group of group automorphisms of $(R, +)$, even though we use the same notation for both. I may write $\text{Aut}_{\text{group}}$ and $\text{Aut}_{\text{ring}}$ to distinguish them.

8.1. Example. The complex-conjugation function $\phi: \mathbb{C} \to \mathbb{C}$ defined by $\phi(a + bi) = a - bi$ is an automorphism of $\mathbb{C}$. Note that $\phi\phi = \text{id}$, so that the subgroup $G = \langle \phi \rangle \leq \text{Aut}(\mathbb{C})$ has order 2 and acts on $\mathbb{C}$ through ring automorphisms.

(Note: confusingly, complex “conjugation” has nothing to do with the “conjugation” automorphism described below.)

8.2. Example. $\text{Aut}(\mathbb{Z}) \approx \{\text{id}\}$. To see this, note that by definition any homomorphism $\phi: \mathbb{Z} \to \mathbb{Z}$ must send $\phi(1) = 1$. But then $\phi(n) = \phi(1 + \cdots + 1) = \phi(1) + \cdots \phi(1) = n$ for $n > 0$. Also $\phi(-1) = -\phi(1) = -1$, so we can extend the result to show $\phi(n) = n$. 


8.3. Example. \( \text{Aut}(\mathbb{Q}) \approx \{ \text{id} \} \). Given \( \phi : \mathbb{Q} \to \mathbb{Q} \), the above argument shows \( \phi(n) = n \) for any integer \( n \). If \( r = ab^{-1} \in \mathbb{Q} \) with \( a, b \in \mathbb{Z} \) and \( b \neq 0 \), then \( a = rb \) so \( \phi(a) = \phi(r)\phi(b) \) which becomes \( a = \phi(r)b \), and thus \( \phi(r) = ab^{-1} = r \).

8.4. Example (Don’t need to know this, it’s just interesting). \( \text{Aut}(\mathbb{R}) \approx \{ \text{id} \} \). This uses the following properties of the real numbers:

1. In \( \mathbb{R} \), the non-negative numbers are exactly the ones which have a square root. Therefore, for \( a, b \in \mathbb{R} \), we have that
\[
a \leq b \quad \text{if and only if} \quad \text{exists } x \in \mathbb{R} \text{ such that } b - a = x^2.
\]

2. Every real number is determined by the rational numbers that are smaller than it. That is, for \( a \in \mathbb{R} \) let \( C_a = \{ q \in \mathbb{Q} \mid q \leq a \} \). Then \( a = b \) if and only if \( C_a = C_b \) are the same set.

Suppose \( \phi : \mathbb{R} \to \mathbb{R} \) is an automorphism.

- By the same proof as above, \( \phi(q) = q \) if \( q \in \mathbb{Q} \) is a rational number.
- If \( a \leq b \), then \( \phi(a) \leq \phi(b) \). The proof exactly uses (1): if \( a \leq b \), then exists \( x \) such that \( b - a = x^2 \). Then
\[
\phi(b) - \phi(a) = \phi(b-a) = \phi(x^2) = \phi(x)^2,
\]
so there exists \( x' = \phi(x) \) such that \( \phi(b) - \phi(a) = x'^2 \), i.e., \( \phi(a) \leq \phi(b) \).
- Therefore, \( C_{\phi(a)} = C_a \), since \( q \in \mathbb{Q} \) satisfies \( q \leq a \) if and only if \( q = \phi(q) \leq \phi(a) \). Hence from (2) we must have \( \phi(a) = a \).

8.5. Example. \( \text{Aut}(\mathbb{C}) \) is uncountably infinite. Most elements in this group (i.e., except identity and complex conjugation) can’t be written down explicitly: their construction relies on the Axiom of Choice.

Any unit \( u \in R^\times \) defines an automorphism \( \text{conj}_u : R \to R \) by \( \text{conj}_u(x) = uxu^{-1} \). Such automorphisms are called \textit{inner automorphisms} of the ring.

8.6. Example. \( \text{conj}_i : \mathbb{H} \to \mathbb{H} \) is given by \( \text{conj}_i(a1 + bi + cj + dk) = i(a1 + bi + cj + dk)(-i) = a1 + bi - cj - dk \) is an automorphism.

Note that \( \text{conj}_u \circ \text{conj}_v = \text{conj}_{uv} \). We get a homomorphism of groups
\[
\text{conj} : R^\times \to \text{Aut}(R), \quad u \mapsto \text{conj}_u.
\]

Exercise: \( \text{Ker(\text{conj})} = \text{Center}(R)^\times \), so we get an isomorphism from \( R^\times / \text{Center}(R)^\times \) to the subgroup of inner automorphisms inside \( \text{Aut}(R) \).

9. Polynomials as functions

Let \( S \) be a commutative ring. We have two new commutative rings:

- The ring \( S[X] \) of polynomials with coefficients in \( S \).
- The ring \( \mathcal{F}(S, S) \) of functions from \( S \) to \( S \), with pointwise addition and multiplication:
\[
(f + g)(s) := f(s) + g(s), \quad (fg)(s) := f(s)g(s).
\]

Define
\[
\psi : S[X] \to \mathcal{F}(S, S)
\]
by the rule
\[
\psi(p)(s) := \sum_{k=0}^{n} a_k s^k \quad \text{if } p = \sum_{k=0}^{n} a_k X^k.
\]
That is, \( \psi(p) \) is the function associated to the polynomial \( p \).

9.1. Proposition. \( \psi \) is a homomorphism of rings.
The homomorphism $\psi$ need not be injective.

9.2. Example. Let $S = \mathbb{Z}/p$ where $p$ is a prime number. Let $p = X^p - X$ in $S[X]$. Then I claim that $\psi(p) = 0$. This amounts to showing that $c^p - c = 0$ for all $c \in \mathbb{Z}/p$, which is Fermat’s little theorem.

Proof of Fermat’s little theorem: either $c = 0$ or $c \neq 0$. If $c = 0$ then obviously $0^p - 0 = 0$. If $c \neq 0$ then $c$ has a multiplicative inverse, i.e., is in the group $\Psi(p) = (\mathbb{Z}/p)^\times$. Since this group has order $p - 1$ we must have $c^{p-1} = 1$, and thus $c^p = c$.

Here’s another proof that $\psi$ is not injective: $\mathbb{Z}/p[X]$ is an infinite set (countably infinite), but $F(\mathbb{Z}/p, \mathbb{Z}/p)$ is a finite set (size $p^p$).

10. Universal property of $S[X]$

The following proposition tells you how to construct homomorphisms out of a polynomial ring $S[X]$. It is an example of what is called a “universal property” for $S[X]$.

10.1. Proposition. Let $S$ and $T$ be rings. Suppose given

1. a ring homomorphism $\phi: S \to T$, and
2. an element $c \in T$, such that
3. $\phi(s)c = c\phi(s)$ for all $s \in S$.

Then there exists a unique ring homomorphism $\psi_c: S[X] \to T$

such that (i) $\psi_c(X) = c$ and (ii) $\psi_c(s) = \phi(s)$ for all $s \in S$.

Note that if $T$ is commutative, then (3) is automatically true.

Proof. Existence. We define $\psi$ by the following rule. If $f \in S[X]$ is given by $f = \sum_{i=0}^n a_i X^i$ with $a_i \in S$, then set

$$\psi_c(f) := \sum_{i=0}^n \phi(a_i)c^i.$$ 

Verify directly that this is a ring homomorphism. (Exercise.) You will need to use the fact that the $\phi(a)_s$ commute with $c$, in order to show that multiplication is associative, as well as the distributive law.

Uniqueness. Conversely, given any $\psi: S[X] \to T$ satisfying the properties $\psi(a) = \phi(a)$ for $a \in S$ and $\psi(X) = c$, the properties of ring homomorphisms recover the formula:

$$\psi(\sum a_i X^i) = \sum \psi(a_i)X^i = \sum \psi(a_i)\psi(X)^i = \sum \phi(a_i)c^i.$$ 

10.2. Example. Fix a commutative ring $S$, and let $T = F(S, S)$, which is also commutative. Let $\phi: S \to T$ be the map that sends $a \in S$ to the constant function $(x \mapsto a)$. Let $c = \text{id}$, the identity function of $S$. Then the proposition gives a homomorphism $\psi: S[X] \to T$, which exactly sends a polynomial to its function.

10.3. Example. Let $F$ be a field, and let $S = M_{n \times n}(F)$. Fix a matrix $A \in S$. Let $\phi: F \to M_{n \times n}(F)$ be the homomorphism defined by $\phi(c) = cI$; note that the image of $\phi$ is in the center, and so every $\phi(c)$ commutes with $A$.

Then the proposition gives a homomorphism $\psi_A: F[X] \to S$, which sends

$$c_0 + c_1 X + \cdots + c_n X^n \mapsto c_0I + c_1A + c_2A^2 + \cdots + c_n A^n.$$ 

That is, we can “plug a matrix into a polynomial”.
10.4. **Example.** Let $S$ be a commutative ring (e.g., a field), and let $\phi: S \to S$ be the identity map. Then for any $c \in S$ we get a homomorphism $\epsilon_c: S[X] \to S$ defined by

$$\epsilon_c(\sum a_i X^i) := \sum a_i c^i.$$ 

This is the **evaluation at $c$ function**.

11. **Ideals**

An **ideal** of a ring $R$ is a subset $I \subseteq R$ such that

1. $I$ is a subgroup of $(R, +)$,
2. if $r, r' \in R$ and $x \in I$, then $r x r' \in I$. (You can write this condition as $R I R \subseteq I$.)

Note that an ideal, under our definition of ring, is not usually a subring. (This differs from books where rings are allowed to not have a multiplicative identity.)

Note that since $1 \in R$, the condition implies $r x, x r \in I$ if $x \in I, r \in R$.

**Warning.** The notion of ideal we have defined is sometimes called a **two-sided ideal**, to distinguish it from the notions of left-ideal and right-ideal.

11.1. **Example.** In any ring $R$, the subsets $R$ and $\{0\}$ are ideals of $R$.

11.2. **Example.** In $R = \mathbb{Z}$, the subsets $\mathbb{Z} n = \{ nx \mid x \in \mathbb{Z} \}$ are ideals for every $n$.

**Observation.** We can replace (1) with the weaker condition:

(1') if $x, y \in I$ then $x + y \in I$.

This is because $-1, 0 \in R$, so $x \in I$ and (2) implies $-x = (-1)x \in I$ and $0 = 0x \in I$.

The **kernel** of a ring homomorphism $\phi: R \to S$ is the set

$$\text{Ker} \phi := \{ r \in R \mid \phi(r) = 0 \}.$$ 

In other words, it is the same as the kernel of $\phi$ thought of as a homomorphism of abelian groups.

11.3. **Proposition.** The kernel $\text{Ker} \phi \subseteq R$ of a ring homomorphism $\phi: R \to S$ is an ideal of $R$.

**Proof.** Straightforward. □

This implies that a ring homomorphism $\phi$ is injective iff $\text{Ker} \phi = \{0\}$ (because $\phi$ is also a homomorphism of abelian groups).

12. **Ideals generated by subsets**

Let $R$ be a ring and $S \subseteq R$ a subset. The **ideal generated by** $S$ is

$$(S) := \bigcap_{S \subseteq J \subseteq R} J,$$

the intersection of all ideals of $R$ which contain the subset $S$. That this is an ideal is because of the following.

12.1. **Proposition.** If $\{J_i\}$ is any collection of ideals in $R$, then $J = \bigcap_i J_i$ is an ideal.

We also have an explicit description of $(S)$.

12.2. **Proposition.** We have that

$$(S) = \{0\} \cup \{ a_1 s_1 b_1 + \cdots + a_k s_k b_k \mid \text{for all } k \geq 1, a_i, b_i \in R, s_i \in S \}.$$
Proof. First check that the RHS is an ideal. Show (1’) it is closed under addition (immediate), and (2) if \( r, r’ \in R \) and \( x \in (S) \) then \( r x r’ \in S \): if \( x = a_1 s_1 b_1 + \cdots + a_k s_k r_k \) then
\[
x r x r’ = (r a_1) s_1 (b_1 r’) + \cdots + (r a_k) s_k (b_k r’).
\]
Second, show that if \( J \leq R \) is any ideal and \( S \subseteq J \), then the RHS above is a subset of \( J \). Also straightforward.

\[ \] \[ \]

**Note.** The ideal \((S)\) contains the subgroup \( \langle S \rangle \) of \((R,+)\) generated by \( S \), but is usually bigger than it.

When \( R \) is a **commutative** ring, this simplifies a bit.

12.3. **Proposition.** If \( R \) is commutative, then
\[
(S) = \{0\} \cup \{a_1 s_1 + \cdots + a_k s_k \mid \text{for all } k \geq 1, a_i \in R, s_i \in S\}.
\]

**Proof.** \( a s b = (a b)s \). \[ \]

A **principal ideal** is an ideal which can be generated by a single element. For \( x \in R \) we write \((x) := \{x\}\). Thus
\[
(x) = \{a_1 x b_1 + \cdots + a_n x b_n \mid a_i, b_i \in R\}.
\]
When \( R \) is **commutative**, we can always rearrange:
\[
a_1 x b_1 + \cdots + a_n x b_n = (a_1 b_1) x + \cdots + (a_n b_n) x = (a_1 b_1 + \cdots + a_n b_n) x.
\]
Thus, for commutative \( R \), principal ideals have the form
\[
(x) = R x = \{r x \mid r \in R\}.
\]

Sometimes I’ll write \( R x \) (or \( x R \)) for principal ideals in commutative rings.

We are going to say a lot about principal ideals in commutative rings. Here is an important fact: principal ideals in commutative rings correspond to elements “up to units”.

12.4. **Exercise** (On PS 9?). Let \( R \) be a commutative ring, and let \( a, b \in R \). Then \( (a) = (b) \) if and only if there exists a unit \( u \in R^\times \) such that \( b = u a, a = u^{-1} b. \)

13. **Simple rings**

A ring \( R \) is **simple**\(^\dagger\) if \( 1 \neq 0 \) and its only ideals are \( \{0\} \) and \( R \).

13.1. **Example.** Let \( D \) be a division ring. Then there are exactly two ideals, namely \( \{0\} \) and \( D \). To see this, suppose \( I \leq D \) is an ideal. Obviously \( 0 \in I \). If there is an \( a \in I \) with \( a \neq 0 \), then because \( D \) is a division ring \( a \) has a multiplicative inverse, so
\[
a^{-1} a = 1 \in I,
\]
which implies \( b = b 1 \in I \) for all \( b \in D \).

13.2. **Proposition.** A commutative ring is simple if and only if it is a field.

**Proof.** We know fields are simple. Suppose \( R \) is a simple commutative ring, so \( \{0\} \) and \( R \) are the only ideals. We show that any non-zero element of \( R \) has a multiplicative inverse.

Consider any non-zero \( a \in R \). Let \( I = (a) \) be the ideal generated by \( a \). Since \( I \neq \{0\} \) we must have \( I = R \). Because \( I \) is a principal ideal in a commutative ring, we have \( I = \{r a \mid r \in R\} \). Since \( 1 \in I \) there exists \( b \in R \) such that \( b a = 1 \), so \( a \) has a multiplicative inverse. \[ \]

This fails for non-commutative rings: a simple ring does not have to be a division ring.

\(^\dagger\) **Warning.** Many references also require simple rings to satisfy an additional condition, which is sometimes called “left Artinian”. If so, they might call my notion a quasi-simple ring. Don’t worry about this; we’ll just use the simple version of the definition of simple lol.
13.3. Example. Let $S = M_{n \times n}(F)$ for some field $F$. Then $S$ is a simple ring. But $S$ is not a division ring if $n \geq 2$.

Here is a sketch proof. Let $I \subseteq S$ be an ideal with a non-zero element $A \in I$. Since $A \neq 0$ it has a non-zero entry, say $a_{uv} \neq 0$. Write $E(i,j)$ for the “elementary matrix” (which has 1 in position $(i,j)$ and 0 for all other entries).

Now let $f \in S$. Suppose that $f$ is a non-zero entry, say $a_{uv} \neq 0$. Write $E(i,j)$ for the “elementary matrix” (which has 1 in position $(i,j)$ and 0 for all other entries).

Note that every matrix satisfies $B = \sum b_{ij}E(i,j)$. Thus, to show $I = S$ it suffices to show all $E(i,j) \in S$. To do this, check that

$$E(i,u)AE(u,j) = a_{uv}E(i,j),$$

and therefore $E(i,j) = a_{uv}^{-1}(a_{uv}E(i,j)) \in S$.

14. Ideals in Polynomial Rings

We recall some exercises from the homework. Let $R$ be a domain, and let $P = R[X]$ the polynomial ring. We defined the degree function

$$\deg: R[X] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$$

which had the properties

- $\deg(f) = -\infty$ if and only if $f = 0$.
- $\deg(f) = 1$ if and only if $f$ is non-zero and “constant”.
- $\deg(fg) = \deg(f) + \deg(g)$.
- $\deg(f + g) = \max\{\deg(f), \deg(g)\}$.

As a consequence, $R[X]$ is a domain: if $f \neq 0$ and $g \neq 0$, then $fg \neq 0$ since $\deg(fg) = \deg(f)\deg(g)$.

In the following, I’ll assume $R = F$ is a field. The following is a statement of “polynomial long division” for polynomials with coefficients in a field.

14.1. Proposition (Division algorithm for polynomials). Let $f, g \in F[X]$ with $g \neq 0$. Then there exists a unique pair $q, r \in F[X]$ such that

- $f = qg + r$ and
- $\deg(r) < \deg(g)$.

**Proof.** Existence. Suppose $\deg(g) = n \geq 0$.

In general, prove this by induction on $\deg(f) = m$: assume the proposition has been proved for $f$’s with degree $< m$.

- If $\deg(f) = -\infty$ then $f = 0$, so just take $q = r = 0$.
- If $\deg(f) < \deg(g)$, set $q = 0$ and $r = f$, so that

$$f = 0g + r.$$

Now suppose $\deg(f) \geq \deg(g)$. That is, $\deg(f) = m \geq n$. Write

$$f = a_mX^m + \cdots, \quad g = b_nX^n + \cdots, \quad a_m, b_n \in F \setminus \{0\},$$

and let

$$u = \frac{a_m}{b_n}X^m = a_m\frac{1}{b_n}X^{m-n},$$

(the fraction in quotes isn’t generally well-defined because $b_nX^n$ may not have a multiplicative inverse, but the expression of the right is defined since $b_n \neq 0$ and $m \geq n$). Thus

$$(b_nX^n)u = a_mX^m.$$

Now let $f' := f - gu$. Looking at the terms of highest degree ($= m$) we have

$$f' = f - gu = (a_mX^m + \cdots) - (b_nX^n + \cdots)(a_m\frac{1}{b_n}X^{m-n} + \cdots) = 0X^m + \text{(lower deg)}.$$
Therefore \( f' \) has degree strictly less than \( m \), so \( \deg(f') < \deg(f) \). By the induction on degree we know that there exist \( q' \) and \( r' \) such that

\[
f' = gq' + r', \quad \deg(r') < \deg(g).
\]

Then

\[
f = f' + gu = gq' + r' + gu = g(q' + u) + r'
\]

so \( q' + u \) and \( r' = r \) is a solution.

**Uniqueness.** If \( f = gq + r = gq' + r' \) with \( \deg(r), \deg(r') < \deg(g) \), then we can take the difference to get

\[
0 = f - f = (gq + r) - (gq' + r') = g(q - q') + (r - r'),
\]

i.e.,

\[
r' - r = g(q - q').
\]

Suppose \( q \neq q' \), we will derive a contradiction. Then \( q - q' \neq 0 \). But also \( g \neq 0 \), which implies the product is non-zero since \( F[X] \) is a domain. So all degrees are numbers, and we have the formula:

\[
\deg(r' - r) = \deg(g) + \deg(q - q').
\]

By hypothesis \( \deg(r), \deg(r') < \deg(g) \), which implies \( \deg(r' - r) < \deg(g) \), and so \( \deg(q - q') < 0 \) which is impossible. \( \square \)

A **monic polynomial** is a polynomial with coefficient of the leading degree term equal to 1. That is, \( f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \). Note that the zero polynomial cannot be a monic polynomial; however, the constant polynomial 1 is monic.

We can classify all ideals in \( F[X] \). The proof is very much like the classification of subgroups/ideals in \( \mathbb{Z} \).

**14.2. Proposition.** Let \( F \) be a field. Then all ideals in \( F[X] \) are principal. In particular, every ideal \( I \leq F[X] \) is of the form \( I = (f) = R[X]f \) for exactly one polynomial \( f \) which is either 0 or a monic polynomial.

**Proof.** The subset \( (0) = \{0\} \) is an ideal, and 0 is the only single element which generates it.

Suppose \( I \leq K[X] \) such that \( I \neq \{0\} \). Since \( I \) contains non-zero elements, it must contain a non-zero element \( f \) of minimal degree \( d \geq 0 \) (by the Well-Ordering Principle of \( \mathbb{Z}_{\geq 0} \)). We are going to show that every \( h \in I \) is of the form \( fq \) for some \( q \in F[X] \), i.e., that \( I = (f) \).

The proof is the division algorithm. Given \( h \in I \) consider the division algorithm for \( h \div f \): there exist \( q, r \in F[X] \) with \( \deg(r) < \deg(f) \) such that \( h = fq + r \). But by hypothesis \( \deg(f) \) is minimal for non-zero elements, so \( r = 0 \), so \( h = fq \in (f) \).

Given \( I = (f) \), write \( f = cX^d + (\text{lower degree}) \) with \( c \neq 0 \). Then \( f' = c^{-1}f \) is monic and \( I = (f) = (f') \). This is the only monic polynomial of degree \( d \) in \( I \), since if there are two such \( f', f'' \), then \( \deg(f' - f'') < d \) so \( f' = f'' \). \( \square \)

**15. Quotient rings**

Given an ideal \( I \) of a ring \( R \), there is a **quotient ring** \( R/I \). Elements of \( R/I \) are cosets

\[
a + I = \{a + x \mid x \in I\} \subset R
\]

of the additive group \((R, +)\) with respect to the subgroup \((I, +)\). Thus, it is automatic that \( R/I \) is an abelian group, with

\[
(a + I) + (b + I) = (a + b) + I.
\]

**Note.** Sometimes I will use the notation \( \overline{a} \in R/I \) for the coset \( a + I \).
15.1. **Proposition.** If \( I \subseteq R \) is an ideal, then \( R/I \) is a ring, with addition as above and multiplication defined by
\[
(a + I)(b + I) := ab + I.
\]
If \( R \) has multiplicative identity 1, then \( R/I \) has multiplicative identity \( 1 + I \).
Furthermore, the obvious projection map \( \pi: R \to R/I \) defined by \( \pi(a) := a + I \) is a ring homomorphism.

**Proof.** Check that the formula for product is well defined. Suppose \( a + I = a' + I \) and \( b + I = b' + I \), which implies
\[
a' = a + x, \quad b' = b + y, \quad x, y \in I.
\]
Then
\[
a'b' = (a + x)(b + y) = ab + (xy + xb + ay) \in ab + I,
\]
since \( ay + xb + xy \in I \). Therefore \( a'b' + I = ab + I \).
Checking the various axioms for \( R/I \) to be a ring is straightforward, using that they are true for \( R \). \[\square\]

15.2. **Example.** \( \mathbb{Z}/n = \mathbb{Z}/(n) \), the quotient of integers by the ideal \( (n) = \mathbb{Z}n \). We already know this is a quotient group (under addition. In fact, it is a quotient ring.

### 16. Quotient Rings of Polynomials

An important example are quotients of polynomial rings by principal ideals.

16.1. **Example.** Let \( S = \mathbb{Q}[X]/J \) where \( J = (f) = (X^2 - 2) \). Any element of \( S \) has the form
\[
g + J = a_0X^n + \cdots + a_1X + a_0 + J, \quad a_0, \ldots, a_n \in \mathbb{Q},
\]
but not uniquely. We can use the division algorithm to find a “canonical form”. For instance, doing
\[
(X^3 + 4X^2 + 5X - 3) \div f
\]
gives
\[
X^3 + 4X^2 + 5X - 3 = (X + 4)(X^2 - 2) + (7X + 5) = Xf + (7X + 5)
\]
so
\[
(X^3 - 2X^2 + 5X - 3) + J = (7X + 5) + J.
\]
Another way to think of this: we replaced every “\( X^2n \)” with “\( 2 \)”.

In general, every element of \( S \) is represented uniquely as
\[
a + bX + J, \quad a, b \in \mathbb{Q}.
\]
In particular, the set \( \{a + J \mid a \in \mathbb{Q}\} \) is a subring of \( S \) which is isomorphic to \( \mathbb{Q} \).

Addition of canonical forms gives a canonical form:
\[
((a + bX) + J) + ((a' + b'X) + J) = ((a + a') + (b + b')X) + J.
\]
Multiplication doesn’t automatically give a canonical form, so we have to work:
\[
((a + bX) + J)((a' + b'X) + J) = (a + bX)(a' + b'X) + J
= (aa' + (ab' + a'b)X + bb'X^2) + J
= (aa' + (ab' + a'b)X + bb'X^2 - bb'(X^2 - 2)) + J
= ((aa' + 2) + (ab' + a'b)X) + J.
\]
In practice we use the following notational tricks to deal with this:
- Given \( a \in \mathbb{Q} \), we use the same symbol “\( a \)” to represent the element \( a + J \in S \).
- We pick a symbol like \( X \) or \( \omega \) to represent the coset \( X + J \in S \).
- Then any element \( u \in S \) can be written uniquely as
\[
u = a + b\omega, \quad a, b \in \mathbb{Q}.
\]
• The symbol $\omega$ satisfies the “reduction rule” $\omega^2 = 2$. We use this rule whenever we need to put expressions in “canonical form”:

$$\omega^3 + 4\omega^2 + 5\omega - 3 = 2\omega + 4(2) + 5\omega - 3 = 7\omega + 5.$$ 

16.2. Example (Continued). Let $T \subseteq \mathbb{R}$ denote the following subset of $\mathbb{R}$:

$$T := \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}.$$ 

Exercise: $T$ is a subring of $\mathbb{R}$.

We can define a function $\phi: S \to T$ by

$$\phi(g + J) := g(\sqrt{2}).$$

That this is well defined relies on the following observation: if $g + J = g' + J$, then $g' = g + hf$, and therefore

$$g'(\sqrt{2}) = g(\sqrt{2}) + h(\sqrt{2})f(\sqrt{2}) = g(\sqrt{2}) + h(\sqrt{2})0 = g\sqrt{2},$$

since $\sqrt{2}$ is a root of the polynomial $f = X^2 - 2$.

As we will soon see, $\phi$ is an isomorphism of rings.

16.3. Example. Let $S = \mathbb{R}[X]/(X^2 + 1)$. If we define $i := X$, then $i^2 = -1$, and an element of $S$ has a unique representation $a + bi$ with $a, b \in \mathbb{R}$. Of course, $S \approx \mathbb{C}$.

16.4. Example. Let $S = \mathbb{Q}[X]/J$ with $J = (f) = (X^3 - 2)$. Write $\omega := [X] = X + J \in S$, and identify elements $a \in \mathbb{Q}$ with $a + J \in S$. Then every element of $S$ can be written uniquely as

$$a + b\omega + c\omega^2,$$

where we identify elements $c \in F$ with elements $c + J \in S$, and $X = X + J$.

You can carry out calculations using the “reduction” formula $\omega^3 = 2$.

Exercise: $S$ is a field. (This is not obvious, and we will return to this.)

Here is the general principle:

16.5. Proposition. Given $S = F[X]/J$ with $J = (f)$ for a monic polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, then every element of $S$ can be written uniquely as

$$c_0 + c_1X + \cdots + c_{n-1}X^{n-1},$$

where we identify elements $c \in F$ with elements $c + J \in S$, and $X = X + J$.

Furthermore, any expression $c_0 + c_1X + \cdots + c_mX^m$ can be reduced to a canonical form by repeated applications of replacing $X^n$ with $-(a_0 + a_1X + \cdots + a_{n-1}X^{n-1})$.

Proof. Division algorithm. The process for finding canonical forms for elements in $S$ is exactly the division algorithm in $R[X]$ for $\div f$. 

Department of Mathematics, University of Illinois, Urbana, IL

E-mail address: rezk@math.uiuc.edu