Rings and Factorization

In this section we study rings like $\mathbb{Z}$ and $F[x]$. In particular we wish to develop an understanding of the factorization of the elements. This will lead to the study of subsets of the multiples of a given element and to a generalization, called ideals.

It may be helpful to consult the section of the notes "Some Useful Definitions" for a perspective of how all of the definitions for group, field, ring, etc. are related to each other.

Definition 1. An *associative ring* R is a non-empty set, together with two operations called *addition* and *multiplication*, denoted by $+$ and $\cdot$, respectively, which satisfy the following axioms:

1. R is a abelian group with respect to $+$ with identity element 0.
2. multiplication $\cdot$ is associative,
3. the left and right distributive laws hold.

Furthermore, we require that R has an *identity* element 1 satisfying

$$1 \cdot x = x \cdot 1 = x$$

for all $x \in R$.

It is easy to check that for any ring, the following hold:

1. $0 \cdot r = r \cdot 0 = 0$ for all $r \in R$.
2. $(-1) \cdot r = r \cdot (-1) = -r$ for all $r \in R$.
3. $(-r)s = r(-s) = -(rs)$ for all $r, s \in R$.

E.g. for the first, compute $(0+0)r$ two different ways.

Note that it is no longer required that every non-zero element have a multiplicative inverse nor that multiplication be commutative.

Here are a number of examples of rings we've already seen. As is commonly done, we omit the term "formal" for rings of polynomials or power series (although that is what is meant).

Example 2. 1. Any field F, such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, etc.

2. The integers $\mathbb{Z}$.

3. Polynomials with coefficients in a field F, $F[x]$.

4. Polynomials in several variables with coefficients in a field F, $F[x_1, x_2, \ldots, x_m]$.

5. Polynomials with coefficents in a ring R, e.g., $\mathbb{Z}[x]$.

6. Square matrices over a field, $F^{n\times n}$, $n > 1$.

7. Square matrices over a ring, $R^{n\times n}$, $n > 1$.

8. All linear transformations from a vector space to itself, $\mathrm{Hom}_F(V, V)$.

9. Functions with values in a field, F^S, S a non-empty set.

10. Power series with coefficients in a field, $F[[x]]$.

11. The continuous real-valued functions on the closed interval $[0, 1]$, $\mathcal{C}([0, 1])$.

There are certain properties of rings which will be important to consider in our discussions.

Definition 3. A ring R is *commutative*, if $xy = yx$ for all $x, y \in R$.

Fields and $\mathbb{Z}$, as well as polynomial or power series rings over them, are commutative. However, matrix rings for $n > 1$ are not commutative, nor are rings such as $\mathrm{Hom}_F(V, V)$ if the vector space V has dimension greater than 1.

Definition 4. Non-zero elements a, b in a ring R are called *zero-divisors* if $ab = 0$. The ring R is a *domain* if it contains no zero-divisors.

Fields and $\mathbb{Z}$ are commutative domains, while F^S, for S a set with two or more elements, is commutative, but not a domain. $F^{n\times n}$ for $n > 1$ as well as $\mathrm{Hom}_F(V, V)$ for $\dim V > 1$ are both non-commutative and contain zero-divisors.

Definition 5. If R is a ring, a subset I of R is called an *ideal* of R if

1. I is an abelian group under $+$.

2. If $i \in I$ and $r \in R$, then both $ri \in I$ and $ir \in I$.

For rings with 1 it is easy to determine if a subset is an ideal:

Lemma 6. *If R is a ring, a subset I of R is an ideal if and only if it satisfies*

1. *I is non-empty,*

2. *if $a, b \in I$, then $a + b \in I$, and*

3. *if $a \in I$ and $r \in R$, then $ra, ar \in I$.*

See the section of the notes "Subobjects" for a discussion of similar ideas.

We will restrict our study of factorization in rings to the case of commutative rings, and so for the remainder of this section of the notes, all our rings will be commutative unless specified. Let $a \in R$. We define the *principal ideal* generated by a as the set of all multiples of a in R:

$$(a) = \{ sa \mid s \in R \}$$

Sometimes this ideal is also denoted by Ra.

We first consider very special rings for which we have additional information.

Definition 7. A ring R is called *euclidean* if it has the following properties:

1. R is a commutative domain,
2. There is a function $d : R \setminus 0 \longrightarrow \mathbb{Z}$ which takes on non-negative values and for every $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ with either $r = 0$ or $d(r) < d(b)$.

Example 8. 1. $\mathbb{Z}$ with the function $d(n) = |n|$.

2. For F a field, the ring $F[x]$ with $d(f) = \deg f$.

3. $\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \} \subseteq \mathbb{C}$ with $d(a + bi) = |a + bi|^2 = a^2 + b^2$.

4. $\mathbb{Z}[\sqrt{2}] = \left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Z} \right\} \subseteq \mathbb{R}$ with $d(a + b\sqrt{2}) = |a^2 - 2b^2|$.

Euclidean rings are just those for which there is a method of "long division" as one has for $\mathbb{Z}$ and polynomials $F[x]$. There are many other examples such as the last two listed here. However, we will mainly be interested in the first two. If you're interested to see why the last two are euclidean, see Exercises 6, 7, 8 and 9 at the end.

Theorem 9. *Every ideal in a euclidean ring is principal.*

Proof. If the ideal I of R contains only 0, then clearly $I = (0)$.

Hence we may now consider only ideals that contain non-zero elements. Consider the set of integers $S = \{ d(s) \mid s \in I,\ s \neq 0 \}$. As S is non-empty and only contains non-negative integers, it will contain a smallest element of the form $d(b) \geq 0$ for some $b \in I$. We will show that in fact $I = (b)$. Since $b \in I$ then $(b) \subseteq I$ as $rb \in I$ as I is an ideal. Consider now any $a \in I$. Applying the fact that R is a euclidean ring to the pair of elements a and $b \neq 0$, we see that there exist elements $q, r \in R$ such that $a = qb + r$ with either $r = 0$ or $d(r) < d(b)$.

Now $r = a - qb \in I$ and if $r \neq 0$, we have an element $d(r) \in S$ which is smaller than its smallest element $d(b)$. This is a contradiction, so it must be true that $r = 0$, that is that $0 = a - qb$ or $a = qb \in I$. That is, we've shown an arbitrary element of I must be a multiple of b. So $I \subseteq (b)$ and $I = (b)$. □

We now generalize our discussion slightly to cover those commutative domains all of whose ideals are principal.

Definition 10. A ring R is called a *principal ideal domain* if it is a commutative domain with all ideals principal. Such a ring will be referred to many times as simply a *PID*.

Our main result will be that all such rings will have "unique factorization", but we must first introduce the relevant terms to explain precisely what this means, and develop the notation and methods for dealing with factorization.

We start with some terms seen in earlier sections.

Definition 11. If R is a ring, an element with a two-sided multiplicative inverse will be called a *unit* of R and said to be *invertible*. The collection of all units of R forms a group, $U(R)$, called the *group of units* of R.

For example, $U(\mathbb{Z}) = \{\pm 1\}$, $U(F) = F^\times$ for F a field, and also $U(F[x]) = F^*$ as we will see below.

We use units to describe precisely the types of factorization that we are not interested in studying, trivial factorizations, those that are of no interest whatsoever. Given $r \in R$ and $u \in U(R)$ we can always factor r as $r = u \cdot (u^{-1}r)$. For $\mathbb{Z}$ this gives two uninteresting ways to factor a single element. In general rings will contain many units that lead to many uninteresting factorizations. The formal way to deal with this and which underlies all of our discussions of factorization is to consider equivalence classes of elements in the ring R given by multiplication by units – see problem EqRel 7 at the end of the section "Equivalence Relations". We will avoid this formality and simply say that we are considering factorization "up to units", and consider two factorizations to be the same if they only differ by some unit elements.

We informally introduced "multiple of" in our discussions above. We reverse the procedure now and define divisibility.

Definition 12. Let R be a commutative ring. A non-zero element $a \in R$ is said to *divide* an element $b \in R$ if there exists an element $c \in R$ with $b = ac$. We also say b is a *multiple* of a. This will be denoted by $a|b$.

Remark 13. Note that $a \neq 0$. We will *never* write $0|b$. If we write $a|b$, it *always* implies that $a \neq 0$.

As 0 could only divide 0 anyway, we are really only excluding one possible statement. Further, if we were to allow this meaning, many statements we wish to make below, would get more complicated and require an extra case to even state.

Divisibility is easily seen to have the following properties:

Lemma 14. *Let R be a commutative ring. Then the following hold for elements of R:*

1. *If $a|b$, then $a|rb$ for any $r \in R$.*
2. *If $a|b_1$ and $a|b_2$, then $a|b_1 + b_2$ and for any $r_1, r_2 \in R$, then $a|r_1b_1 + r_2b_2$.*

3. If $a|b$ and $b|c$, then $a|c$.

We next introduce the ultimate elements in a factorization, the "atoms", the indivisible ones which can be broken down no further and at the same time introduce those with a special property.

Definition 15. Let R be a commutative ring. An element $q \in R$ is called *irreducible* if

1. $q \neq 0$ and q is not a unit,
2. if $q = ab$, then either a or b is a unit.

Let R be a commutative ring. An element $p \in R$ is called *prime* if

1. $p \neq 0$ and p is not a unit,
2. if $p|ab$, then either $p|a$ or $p|b$.

Remark 16. If R is a domain, then a prime is always irreducible.

For if $p = ab$ and $p|a$ we have $a = cp$ for some c. So $p = cpb$, $p(1 - cb) = 0$ and as R is a domain, we have $1 = cb$, that is, b is a unit. A similar argument works in case $p|b$ to show that a is a unit.

In general the two concepts are different even in domains. See Exercise 5 for a simple example where they are different.

Definition 17. Let R be a commutative ring and $a, b \in R$. An element $d \in R$ is a *greatest common divisor* of a and b if

1. $d \neq 0$,
2. $d|a$ and $d|b$,
3. if $d'|a$ and $d'|b$, then $d'|d$.

Let R be a commutative ring and $a, b \in R$. An element $m \in R$ is a *least common multiple* of a and b if

1. $m \neq 0$,
2. $a|m$ and $b|m$,
3. if $a|m'$ and $b|m'$, then $m|m'$.

Remark 18. 1. We will commonly refer to a "greatest common divisor" as simply a "gcd". Similarly, "lcm" will be a short version of "least common multiple".

2. As we never allow a 0 on the left in a statement $a|m$, the second definition requires that both a and b be non-zero. This is not the case in the first definition.

3. Keep in mind that these are definitions. In a given situation in a given ring, it may or may not be true that such elements d or m even exist.

4. If R is a domain, and if a gcd exists, then it is unique up to units. Such an element will be denoted by (a, b).

   If d and d' both satisfy the conditions to be a gcd for a and b, then as $d'|a$, $d'|b$, we must have $d'|d$. Switching the roles of the two in this argument, gives $d|d'$. So $d = c_1 d'$ and $d' = c_2 d$ for some $c_1, c_2 \in R$. Thus $d = c_1 c_2 d$ and as $d \neq 0$ we have $1 = c_1 c_2$, so the c_i are units.

5. If R is a domain, and if an lcm exists, then it is unique up to units by an argument similar to the preceding one. Such an element will be denoted by $[a, b]$.

Lemma 19. *Let R be a PID and $a, b \in R$.*

1. *If a and b are not both 0, then a gcd d exists and is unique up to units. Further, there exist $r, s \in R$ such that $d = ra + sb$.*

2. *If neither a nor b is 0, then an lcm exists and is unique up to units.*

3. *If neither a nor b is 0, then*

$$ab = (a, b)[a, b]$$

   up to units.

Remark 20. For R a ring containing ideals I and J, it is easy to see that the set

$$I + J = \{\, i + j \mid i \in I,\ j \in J \,\}$$

is an ideal of R. Similarly the set $I \cap J$ is an ideal in R.

The set IJ is defined to be the smallest ideal containing all of the products ij for $i \in I$ and $j \in J$ (that is, the intersection of all ideals containing this set of products). It is clearly an ideal, and moreover is easily seen to be the set of all finite sums $\sum_{s=1}^{n} i_s j_s$, $i_s \in I$ and $j_s \in J$.

Proof. Since R is a PID the ideal $(a) + (b)$ is principal, so there exists a $d \in R$ with $(a) + (b) = (d)$. Hence by the definition of principal ideal and sum of ideals, there exist $r, s \in R$ with $d = ra + sb$. Now

- $d \neq 0$ as at least one of a and b is not 0,
- $(d) \supseteq (a)$ implies that $d|a$
  $(d) \supseteq (b)$ implies that $d|b$,
- if $d'|a$ and $d'|b$, then $d'|ra + sb = d$.

Since R is a PID the ideal $(a) \cap (b)$ is principal, so there exists an $m \in R$ with $(a) \cap (b) = (m)$. Now

- $m \neq 0$ as $ab \in (a) \cap (b)$, and $ab \neq 0$ since R is a domain and neither a nor b is 0,
- $(m) \subseteq (a)$ implies that $a|m$
  $(m) \subseteq (b)$ implies that $b|m$,
- if $a|m'$ and $b|m'$, then $m' \in (a) \cap (b) = (m)$, so $m|m'$.

You should check the last one. Show

$$((a) + (b))((a) \cap (b)) = (d)(m) = (a)(b)$$

directly. □

Remark 21. We'll give a different proof of the third part of this lemma once we've proved the existence of unique factorizations into primes for a PID.

For elements a, b in a PID we say that they are *relatively prime* if $(a, b) = 1$ (that is, the gcd is a unit).

Lemma 22. *Let R be a PID with $a, b \in R$. If $(a, b) = 1$ and $a|bc$, then $a|c$.*

Proof. As $(a, b) = 1$ there exist $r, s \in R$ with $ra + sb = 1$. Multiplying this equation by c yields, $rac + sbc = c$. Now a divides the left term and a divides the right term since it divides bc. Hence a divides the sum, which is c. □

Lemma 23. *Let R be a PID with $a, b \in R$. If $(a, b) = 1$, $a|c$ and $b|c$, then $ab|c$.*

Proof. As in the previous proof, write $ra + sb = 1$ and multiply the equation by c yieldig $rac + sbc = c$. Now ab divides the first term as a appears and $b|c$. Similarly ab divides the second term as b appears and a divides c. Hence ab divides their sum which is c. □

Lemma 24. *Let R be a PID. If p is irreducible, then p is a prime. Hence, prime and irreducible are the same in a PID.*

Proof. Given $p|ab$ consider (a, p). The latter is a divisor of p so must be 1 or p (up to units) since p is irreducible. If $(a, p) = p$, then $p|a$. On the other hand, if $(a, p) = 1$, then by Lemma 22, $p|b$.

As we already observed in Remark 16 that any prime is irreducible in a domain we now conclude that in a PID the two concepts are identical. □

Corollary 25. *Let R be a PID with $p, a_1, \ldots, a_n \in R$. If p is irreducible (prime) and $p|a_1 \cdots a_n$, then $p|a_i$ for some i.*

Proof. Because irreducible and prime are the same, this follows from a simple induction argument with the cases $n = 1$ trivial and $n = 2$ the definition of prime. □

In many of the standard proofs of the uniqueness of factorization for the euclidean rings $\mathbb{Z}$ or $F[x]$, arguments (mathematical induction) are given which use the "size" of the elements (i.e., the integer $d(r)$). Typical arguments are of the form: "If $a = bc$ and neither b nor c is a unit, then the size of each of b and c is smaller than that of a. Hence it is not possible to factor a into an arbitrarily large number of smaller pieces none of which are units." For the general PID this notion of "size" is not available, but there is a convenient replacement for the way "size" is used. The definition we make below may sound exotic, but that the condition holds for any PID is almost trivial. The way it will be used is just as described above: to force possible infinite processes to actually stop in a finite number of steps.

Definition 26. Let R be a ring containing ideals $\{ I_i \mid i = 1, 2, \ldots, j, \ldots \}$ such that

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_j \subseteq \cdots$$

Such a collection of ideals is called an *ascending chain* of ideals.

R is said to satisfy the *ascending chain condition* if there exists an integer N so that $I_j = I_N$ for all $j \geq N$. We'll abbreviate this as simply the *ACC*. This condition is also sometimes referred to by saying that R is *noetherian*.

Lemma 27. *A PID satisfies the ascending chain condition.*

Proof. Let $\{ I_i \mid 1 \leq i \}$ be an ascending chain of ideals and define $I = \bigcup_{1 \leq i} I_i$ to be their union. Note the following

- $0 \in I$ as $0 \in I_1$ so I is non-empty.
- if $a, b \in I$, then $a \in I_k$ for some k and $b \in I_\ell$ for some ℓ; let $m = \max\{ k, \ell \}$, then both are in I_m and thus $a + b \in I_m \subseteq I$,
- if $a \in I$, then $a \in I_k$ for some k, so for $r \in R$, $ra \in I_k \subseteq I$.

Hence I is an ideal of R and as R is a PID, $I = (b)$ for some $b \in R$. Again as I is the union of all I_j, there is some N so that $b \in I_N$. Hence for $j \geq N$ we have

$$I = (b) \subseteq I_N \subseteq I_j \subseteq I$$

thus proving that all of these ideals are equal starting at N, as required for the ACC. □

Definition 28. A ring R will be called a *unique factorization domain* if it is a commutative domain such that:

> Every non-zero, non-unit of R is a product of a finite number of irreducible elements.

If r is a non-zero, non-unit of R with

$$\begin{aligned} r &= up_1 \cdots p_n \\ &= vq_1 \cdots q_m \end{aligned}$$

for some units u, v and irreducibles p_i, q_j then

(1) $n = m$,

(2) There exists a one-to-one, onto function $\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ and units u_i such that

$$q_{\sigma(i)} = u_i p_i$$

for $i \in \{1, \ldots, n\}$.

We will abreviate this by saying that R is a *UFD*.

Informally we will say that "every non-zero, non-unit of R is a product of irreducibles with the product being unique up to order and multiplication by units". Our goal now is to prove that every PID is a UFD. The proof of the uniqueness of factorization will look very much like a proof for $\mathbb{Z}$ or $F[x]$ that you may have already seen. The existence part will probably be different as we use the ACC to replace arguments that usually use an induction on the "size" of elements.

Theorem 29. *Every principal ideal domain is a unique factorization domain.*

This has as an immediate consequence a standard result.

Corollary 30. *$\mathbb{Z}$ and $F[x]$ have unique factorization into primes.*

Proof. **Existence of factorization:**
We break this part down into two steps, each of which will use the ACC in essentially the same way. First note that for non-zero elements $s, t \in R$, $(s) \subseteq (r)$ just means $r|s$ and as R is a domain, $(s) = (r)$ means there exist units $u, v \in R$ with $s = ur$ and $r = vs$.

Step 1:
Every non-zero, non-unit r has an irreducible factor.

If r is irreducible, then we are done. If r is not irreducible, then $r = a_1 b_1$ with neither a_1 nor b_1 units. If a_1 is irreducible, we are done. If not $a_1 = a_2 b_2$ with neither units. Apply the same argument to a_2. If we never obtain an irreducible by this process, we have found an infinite strictly ascending chain of ideals

$$(r) \subset (a_1) \subset (a_2) \subset \cdots (a_j) \cdots$$

There are no equalities as the b_i are all non-units. This, however, contradicts the ACC for a PID. Thus any such process must terminate after a finite number of steps at which point it produces an irreducible factor of r.

Step 2:
Every non-zero, non-unit r is a product of a finite number of irreducibles.

If r is irreducible, we are done. If not, write $r = q_1 a_1$ with q_1 irreducible and a_1 not a unit. If a_1 is irreducible, we are done. If not, write $a_1 = q_2 a_2$ with q_2 irreducible and a_2 not a unit. If this process never terminates, then we have found a strictly ascending chain of ideals

$$(r) \subset (a_1) \subset (a_2) \subset \cdots$$

There are no equalities since the q_i are not units. Again we have a contradiction to the ACC and conclude that the process must indeed terminate. That is, it results in a factorization of r into a finite product of irreducible elements.

Uniqueness of factorization:
Assume we have

$$\begin{aligned} r &= up_1 \cdots p_n \\ &= vq_1 \cdots q_m \end{aligned}$$

for some units u, v and irreducibles p_i, q_j. We assume $n \leq m$. The proof will be by induction on n.

In case $n = 1$ and $m > 1$ this can be simplified to $p_1 = q \cdot q_m$ for $q = u^{-1} v q_1 \cdots q_{m-1}$. q is not a unit since q_1 is not a unit. This equation violates the fact that p_1 is irreducible. Hence it must be that $m = n = 1$. The sought-after function σ is the identity and the required unit is $u_1 = v^{-1} u$.

Assume the result holds for integers smaller than n and that $n > 1$. Since p_n is prime and divides r it must divide some q_j. That is, there is a unit u_n so that $q_j = u_n p_n$. Replacing q_j in the right-hand side of the equation

$$up_1 \cdots p_n = vq_1 \cdots q_m$$

and factoring out the p_n (that's valid as R is a domain) leaves

$$up_1 \cdots p_{n-1} = (u_n v) q_1 \cdots q_{j-1} q_{j+1} \cdots q_m \ .$$

Counting the number of irreducibles remaining gives

$$n - 1 \leq m - 1$$

and by induction we must have $n - 1 = m - 1$ or $n = m$.

Induction also gives a collection of units $\{ u_1, \ldots, u_{n-1} \}$ and a one-to-one correspondence τ between the sets $\{ 1, \ldots, n-1 \}$ and $\{ 1, \ldots, j-1, j+1, \ldots, n \}$ so that $q_{\tau(i)} = u_i p_i$. The function τ together with $q_j = u_n p_n$ allow one to define the required function σ:

$$\sigma(i) = \begin{cases} \tau(i) & \text{for } 1 \leq i \leq n-1 \\ j & \text{for } i = n \ . \end{cases}$$

□

Remark 31. In any UFD, so in particular for any PID, there is a common method for writing the factorization of any non-zero element r: One collects together all copies of the same irreducible at the cost of generating some units which one collects together yielding

$$r = up_1^{n_1} \cdots p_k^{n_k}$$

where u is a unit, the p_i are distinct irreducibles (none is a unit times any other) and the $n_i \geq 1$. For some special rings there are even standard choices for representatives of the primes. There are a number of standard consequences of these observations.

1. For $\mathbb{Z}$ one usually adds the extra condition that a prime p is positive. Factorizations then take the form
$$n = \pm 1 \cdot p_1^{n_1} \cdots p_k^{n_k}$$
(so $u = \pm 1$).

2. For $F[x]$ one usually adds the extra condition that a prime p is monic (leading coefficient 1). Factorizations then take the form
$$f = up_1^{n_1} \cdots p_k^{n_k} \ .$$

3. **Formula for the gcd**
If $a, b \in R$, not both 0, for R a UFD, then $(a, b) = 0$ if either $a = 0$ or $b = 0$. We now consider only the case where both are non-zero. We factor each as remarked above, but relabel the primes so that there is one common set of subscripts. The cost we must pay for this is that we must then allow that an exponent n_i be 0 is that particular prime does not appear in the factorization. We now write
$$a = up_1^{n_1} \cdots p_k^{n_k}$$
$$b = vp_1^{m_1} \cdots p_k^{m_k}$$
where u, v are units, $n_i, m_i \geq 0$, and the p_i are distinct primes. We then have the formula
$$(a, b) = p_1^{\min(n_1, m_1)} \cdots p_k^{\min(n_k, m_k)}$$
which is easy to check.

4. **Formula for the lcm**
Continuing with the same notation when both a and b are non-zero we have the formula
$$[a, b] = p_1^{\max(n_1, m_1)} \cdots p_k^{\max(n_k, m_k)}$$
which is also easy to check.

5. Using these two formulas one obtains the equation
$$(a, b)[a, b] = ab$$
up to units upon verifying the simple observation
$$\min(x, y) + \max(x, y) = x + y$$
which holds for any two integers (even real numbers) x, y.

Theorem 32 (Characterization of Unique Factorization Domains)**.** *Let R be a commutative domain. Then R is a UFD if and only if R satisfies*

1. *every irreducible in R is prime, and*

2. *the ascending chain condition on principal ideals.*

Proof. See Exercise 13 for an outline of the proof. □

Remark 33. If R is a UFD, then $R[x]$ is also a UFD. We do not need that result in this course nor do we have the means to prove it with what we've done thus far. See Exercises 13, 14, 15, and 16 for a development of the necessary ideas.

Polynomials

Let R be a ring. The ring $R[x]$ can be thought of (as in the case of fields) as the set of formal expressions $f = a_0 + a_1x + \cdots a_nx^n$ which are considered to be different precisely when there exists a non-negative integer i such that the coefficients of x^i in the two expressions are not equal (any term that does not appear is considered to be 0). (We'll give a formal description a little later when we discuss free modules – then we'll say that the set $\{1, x, x^2, \ldots, x^i, \ldots\}$ is a basis for the free module.) Addition and multiplication are defined in the same way as for fields. Note that in particular $rx = xr$ for any $r \in R$.

A polynomial $f \in R[x]$ described as above is said to have *degree* n if $a_n \neq 0$. We abbreviate this as $\deg f = n$. We do not define the degree of the 0 polynomial. In the following formulas it is always assumed that if a term $\deg h$ appears, then h is not 0. For any ring R it is easy to verify the following:

$$\begin{aligned} \deg(f+g) &\leq \max(\deg f, \deg g) \\ \deg(fg) &\leq \deg f + \deg g \ . \end{aligned}$$

In fact if $\deg f \neq \deg g$ one has

$$\deg(f+g) = \max(\deg f, \deg g) \ .$$

If R is a domain. then one has

$$\deg(fg) = \deg f + \deg g \ .$$

In case R is a field, then one can easily give an induction argument to show that $F[x]$ is a euclidean ring. More generally, it always possible to carry out such a "long division with remainder" in case the second polynomial has leading coefficient a unit (see Exercise 2).

Polynomials as Functions

For F be a field consider the ring F^F, the collection of all functions from F to F where functions are added and multiplied by using their values. For a given $a \in F$ there is a linear transformation

$$E_a : F[x] \longrightarrow F$$

given by $E_a(f) = f(a)$, that is, on a basis E_a sends x^i to a^i. This then gives a function

$$E : F[x] \longrightarrow F^F$$

given by $E(f)(a) = E_a(f)$. To rephrase, evaluation associates to each polynomial a function in F^F, which of course is computed in the usual way. Now E_a is in fact not only a linear transformation

$$\begin{aligned} E_a(f+g) &= E_a(f) + E_a(g) \\ E_a(cf) &= cE_a(f) \end{aligned}$$

for $f, g \in F[x]$, $c \in F$, but it is also a ring homomorphism

$$E_a(fg) = E_a(f)E_a(g)$$

which follows easily. Indeed, since E_a is a linear transformation we need only check what happens on basis elements:

$$\begin{aligned} E_a(x^i \cdot x^j) &= E_a(x^{i+j}) \\ &= a^{i+j} \\ E_a(x^i)E_a(x^j) &= a^i \cdot a^j \ . \end{aligned}$$

This now implies that the function E is not only a linear transforation but also a ring homomorphism, that is, both $F[x]$ and F^F are F-algebras and E is an F-algebra homomorphism. (To put this in context, see the section "Some Useful Definitions".)

It is easy to see that in general (formal) polynomials and functions are not the same thing, that is, they are not isomorphic rings. For example, if $F = \mathbb{F}_2$ is the field with two elements, then there are only $4 = 2^2$ functions from $\mathbb{F}_2$ to $\mathbb{F}_2$. However there are an infinite number of distinct polynomials. Note that the polynomials $\{ x, x^2, x^3, \dots \}$ all give the same function when evaluated at the two elements of $\mathbb{F}_2 = \{ 0, 1 \}$. In Exercise 22 you will show that

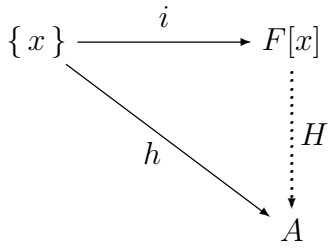
(1) E is one-to-one if and only if F is an infinite field, and

(2) E is onto if and only if F is a finite field,

So in particular, if F is infinite, not all functions are polynomial, and if F is finite, all functions are given by polynomials (each in an infinite number of different ways).

Evaluation for the F-algebra $F[x]$ is universal in a certain sense (see the section "Universal Mapping Properties").

Theorem 34 (UMP for $F[x]$)**.** *Let A be any (not necessarily commutative) F-algebra. Then for any function $h : \{x\} \longrightarrow A$ (i.e., for any $a \in A$ with $h(x) = a$). there exists a unique homomorphism H of F-algebras such that the following diagram commutes:*



that is, $H \circ i = h$ (or $H(x) = a$).

That is, $\{x\}$ plays the role of a one-element basis in the context ("category") of F-algebras. The universal mapping property provides a bijection

$$\mathrm{Hom}_{\mathbf{Set}}(\{x\}, A) \longleftrightarrow \mathrm{Hom}_{\mathbf{F-Alg}}(F[x], A) \ .$$

Polynomials in n-variables over a field, $F[x_1, \ldots, x_n]$, have a similar universal mapping propery given by evaluating at n elements of a *commutative* F-algebra A.

Polynomials in Linear Algebra

A number of ideas discussed above will play a special role in linear algebra.

Suppose A is a (not necessarily commutative) F-algebra and $a \in A$. Now E_a, evaluation at a, gives an F-algebra homomorphism $E_a : F[x] \longrightarrow A$. Let $\ker E_a \subseteq F[x]$ be the usual kernel of E_a. So $\ker E_a$ is a subspace of $F[x]$. Because E_a has the extra property that it is a ring homomorphism, it follows that $\ker E_a$ is an ideal of $F[x]$: as

$$E_a(fg) = E_a(f)E_a(g)$$

it follows that if $E_a(g) = g(a) = 0$ ($g \in \ker E_a$, then also $fg \in \ker E_a$ for all $f \in F[x]$.

Thus as $F[x]$ is a PID, there exists an element $h \in F[x]$ with $\ker E_a = (h)$. If $\ker E_a$ is not 0, we may choose a unique monic polynomial for h with $\ker E_a = (h)$. Such a polynomial h is called the *minimal* polynomial of $a \in A$.

In case A has finite dimension over F, then $\ker E_a$ is never 0 and hence a non-zero minimal polynomial h will exist. For suppose $\dim_F A = n < \infty$. Then $\{1, a, a^2, \ldots, a^n\} \subseteq A$ will be a subset containing $n+1$ elements so it is dependent and thus there will be a non-trivial linear combination of these elements which is 0 (i.e., a non-zero polynomial in a which is 0).

For example, if $M \in F^{m \times m}$ is an $m \times m$ polynomial, this argument says that it has a unique non-zero minimal polynomial. Similarly, if V is a finite-dimensional vector space over F and $T \in \mathrm{Hom}_F(V, V)$ is a linear transformation, then T has a unique non-zero minimal polynomial.

There will be many other places we will use the fact that $F[x]$ is a PID. See the section "The Structure of Modules over a PID" and its application to the construction of canonical forms for matrices.

How F Affects $F[x]$

The elements of F clearly affect the factorization of elements in $F[x]$. That is, if F is very "large" in a certain sense, then many factorizations are possible. We begin by considering the ultimate case.

If $F \subseteq K$ are fields, an element $a \in K$ is said to be a *root* of a non-constant polynomial $f \in F[x]$ if f evaluated at a is zero: $f(a) = 0$.

Definition 35. A field F is called *algebraically closed* if it satisfies any of the following three equivalent conditions:

(1) Every non-constant $f \in F[x]$ has a root in F.

(2) Every non-constant polynomial $f \in F[x]$ is a product of polynomials of degree 1.

(3) Every irreducible polynomial in $F[x]$ has degree 1.

It is easy to verify that these three conditions are equivalent (see Exercise 23).

Theorem 36 (Fundamental Theorem of Algebra)**.** *The field $\mathbb{C} = \mathbb{R}[i]$ is algebraically closed.*

This theorem is really a theorem from analysis, not algebra, as proofs require the fundamental properties of the real numbers. There are many proofs of this theorem with one of the simplest using algebra to reduce to the case of odd degree polynomials with real coefficients. For such polynomials the Intermediate Value Theorem asserts that they have real roots.

Corollary 37. *Every non-constant polynomial in $\mathbb{R}[x]$ is a product of linear and quadratic polynomials. Equivalently, every irreducible polynomial in $\mathbb{R}[x]$ has degree 1 or 2.*

Proof. Consider non-constant $f \in \mathbb{R}[x]$ of degree n. We may as well assume that f is monic. As $\mathbb{R} \subset \mathbb{C}$, we have $\mathbb{R}[x] \subset \mathbb{C}[x]$ and in $\mathbb{C}[x]$ we can factor f as

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$$

for some $a_i \in \mathbb{C}$.

Ordinary complex conjugation $^- : \mathbb{C} \longrightarrow \mathbb{C}$ (an isomorphism of fields) induces an isomorphism of rings

$$^- : \mathbb{C}[x] \longrightarrow \mathbb{C}[x]$$

by defining $\overline{h} = \overline{b_0} + \overline{b_1}x + \cdots + \overline{b_k}x^k$ for $h = b_0 + b_1 x + \cdots + b_k x^k \in \mathbb{C}[x]$. You should verify the details (see Exercise 24).

Note that $z \in \mathbb{C}$ actually lies in $\mathbb{R}$ if and only of $\overline{z} = z$. For our polynomial $f \in \mathbb{R}[x]$ we then have that $\overline{f} = f$. We now break the set of roots (in $\mathbb{C}$) of f into two collections: Those that are in $\mathbb{R}$ and those that are not. Now as $f = \overline{f}$ it follows that for the roots a_k of f that are not in $\mathbb{R}$, then $\overline{a_k}$ must also be a root of f (using the fact that $^-$ is a ring isomorphism):

$$\begin{aligned} 0 &= f(a_k) \\ &= \overline{f(a_k)} \\ &= \overline{f}(\overline{a_k}) \\ &= f(\overline{a_k}) \ . \end{aligned}$$

We then have a factorization of f as follows

$$f = \prod_{a_k \in \mathbb{R}} (x - a_k) \prod_{a_k \notin \mathbb{R}} (x - a_k)$$

with the second set of factors appearing in pairs: $(x - a_k)(x - \overline{a}_k)$ for $a_k \notin \mathbb{R}$. Each of these products equals $x^2 - (a_k + \overline{a}_k)x + a_k\overline{a}_k$. All of the coefficients are then real numbers, for given any $a \in \mathbb{C}$ both $a + \overline{a} \in \mathbb{R}$ and $a\overline{a} \in \mathbb{R}$ hold. We have thus factored f completely as a product of polynomials of degrees 1 and 2. $\square$

Exercises

Ring 1. Let $S \subseteq \mathbb{Z}$ be a non-empty set of non-negative integers.

(1) Use mathematical induction to prove that S contains a smallest integer.

(2) Assume that every such non-empty subset S of non-negative integers contains a smallest element. Prove that mathematical induction is valid.

Ring 2. Let R be a commutative ring with 1. Let $g, f \in R[x]$ with g monic (leading coefficient 1; any unit would do as well). Show that there exist $q, r \in R[x]$ so that $f = qg + r$ with either $r = 0$ or $\deg(r) < \deg(g)$. Show that both q and r are unique.

Ring 3. Verify the assertions in Remark 20.

Ring 4. Verify the formula $(a, b)[a, b] = ab$ (up to units) for a, b non-zero elements of a PID using the outline given in the third part of Lemma 19: Show

$$((a) + (b))\,((a) \cap (b)) = (d)(m) = (a)(b)$$

directly.

Ring 5. Let $R = \mathbb{Z}[\sqrt{-5}] = \left\{ a + b\sqrt{-5} \;\middle|\; a, b \in \mathbb{Z} \right\} \subseteq \mathbb{C}$. Define $d : R \longrightarrow \mathbb{Z}$ by $d(a + b\sqrt{-5}) = |a + b\sqrt{-5}|^2 = a^2 + 5b^2$, Note that $d(xy) = d(x)d(y)$. Consider $3 \cdot 3 = 9 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$.

a. Determine all of the units of R. [Hint: If $xy = 1$, then ...]

b. Show that each of 3, $2 + \sqrt{-5}$ and $2 - \sqrt{-5}$ is irreducible. [Hint: If $xy = 3$, then ...]

c. Show that the three irreducibles given above are distinct (i.e., none is a unit times another).

d. Conclude that prime and irreducible do not mean the same thing in R. Hence R is not euclidean with respect to any function, R is not a PID, and R is not a UFD.

Ring 6. Let R be a commutative domain with field of fractions F. Assume there exists a function

$$N : R \longrightarrow \mathbb{Z}$$

satisfying

1. $N(ab) = N(a)N(b)$ for $a, b \in R$, and

2. $N(a) \geq 0$ for all $a \in R$ with $N(a) = 0$ if and only if $a = 0$.

Show that N can be extended to a function

$$N : F \longrightarrow \mathbb{Q}$$

by defining $N(\frac{a}{b}) = \frac{N(a)}{N(b)}$ for $b \neq 0$ and that this function also satisfies the two properties. [Why is the extended N well-defined?]

Prove that R is euclidean with respect to the function N if and only if for every $x \in F$ there exists $q \in R$ such that $N(x - q) < 1$. [Hint: Try $x = a/b$ for one direction.]

Ring 7. Let $\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \} \subseteq \mathbb{C}$. Define $d : \mathbb{Z}[i] \longrightarrow \mathbb{Z}$ by $d(a + bi) = |a + bi|^2 = a^2 + b^2$. Note that d is a multiplicative function that is the restriction of the function on $\mathbb{Q}[i]$ which has values in $\mathbb{Q}$. Show that $\mathbb{Z}[i]$ being euclidean with respect to this function will follow from the fact that the plane $\mathbb{R}^2$ (thought of as the complex numbers the usual way $(a, b) \leftrightarrow a + bi$) is covered by the interiors of all the circles of radius 1 centered at integral lattice points in the plane (i.e., the centers are (m, n) for $m, n \in \mathbb{Z}$). Verify that this geometric statement is in fact correct.

Ring 8. Let $\mathbb{Z}[\sqrt{2}] = \left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Z} \right\} \subseteq \mathbb{R}$. Define $d : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}$ by $d(a + b\sqrt{2}) := |a^2 - 2b^2|$. Verify that d is a multiplicative function. Give a geometric interpretation of what would imply euclidean with respect to d when using the basis $(1, 0)$ and $(1, \sqrt{2})$ for $\mathbb{R}^2$ (analogous to the previous problem). If $(x, y) \in \mathbb{R}^2$ choose an integer lattice point (m, n) as "close as possible" to (x, y) – how small can you make the differences $|x - m|$ and $|y - n|$? How small does that make $d\left((x + y\sqrt{2}) - (m + n\sqrt{2})\right)$? Conclude that $\mathbb{Z}[\sqrt{2}]$ is a euclidean ring with respect to d.

Ring 9. Try ideas similar to the preceding three exercises for other subrings of $\mathbb{R}$ or $\mathbb{C}$ (e.g., $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{6}]$ or ...) and see if you can find other euclidean rings. Note that the example of a ring which is not euclidean in Exercise 5 was $\mathbb{Z}[\sqrt{-5}]$ so don't expect to succeed too often. In fact, for $\sqrt{-3}$ show that the proof "just barely" fails (explain). Convert then to a proof that shows $\mathbb{Z}[\omega]$ is euclidean for $\omega = (1 + \sqrt{-3})/2$.

Ring 10 (Exact Sequence of a Pair in a PID)**.** Let R be a principal ideal domain (PID). Let $a, b \in R$, not both of which are 0. Define $f : R \times R \longrightarrow R$ by $f(s, t) = sa + tb$. Note that $R \times R$ is also a commutive ring with 1 when addition and multiplication are defined coordinate-wise:

(1) $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

(2) $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$

Further note that $R \times R$ is an R-module with scalar multiplication defined by

(3) $r \cdot (a, b) = (ra, rb)$

a. Show that f satisfies

(i) $f(x+y) = f(x) + f(y)$ for all $x, y \in R \times R$.

(ii) $f(rx) = rf(x)$ for $r \in R$, $x \in R \times R$.

Hence f is an R-module homomorphism.

b. Show that $\operatorname{im} f \subseteq R$ is non-empty and is closed under addition and scalar multiplication; that is, $\operatorname{im} f$ is an R-submodule of R.

c. Compute $\operatorname{im} f$.

d. Show that $\ker f \subseteq R \times R$ is an R-submodule of $R \times R$.

e. Determine $\ker f$ explicitly: Show that there exists a function $g : R \longrightarrow R \times R$ of the form $g(r) = (r\alpha, r\beta)$ for some $\alpha, \beta \in R$ such that $\operatorname{im} g = \ker f$. Note that g satisfies the analogue of (i) and (ii) above (i.e., is an R-module homomorphism).

f. Show that there exists an exact sequence of R-modules

$$0 \longrightarrow X \xrightarrow{i} R \times R \xrightarrow{f} R \xrightarrow{p} Y \longrightarrow 0 \ .$$

What are X, i, Y, p?

g. Determine precisely all solutions (s,t), $s,t \in R$ of the equation $sa + tb = \gcd(a,b)$ where $\gcd(a,b)$ denotes the greatest common divisor of a and b.

Ring 11 (Partial Fractions)**.** For the commutative domain R, we will let F denote its field of fractions.

a. Let R be a PID. For non-zero $a, b, c \in R$ with $\gcd(a,b) = 1$, show that there exist $\alpha, \beta \in R$ such that

$$\frac{c}{ab} = \alpha\frac{1}{a} + \beta\frac{1}{b}$$

in F.

b. Let R be a Euclidean ring with function d and $q \in R$ with $q \neq 0$. Show that any element of $a \in R$ has a *base* q expansion: that is, there exist $\alpha_i \in R$, $0 \leq i \leq m$ with either $\alpha_i = 0$ or $d(\alpha_i) < d(q)$, $\alpha_m \neq 0$ such that

$$a = \alpha_0 + \alpha_1 q + \alpha_2 q^2 + \cdots + \alpha_m q^m$$

in F.

c. Let R be a Euclidean ring with function d. Assume $a.q \in R$ are not zero and $s > 0$ is an integer. Then show there exist $a_i \in R$, $0 \leq i \leq s$ with $a_i = 0$ or $d(a_i) < d(q)$ when $0 < i$ which satisfy

$$\frac{a}{q^s} = \frac{a_s}{q^s} + \frac{a_{s-1}}{q^{s-1}} + \cdots + \frac{a_1}{q} + a_0$$

in F.

d. For R a Euclidean ring, combine the preceding parts and show that for $a, q \in R$, q not 0, if $q = up_1^{n_1} \dots p_m^{n_m}$ is the factorization of q ($u \in R$ a unit, $p_i \in R$ distinct irreducibles, $m_i > 0$), there exists a partial fraction decomposition in F

$$\frac{a}{q} = b + \sum_{i=}^{m} \sum_{j=1}^{n_i} \frac{\beta_{i,j}}{p_i^j}$$

with $b, \beta_{i,j} \in R$, where $\beta_{i,j} = 0$ or $s(\beta_{i,j} < d(p_i)$.

Show that if $R = F[x]$ and $d(g) = \deg(g)$, show that this decomposition is unique. Show that for $\mathbb{Z}$ and $d(k) = |k|$, such decompositions are never unique in case $\frac{a}{q}$ is not in $\mathbb{Z}$.

Ring 12 (Resultant)**.** Let F be an arbitrary field and $k > 0$ an integer. V_k will denote the subspace of $F[x]$ spanned by the ordered basis $\mathcal{B}_k = \{ x^{k-1}, x^{k-2}, \dots, x^1, 1 \}$ and $\mathcal{B}_0 = \varnothing$, the empty set. Let $f, g \in F[x]$ be two non-zero polynomials. Let $m = \deg(f)$ and $n = \deg(g)$. Define $T : V_n \oplus V_m \longrightarrow V_{m+n}$ by $T(u, v) = uf + vg$.

a. Give an explicit description of $\operatorname{im} T$. That is, it is the subset of V_{m+n} which has a very specific property.

b. Give an explicit description of $\ker T$. That is, give a precise formula for all pairs (u, v) in $\ker T$.

c. Show that there is an exact sequence of the form

$$0 \longrightarrow V_a \xrightarrow{i} V_n \oplus V_m \xrightarrow{T} V_{m+n} \xrightarrow{p} V_b \longrightarrow 0 \ .$$

Determine a, b and the linear transformations i, p explicitly in terms of the previous parts and standard results about polynomials.

d. Compute the rank of T in terms of f and g. Show that T is an isomorphism if and only if f and g are relatively prime.

e. Compute the matrix of T with respect to the two ordered bases $\mathcal{B}_n \oplus \mathcal{B}_m$ and $\mathcal{B}_{m+n}$. We define $R(f, g) = \det T$.

f. Show that

(1) $R(g, f) = (-1)^{mn} R(f, g)$

(2) $R(af, bg) = a^n b^m R(fg)$ for $a, b \in F$.

(3) $R(f_1 f_2, g) = R(f_1, g) R(f_2, g)$

(4) Compute $R(f, g)$ for $f(x) = x - r$.

(5) If r_i are all the roots of f and they lie in F, then $R(f, g) = \prod g(r_i)$.

Ring 13. Prove Theorem 32 as follows.

1. First show that a UFD does satisfy the asserted conditions: Verify that a UFD satisfies the ACC on principal ideals by considering the function $s(up_1^{n_1}\cdots p_k^{n_k}) = n_1+\cdots+n_k$ on generators of the ideals in the ascending chain.

2. Follow the outline used in proving that a PID is a UFD to show that only these conditions are needed in the proof.

Ring 14. Let R be a commutative domain satisfying the ascending chain condition on principal ideals. Show that $R[x]$ satisfies this condition as well. The following outline should be helpful:

1. If all ideals in the ascending chain are 0, the result is clear. So we may assume there are some non-zero ideals. To prove the result we may as well assume all ideals are non-zero.

2. Let $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_j \subseteq \cdots$ be an ascending chain of principal ideals. Now $I_j = (f_j)$ for some non-zero $f_j \in R[x]$. How are the degrees of the f_j related? Conclude that there exists a positive integer n_f so that $\deg f_j = \deg f_{n_f}$ for all $j \geq n_f$.

3. Let the leading coefficient of f_j be $a_j \in R$. How are the ideals (a_j) all related? Conclude that there exists a positive integer n_c such that for all $j \geq n_c$ there exists a unit $u_j \in U(R)$ so that $u_j a_j = a_{n_c}$.

4. Conclude that for sufficiently large N (how large?), then $I_j = I_N$ for all $j \geq N$.

Ring 15. Let R be a UFD and let F be its field of fractions. Prove that every irreducible in $R[x]$ is prime in $R[x]$ as follows. Define the *content* of a non-zero polynomial $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ to be the gcd of the set of coefficients $\{a_0, a_1, \ldots, a_n\}$. Denote this by $c(f)$.

a. Show that any non-zero $f \in R[x]$ can be written as $f = c(f)f_0$ for some $f_0 \in R[x]$. Show that $c(f_0)$ is a unit. Show that this decomposition of f is unique (up to units).

b. A polynomial f with $c(f)$ a unit is called *primitive*. Show that if $f, g \in R[x]$ are primitive polynomials, then their product fg is also primitive. [Hint: Assume that fg is not primitive and $p \in R$ is a prime that divides $c(fg)$. This prime p does not divide all of the coefficients of f or of g as they are primitive. Look at the first coefficient (counting from the bottom) that p does not divide for each of f and g. Now look at fg and reach a contradiction.]

c. For any two non-zero polynomials $f, g \in R[x]$ show that $c(fg) = c(f)c(g)$ (up to units).

d. Note that $R[x] \subseteq F[x]$ and that every element h of $F[x]$ can be written as $1/mh_1$ where m is a lcm for the denominators that appear in the coefficients of h and $h_1 \in R[x]$. Thus one can write $h = c/mh_0$ for $h_0 \in R[x]$ a primitive polynomial and $c, m \in R$ are non-zero.

e. Show that for non-zero polynomials $f, g \in R[x]$, then $f|g$ if and only if both $c(f)|c(g)$ in R and $f|g$ in $F[x]$.

f. Show that a non-zero polynomial $f \in R[x]$ is irreducible in $R[x]$ if and only if

(1) f is primitive, and

(2) f considered as an element of $F[x]$ is irreducible.

Assume that f can be non-trivially factored in $F[x]$. Show that by clearing denominators this yields a factorization of f in $R[x]$.

g. Conclude that the only irreducible elements of $R[x]$ are either irreducible elements of R or primitive polynomials of $R[x]$ which are irreducible when considered as elements of $F[x]$. Finally conclude that these are prime elements of $R[x]$.

Ring 16. Let R be a UFD. Prove that $R[x]$ is a UFD.

Ring 17. Let F be an arbitrary field.

a. Show that the intersection of an arbitrary number of ideals in $F[x]$ is an ideal in $F[x]$.

b. Let $f_1, \ldots, f_k \in F[x]$. The ideal generated by these is

$$(f_1, \ldots, f_k) = \{ g_1 f_1 + \cdots + g_k f_k \mid g_i \in F[x] \} ,$$

the set of all $F[x]$-linear combinations of $f_1, \ldots, f_k$. Show that this ideal is precisely the intersection of the ideals which contain all f_i, $1 \leq i \leq k$.

Ring 18. Let F be a field of characteristic 0, let $a \in F$, and let $f \in F[x]$ be a non-zero polynomial of degree less than n.

a. Then show (Taylor's Theorem)

$$f = \sum_{i=0}^{n-1} \frac{(D^i f)}{i!}(a)(x-a)^i .$$

[Hint: As the D^i are linear transformations, it suffices to prove for x^m. (why?) Apply the binomial theorem to $x^m = [?+?]^m$.]

b. Show that this representation of f is unique. [Hint: This part is easy.]

Ring 19. Let F be a field and let $f \in F[y]$ be a polynomial. Since the ideal $I = (f)$ generated by f is a subspace of $F[y]$, we can form the quotient vector space $F[y]/(f)$. Assume that f is not constant. (This exercise is the rigorous definition of root adjunction.)

a. For $a, b \in F[y]$, show $a + (f) = b + (f)$ if and only if f divides $a - b$.

b. Show $F[y]/(f)$ has a well-defined multiplication operation given by

$$(a+(f))(b+(f)) := ab+(f).$$

(In other words, if $a+(f) = a'+(f)$ and $b+(f) = b'+(f)$, show that $ab+(f) = a'b'+(f)$). Conclude that $F[y]/(f)$ is an F-algebra, and that there is a natural one-to-one homomorphism $F \longrightarrow F[y]/(f)$ (hence we can consider F as a subring).

c. Prove that $F[y]/(f)$ is a field if and only if f is irreducible.

d. Let f be irreducible and let $K = F[y]/(f)$. Let $h \in F[x]$. For $a \in K$ (or indeed for any F-algebra K), we can evaluate $h(a) \in K$ as usual. Show that there is an $a \in K$ such that $f(a) = 0$. Hence we have constructed a field K which contains F and which contains a root of the irreducible polynomial f.

Ring 20. Let $A \subseteq B$ be commutative domains.

a. Show that if A is a field and every element of B is the root of a non-trivial polynomial in $A[x]$, then B is a field.

b. Show that if B is a field and every element of B is the root of a non-trivial monic polynomial over $A[x]$, then A is a field.

Ring 21. Let R be a UFD. Let F denote the field of fractions of R. Note that there is a natural inclusion $R \subseteq F$ given via $r \mapsto \frac{r}{1}$. Let $f \in F[x]$ be a monic polynomial. Suppose $q \in F$ is a root of $f(x)$. Prove that q actually lies in R. [Hint: Write $q = \frac{a}{b}$ with $a, b \in R$ and b not 0. We may assume the gcd $(a,b) = 1$ because .... Conclude that b must be a unit of R (and hence $q \in R$) because if not, there will exist a prime p dividing b which we can conclude also divides a because .... Hence ....]

You've just found a necessary condition for a commutative domain R to be a UFD. It must be *integrally closed* in its field of fractions (the propery you just proved to hold).

Ring 22. a. Let F be a field and let F^F denote the set of all functions from F to F. Recall that this is a ring under the usual definition of addition and multiplication of functions (that is, add or multiply their values). As is shown avove, there is a function $E: F[x] \longrightarrow F^F$ given by sending the formal polynomial in $F[x]$ to the function which is computed by using the given polynomial as the formula for computation. This function E preserves both addition and multiplication (it is what is called a *ring homomorphism*). Further it was noted that this function is not always one-to-one. Prove that it is one-to-one if and only if F is an infinite field. Prove that it is onto if and only if F is a finite field. Show that the kernel of E (the polynomials that go to 0) is an ideal of $F[x]$. Give an explicit monic generator of this ideal.

b. If F has q elements, show that the generator you found in the preceding part is equal to $x^q - x$.

Ring 23. Verify that the three conditions in Definiton 35 are equivalent.

Ring 24. Let $^- : \mathbb{C} \longrightarrow \mathbb{C}$ denote ordinary complex conjugation. Show that $^-$ is an isomorphism of fields. (Even an $\mathbb{R}$-algebra isomorphism.) Show that $^-$ induces an isomorphism of rings

$$^- : \mathbb{C}[x] \longrightarrow \mathbb{C}[x]$$

by defining $\overline{h} = \overline{b_0} + \overline{b_1}x + \cdots + \overline{b_k}x^k$ for $h = b_0 + b_1x + \cdots + b_kx^k \in \mathbb{C}[x]$.

Ring 25. Let F be an arbitrary field. Denote by $D : F[x] \longrightarrow F[x]$ the usual derivative.

a. Let $f \in F[x]$ be a non-zero polynomial. Determine precisely when $Df = 0$.

b. Exhibit a field F and an irreducible polynomial $q \in F[x]$ with $Dq = 0$. [Hint: Consider the rational function field $F = \mathbb{F}_p(y)$, i.e.,the field of fractions of the domain $\mathbb{F}_p[x]$.]

Ring 26. Let $F[x]$ the ring of polynomials over a field F which has characteristic 0. Show that $f \in F[x]$ is a product of distinct irreducible polynomials if and only if $(f, Df) = 1$ where Df denotes the derivative of f. Is the same statement true if the field F has characteristic p for $p > 0$ a prime?

Ring 27. a. Prove $\{ 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \}$ is a linearly independent set over $\mathbb{Q}$.

b. Let $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{R}$. Find the minimal polynomial of α over $\mathbb{Q}$. That is, the monic polynomial $f(x) \in \mathbb{Q}[x]$ of least degree such that $f(\alpha) = 0$.

Ring 28. Let F be a field. Assume that A is an algebra with identity over F (see "Some Useful Definitions"). Assume further that

(1) A is a domain:
If $ab = 0$ for $a, b \in A$, then either $a = 0$ or $b = 0$.

(2) The dimension of A over F is finite.

a. Prove that every non-zero element of A has a multiplicative inverse. [Hint: Let $a \in A$, $a \neq 0$, and define $T_a : A \longrightarrow A$ by $T_a(b) = ba$. Show that T_a is a linear transformation and use theorems about linear transformations to prove that a has a left inverse. Then show that if every non-zero element of A has a left inverse, then the left inverses are actually two-sided inverses. (Note that this last part would not have been necessary if we assumed that A had commutative multiplication.)]

b. Let A be a subset of the complex numbers which is a commutative ring under the usual addition and multiplication of complex numbers. If A contains $\mathbb{Q}$ (the field of rational numbers) and is finite dimensional over $\mathbb{Q}$, conclude that A is a field. In particular, if $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$ and $r \in \mathbb{C}$ is a root of $f(x)$, prove that the set

$$\mathbb{Q}[r] = \{ q_0 + q_1r + \cdots + q_{n-1}r^{n-1} \mid q_i \in \mathbb{Q} \}$$

is a field.

c. If $f(x)$ is a prime polynomial and $r \in \mathbb{C}$ is a root of $f(x)$, show that the dimension of $\mathbb{Q}[r]$ over $\mathbb{Q}$ is the degree of $f(x)$. [Hint: Consider the ideal of polynomials which have r as a root.]

d. Prove that $x^3 - 29$ is irreducible in $\mathbb{Q}[x]$. Let r be the unique (positive) real number whose cube is 29. Let $\alpha = a + br + cr^2$ be a non-zero element of $\mathbb{Q}[r]$. Give a *formula* for α^{-1} in terms of a, b, c and r. [Hint: Consider part a. Find a matrix for T_α with respect to the basis $\{1, r, r^2\}$. (How can you determine α from this matrix?) Now find the matrix for α^{-1}. Linear algebra should now give you the formula!]

Ring 29. Let F be an arbitrary field.

a. Let $N = e_{2,1} + e_{3,2} + \cdots + e_{n,n-1} \in F^{n\times n}$. Determine the minimal polynomial of N.

b. Let $c \in F$. Let $S = cI + N \in F^{n\times n}$. Determine the minimal polynomial of S.

c. Let $M = N + e_{1,n} = e_{2,1} + e_{3,2} + \cdots + e_{n,n-1} + e_{1,n} \in F^{n\times n}$. Determine the minimal polynomial of M.

d. Let $c_1, \ldots, c_n \in F$ and let $D = \operatorname{diag}(c_1, \ldots, c_n) \in F^{n\times n}$ be the diagonal matrix with c_i in position (i, i). Determine the minimal polynomial of D.

e. Compute the minimal polynomial for the matrix

$$\begin{bmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & c \end{bmatrix}.$$

f. Let $A \in F^{n\times n}$ and let $B \in F^{m\times m}$. Assume f is the minimal polynomial of A and that g is the minimal polynomial of B. Let

$$D = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

be the block diagonal matrix in $F^{(n+m)\times(n+m)}$. Determine the minimal polynomial of D in terms of f and g.

Ring 30. The following is the Euclidean algorithm for computing the greatest common divisor of nonzero polynomials f_0 and f_1 in $F[x]$ (note that all of its steps can be computed by hand). Let's assume that we have labelled f_0 and f_1 so that $\deg(f_1) \leq \deg(f_0)$. Then define f_2 to be the remainder of f_0 when divided by f_1. Note that either $\deg(f_2) < \deg(f_1)$ or $f_2 = 0$. In general, inductively define f_{i+1} to be the remainder of f_{i-1} by f_i for as long as $f_i \neq 0$. Since $\deg(f_{i+1}) < \deg(f_i)$ for all i, at some step k we obtain $f_{k+1} = 0$. Set d to be the monic polynomial associated to f_k.

a. Prove that d is the greatest common divisor of f_0 and f_1.

b. Use the Euclidean algorithm to find the greatest common divisor of $x^5+x^4+3x^3+2x^2+3x+2$ and $x^4+x^3-2x^2-4x-8$ in $\mathbb{Q}[x]$.

c. Let K be a subfield of F, and suppose $f, g \in K[x]$. Let I_K be the ideal generated by f and g in $K[x]$, and let I_F be the ideal generated by f and g in $F[x]$. Prove that I_K and I_F have the same monic generator.

d. Let K be a subfield of the complex numbers $\mathbb{C}$, and let $f \in K[x]$. Suppose that f as a complex polynomial has a double root (that is, a root $\alpha \in \mathbb{C}$ of multiplicity ≥ 2). Prove that f is reducible in $K[x]$.

e. Show that the following process can be used to compute the greatest common divisor d of f_0, f_1 and at the same time yield s, t so that $sf_0+tf_1=d$.

   (i) Put $X=(1,0,f_0)$, $Y=(0,1,f_1)$, and $Z=(0,0,0)$.

   (ii) Divide the third component of X by the third component of Y to obtain q and r (Division Algorithm).

   (iii) If $r=0$, terminate the algorithm with $Y=(s,t,d)$. If $r\neq 0$, replace Z by Y, Y by $X-qY$ and X by Z. Note that Z is really just a temporary place to store the value of Y. Repeat step (ii).

   Find a way to interpret the preceding process as the multiplication of a certain 2 by 3 matrix on the left by elementary matrices with integer entries (i.e., row operations)

Ring 31. Let $f=x^3+x^2+x-3$ and $g=x^4-x^3+3x^2-x+4$. For each of the fields $F=\mathbb{Q}$, $\mathbb{F}_3$, $\mathbb{F}_{11}$ determine (f,g) and $[f,g]$ in $F[x]$.

Ring 32. Let F be a field. Let $f \in F[x]$ be non-zero polynomial. For $m>0$ a scalar $a \in F$ is called a *root of multiplicity* m of f if for some polynomial $g \in F[x]$, $f=(x-a)^m g$ and $g(a)\neq 0$.

a. If F is of characteristic 0, $f \in F[x]$ is non-zero, and $a \in F$, then a is a root of f of multiplicity $m>0$ if and only if

$$(D^i f)(a)=0, \quad 0\leq i\leq m-1$$

$$(D^m f)(a)\neq 0\ .$$

b. Let F be a field of characteristic 0 and let $f \in F[x]$ be a non-zero polynomial. Show that f is a product of distinct irreducible factors if and only if f and Df are relatively prime. [Hint: Consider the unique factorization of f.]

c. Show that one implication of the previous statement is true for any field, and give a counter-example to the other. [The last is a bit harder. Let $F(y)$ be the field of fractions of $F[y]$ (see earlier exercises). Choose F and a polynomial in $F(y)[x]$.]

Ring 33. Let R be a PID and let $a, b \in R$ be two non-zero elements. Show that there exist elements $r, s, u, v \in R$ such that

a. $(a, b) = au + bv$,

b. $a = (a, b)r$, $b = (a, b)s$, $[a, b] = (a, b)rs$,

c. the matrices $A, B \in R^{2\times 2}$

$$A = \begin{bmatrix} u & v \\ -s & r \end{bmatrix}$$

and

$$B = \begin{bmatrix} 1 & -vs \\ 1 & ur \end{bmatrix}$$

are invertible and $\det A = \det B = 1$,

d. and further the following holds:

$$A \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} B = \begin{bmatrix} (a, b) & 0 \\ 0 & [a, b] \end{bmatrix}.$$

Ring 34. Let R be a PID and $a_1, \ldots, a_n \in R$ be non-zero. Let $[a_1, a_2, \ldots, a_n]$ and $(a_1, a_2, \ldots, a_n)$ denote the least common multiple and greatest common divisor, respectively. Prove that (up to units)

$$\frac{[a, b, c]^2}{[a, b][b, c][c, a]} = \frac{(a, b, c)^2}{(a, b)(b, c)(c, a)}$$

.

Ring 35. Let R be a PID with $a, b, c \in R$ non-zero. Verify that

a. $[ab, ac] = a[b, c]$,

b. $(ab, ac) = a(b, c)$.

Ring 36. Let R be a UFD with $a, b, c \in R$ non-zero. Verify that

a. $[(a, b), (a, c)] = (a, [b, c])$,

b. $([a, b], [a, c]) = [a, (b, c)]$.

Ring 37. Let R be a commutative domain.

a. If (a, b) exists for all non-zero $a, b \in R$, then show that $[a, b]$ exists for all non-zero $a, b \in R$ and further that $(a, b)[a, b] = ab$, up to units.

b. Show that if $Ra + Rb$ is a principal ideal for all $a, b \in R$, then $Ra \cap Rb$ is a principal ideal for all $a, b \in R$.

Ring 38. Let $R = \mathbb{Z}[x]$. Show that there exist ideals in R which are not principal.

Ring 39. Let $R = F[x, y]$, polynomials in two variables over a field. Show that there exist ideals in R which are not principal.

Ring 40. Let R be a commutative ring. An ideal $I \subseteq R$ is called *maximal* if $I \neq R$ and if J is an ideal with $I \subseteq J \subseteq R$ then either $J = I$ or $J = R$.
An ideal $I \subseteq R$ is called *prime* if $I \neq R$ and if whenever $a, b \in R$ are such that $ab \in I$ then it must be that either $a \in I$ or $b \in I$.

a. Prove that a maximal ideal must be a prime ideal.

b. Prove that I is a maximal ideal if and only if R/I is a field.

c. Prove that I is a prime ideal if and only if R/I is a domain.

d. Let R be a principal ideal domain (such as $F[x]$). Determine all maximal ideals and all prime ideals of R.

e. Give an example to show that prime ideals are not always maximal.

Ring 41. Let V be a vector space over the field F. Let $T \in \mathrm{Hom}_F(V, V)$ be a linear transformation with minimal polynomial $\pi(x) = (x - c_1)(x - c_2) \cdots (x - c_k)$ where $c_1, c_2, \ldots, c_k \in F$ are distinct. Let $\pi_i(x) = \pi(x)/(x - c_i)$ and $p_i(x) = \pi_i(x)/\pi_i(c_i)$. Assume $k \geq 2$.

a. Apply Lagrange Interpolation (i.e., the fact that $\{ p_1, \ldots, p_k \}$ is the basis of $\mathcal{P}_k$ (all polynomials of degree less than k) which is dual to the set of evaluations $\{ E_{c_1}, \ldots, E_{c_k} \}$ (elements of ${\mathcal{P}_k}^*$) to write 1 as a linear combination of the p_i.

b. Let $T_i = p_i(T) \in \mathrm{Hom}_F(V, V)$. Prove that

$$I = T_1 + \cdots + T_k$$

holds in $\mathrm{Hom}_F(V, V)$. Here I denotes the identity linear transformation on V. Prove that

$$T_i T_j = 0$$

for $i \neq j$, and

$$T_i^2 = T_i$$

that is, T_i is idempotent.

c. Prove that $\mathrm{im}\, T_i = \ker(T - c_i I)$ and all are non-zero subspaces of V.

d. Prove that

$$V = \mathrm{im}\, T_1 \oplus \cdots \oplus \mathrm{im}\, T_k \ .$$

e. Let V be finite dimensional. Let $d_i = \dim \mathrm{im}\, T_i$. Note that $d_i > 0$. Choose bases for $\mathrm{im}\, T_i$ and let $\mathcal{B}$ be the basis of V which is their union. Compute the matrix $[\, T \,]_{\mathcal{B}}$.

f. Let A, $B \in F^{n\times n}$ each have minimal polynomial $\pi(x)$. Let $t = (d_1, \ldots, d_k)$ be the sequence of d_i as defined in the previous part for $T = L_A$. Let s be the corresponding series of integers for L_B. Prove that A and B are similar if and only if $t = s$.

g. Let T be as in the second previous part. Prove that the characteristic polynomial of T is $(x - c_1)^{d_1} \cdots (x - c_k)^{d_k}$.

h. In case $k = 1$, give the simplified version of the above.

Ring 42. Let R be a not necessarily commutative ring with identity. Then R is *local* if the sum of any two non-units is a non-unit. Recall that a *divison ring* is any ring with identity ($1 \neq 0$) such that every non-zero element has a multiplicative inverse.

a. Show that the set M of non-units of R is a two-sided ideal. Show that M is the unique maximal ideal of R. Show that R/M is a division ring. (If your proof of this is really short, it is WRONG.)

b. Let R be a ring in which every element is either a unit or nilpotent. Show that R is a local ring.

c. Determine for which integers n the ring $\mathbb{Z}_n$ is a local ring.

d. Let R be commutative domain with P a prime ideal. Let S be the complement of P in R. Let F be the field of fractions of R. Show that

$$S^{-1}R = \{\, r/s \in F \mid r \in R,\ s \in S \,\}$$

is a local ring. This ring is called the *localization of R at P*.

e. Let R be a commutative ring with M a maximal ideal. Show that R/M^k is local for $k > 0$ an integer.

f. Let F be a field and let $R = F[[x_1, x_2, \ldots, x_n]]$ be the ring of formal power series in n commuting variables. Show that R is a local ring.

g. Let F be a field, $n > 1$ an integer and let R be the set of upper triangular $n \times n$ matrices over F for which all of the entries on the diagonal are equal. Show that R is a local ring.

h. Let F be a division ring, $n > 1$ an integer and let R be the set of upper triangular $n \times n$ matrices over F for which all of the entries on the diagonal are equal. Show that R is a local ring.

The Notes for the course *Math 4330, Honors Linear Algebra* at Cornell University have been developed over the last ten years or so mainly by the following (in chronological order):

Gerhard O. Michler

R. Keith Dennis

Martin Kassabov

W. Frank Moore

and

Yuri Berest.

Most sections have been revised so many times the original author may no longer recognize it. The intent is to provide a modern treatement of linear algebra using consistent terminology and notation. Some sections are written simply to provide a central source of information such as those on "Useful Definitions", "Subobjects", and "Universal Mapping Properties" rather than as a chapter as one might find in a traditional textbook. Additionally there are sections whose intent is to provide proofs of some results which are not given in the lectures, but rather provide them as part of a more thorough development of a tangential topic (e.g., Zorn's Lemma to develop cardinal numbers and the existence of bases and dimension in the general case).

A large number of challenging exercises from many different sources have been included. Although most should be readily solvable by students who have mastered the material, a few even more challenging ones still remain.

Much still remains to be done. Corrections and suggestions for additional exercises, topics and supplements are always welcome.