

# *An Introduction to Algebra*

by

Pat Goeters

Department of Mathematics  
Auburn University  
Auburn, AL 36849-5310

These notes cover a standard one-term course in Groups, Rings and Modules, as presented at Auburn University, Fall 2001. The notes were also presented to a large group of Central American Mathematics Professors who gathered at the University of Nicaragua at Managua, Nicaragua, during the Summer of 2002. Before presenting these notes at UNAM, copies were made by the department head and sold at a vending table to interested faculty for \$ 2.00. (There were about 60 faculty from Central American countries.) Copies of my colleagues' (Geraldo de Souza) notes on the subject of Harmonic Analysis were also on sale at the vending table; the price, \$ 3.00. His must have

2

weighed more.

# Chapter 1

## An Introduction to Some Important Topics in Group Theory

### 1.1 Permutations on $n$ Letters

By a *permutation on  $n$  letters* we merely mean a one-to-one, onto function  $\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ . The set or collection of all permutations on  $n$  letters is denoted by  $S_n$  ( $S$  refers to the term symmetric, which will be used later on).

One way to express a permutation  $\sigma$  is:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix},$$

where  $i_1, i_2, \dots, i_n$  is just a reordering of  $1, 2, \dots, n$ . Using this notation, we can count the number of permutations on  $n$  letters; there are  $n$  choices for the number  $i_1$ ,  $n-1$  choices remaining for  $i_2$ ,  $n-2$  remaining for  $i_3$ , and so on. So, there are  $n(n-1)(n-2) \cdots 2 \cdot 1$  permutations on  $n$  letters;

$$|S_n| = n!$$

By a *cycle*, we mean the expression

$$\sigma = (i_1, i_2, \dots, i_m),$$

where  $i_1, i_2, \dots, i_m$  are distinct numbers in  $\{1, 2, \dots, n\}$ . This cycle represents the permutation that sends

$$i_1 \mapsto i_2, i_2 \mapsto i_3, \dots, i_m \mapsto i_1,$$

and all numbers other than  $i_1, i_2, \dots, i_m$  are left fixed (i.e.,  $\sigma(i) = i$  if  $i$  is not one of  $i_1, i_2, \dots, i_m$ ).

The function composition of  $\sigma$  and  $\delta$ , where  $\sigma, \delta$  in  $S_n$ , produces the element  $\sigma\delta$  in  $S_n$  by Exercise 1.2. By this we mean that  $(\sigma\delta)(j) = \sigma(\delta(j))$ .

**Observations:**

- (i) The function  $\iota : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  defined by  $\iota(j) = j$  belongs to  $S_n$ , and is called the *identity* map.
- (ii) If  $\sigma \in S_n$ , then  $\sigma^2, \sigma^3, \dots \in S_n$ , as well (Exercise 1.2).
- (iii) The functional inverse of  $\sigma \in S_n$ ,  $\sigma^{-1}$ , is also in  $S_n$ . By definition  $\sigma^{-1}(i) = j$  exactly when  $\sigma(j) = i$ . Another point of view yields that  $\sigma^{-1}$  is the only permutation for which  $\sigma\sigma^{-1} = \iota = \sigma^{-1}\sigma$ .

**Example 1** (a) If

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix},$$

then

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

(and then put the top row of the latter expression in order). For example, if

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix},$$

then

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}.$$

(b) Given a transposition  $\tau = (i_1, i_2, \dots, i_m)$ ,  $\tau^{-1} = (i_m, i_{m-1}, \dots, i_1)$ .  
For example,  $(1, 4, 3, 5, 2)^{-1} = (2, 5, 3, 4, 1)$ .

(iv)  $\sigma^k = \iota$  for some positive integer  $k$ , and therefore  $\sigma^{-1} = \sigma^{k-1}$ . To see this,  $S_n$  is finite so there are distinct positive integers  $m, \ell$  with  $\sigma^\ell = \sigma^m$ . If  $m < \ell$  multiply both sides by  $\sigma^{-m}$  to get  $\iota = \sigma^{\ell-m}$ .

## 1.2 Decompositions of Permutations

By *decomposition* we mean an appropriate way to break down a permutation into more elementary parts. This does not directly relate to the word composition from the phrase function composition.

**Permutation Decomposition:** Any permutation  $\sigma \in S_n$  can be expressed as a product (or composition) of cycles. Moreover, the cycles are disjoint, in that no number appears in two different cycles.

Here is how this works:

Choose any  $i \in \{1, 2, \dots, n\}$ , and call  $i_1 = i$ . Take  $i_2 = \sigma(i_1)$ ,  $i_3 = \sigma(i_2)$ , and so on; we quit this process as soon as  $\sigma(i_k)$  appears among  $i_1, i_2, \dots, i_k$ . We claim that  $\sigma(i_k) = i_1$ .

Note that, in this procedure,  $i_s = \sigma^{s-1}(i_1)$  where  $\sigma^0$  is defined to be  $\iota$ . If  $\sigma(i_k) = i_s$  with  $1 < s \leq k$ , then  $\sigma^{s-1}(i_1) = \sigma^{k-1}(i_1)$ ; and so,

$$i_1 = \sigma^{1-s}\sigma^{k-1}(i_1) = \sigma^{k-s}(i_1),$$

which contradicts our choice of  $k$ .

We have just produced the cycle  $\tau_1 = (i_1, i_2, \dots, i_k)$  which conforms to  $\sigma$  at each of  $i_1, i_2, \dots, i_k$ ;

$$\sigma(i_1) = i_2 = \tau_1(i_1)$$

$$\sigma(i_2) = i_3 = \tau_1(i_2)$$

...

$$\sigma(i_k) = i_1 = \tau_1(i_k).$$

Choose  $j$  not among  $i_1, i_2, \dots, i_k$  (if there is no such  $j$ , then we have finished). Set  $j_1 = j$ , and  $j_2 = \sigma(j_1)$ , and proceed as before. We have obtained a second cycle  $\tau_2 = (j_1, j_2, \dots, j_\ell)$  which agrees with  $\sigma$  on all of the numbers  $j_1, j_2, \dots, j_\ell$ . We continue producing cycles  $\tau_1, \tau_2, \dots, \tau_s$  until all of the numbers  $1, 2, \dots, n$  have been exhausted. Then

$$\sigma = \tau_1 \tau_2 \cdots \tau_s. \quad \diamond$$

A cycle

$$(i_1, i_2, \dots, i_k),$$

is said to be of *length*  $k$  and we will refer to this cycle as a  $k$ -*cycle*.

We can express the cycle above as a product of 2-cycles

$$(i_1, i_2, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_2).$$

This expression is not unique since for example

$$(i_1, i_2, \dots, i_k) = (i_2, i_3, \dots, i_k, a_1) = (i_2, i_1)(i_2, i_k) \cdots (i_2, i_3).$$

A 2-cycle is also called a transposition.

**Even/Odd Permutation Theorem:** Every permutation  $\sigma$  is a product of transpositions; the number of which is always even or always odd (depending upon  $\sigma$  and not the technique we use to decompose  $\sigma$ ).

**Proof:** It remains to compare the parities (remainders when divided by 2) of the number of factors in two decompositions

$$(a_1, b_1)(a_2, b_2) \cdots (a_k, b_k) = (c_1, d_1)(c_2, d_2) \cdots (c_m, d_m).$$

Getting all cycles to one side we find

$$(c_m, d_m) \cdots (c_1, d_1)(a_1, b_1) \cdots (a_k, b_k) = \iota.$$

So, in order to argue that  $k$  and  $m$  have the same parity (both are even or both are odd), we must show that  $m + k$  is even. That is, if  $\iota$  can be expressed as a product of say  $\ell$  transpositions, then  $\ell$  is even.

So we can forget about the notation used thus far and assume that  $\iota$  can be expressed as

$$(\dagger) (a_\ell, b_\ell)(a_{\ell-1}, b_{\ell-1}) \cdots (a_1, b_1) = \iota,$$

in order to show that  $\ell$  is even. Let  $c$  be any number appearing in one of the transpositions in  $(\dagger)$ , and let  $k$  be the smallest index for which  $c$  is one of  $a_k, b_k$ .

Write  $(a_k, b_k) = (c, d)$  and  $(a_{k+1}, b_{k+1}) = (a, b)$  and note that  $\ell > k$  since  $c$  cannot appear for the first time in the leftmost transposition.

One of the following applies:

- (i)  $(a, b)(c, d) = \iota$  when  $(a, b) = (c, d)$ ;
- (ii)  $(a, b)(c, d) = (c, d)(a, b)$  when  $(a, b)$  and  $(c, d)$  are disjoint;
- (iii)  $(c, b)(c, d) = (c, d, b) = (d, b, c) = (c, d)(d, b)$  when  $c = a$ ; likewise  $(c, a)(c, d) = (c, d, a) = (c, d)(a, d)$ , or the last possibilities,
- (iv)  $(a, b)(c, a) = (a, c, b) = (b, a, c) = (b, c)(b, a)$  when  $a = d$ , and  $(a, b)(c, b) = (a, c)(a, b)$ , when  $b = d$ .

When (i) holds we can reduce the number of transpositions in  $(\dagger)$  by two and produce a representation of  $\iota$  as a product of  $\ell - 2$  transpositions. Otherwise, (ii) – (iv) apply and we can rewrite  $\dagger$  to obtain an expression of  $\iota$  as a product of  $\ell$  transpositions where  $c$  appears for the first time in the  $(k + 1)^{st}$  transposition.

Focusing on the incident that one of (ii) – (iv) are applicable, once we have rewritten  $(\dagger)$  so that the first occurrence of  $c$  is in the  $(k + 1)^{st}$  transposition, we repeat the above steps to either cancel two transpositions from the rewritten form of  $(\dagger)$ , or rewrite  $(\dagger)$  yet again in order to move the first occurrence of  $c$  into the  $(k + 2)^{nd}$  transposition.

Again, since  $c$  cannot appear for the first time in the left-most transposition, we are eventually led to canceling two transpositions.

Repeating the above steps, leads to reducing transpositions in pairs from  $(\dagger)$ ; eventually leaving only  $\iota$  on the left-hand side. So,  $\ell$  must be even as desired.  $\diamond$

We call a permutation *odd* or *even* depending upon whether it can be expressed as either an odd-numbered product or even-numbered product of transpositions. The collection  $A_n$  consisting of the *even* permutations plays a prominent role in the history of Algebra:

$$A_n = \{\rho \in S_n \mid \rho \text{ is even}\}$$

By  $(1, 2)A_n$  we mean the set of permutations which are of the form  $(1, 2)\rho$  with  $\rho \in A_n$ . It is easy to see that  $(1, 2)A_n$  is the set of all *odd* permutations from  $S_n$ , and that

$$|(1, 2)A_n| = |A_n|.$$

So,

$$2|A_n| = |S_n| = n!$$

and therefore

$$|A_n| = n!/2 \text{ when } n \geq 2.$$

### 1.3 The Integers

Given two integers  $n, m$ , the *greatest common divisor of  $n$  and  $m$*  is the positive integer  $d$  that divides both  $n$  and  $m$ , with the additional feature that (\*) if  $k > 0$  divides both  $n, m$ , then  $d \geq k$ .

**Quotient and Remainder:** If  $n, m$  are positive integers, then there are non-negative integers  $q, r$  such that

$$n = qm + r, \text{ and either } r = 0 \text{ or } 0 < r < m.$$

**Euclid's Division Algorithm:** Given two positive integers  $n, m$ ; Set  $r_0 = m$ , and  $r_1$  equal to the remainder of  $n$  when divided by  $m$ . If  $r_1 \neq 0$ , set  $r_2$  equal to the remainder of  $r_0$  when divided by  $r_1$ . If  $r_2 \neq 0$ , set  $r_3$  equal to the remainder of  $r_1$  when divided by  $r_2$ . Note that as long as zero is not encountered for any  $r_i$ , we have  $r_0 > r_1 > r_2 > \dots$ . So, continuing this process must eventually lead to some subsequent  $r_j = 0$  (assume that no previous remainder was zero; i.e.,  $j$  is the first index for which  $r_j = 0$ ).

A.  $r_{j-1}$  is the greatest common divisor of  $n, m$ .

B. The greatest common divisor of  $n, m$  can be expressed as  $kn + \ell m$  for some integers  $k, \ell$ .



To see why Euclid's Division Algorithm is true, we must first unravel the sequence of quotient/remainder equations:

$$\begin{aligned} n &= q_1m + r_1 \\ m &= q_2r_1 + r_2 \\ r_1 &= q_3r_2 + r_3 \\ &\dots \\ r_{j-3} &= q_{j-1}r_{j-2} + r_{j-1} \\ r_{j-2} &= q_jr_{j-1}. \end{aligned}$$

Disregarding the last equation for the moment, we will work backwards from the second-to-the-last:

$$\begin{aligned} r_{j-1} &= r_{j-3} - q_{j-1}r_{j-2} \\ r_{j-1} &= r_{j-3} - q_{j-1}(r_{j-4} - q_{j-2}r_{j-3}) \\ r_{j-1} &= (1 + q_{j-1}q_{j-2})r_{j-3} - q_{j-1}r_{j-4}. \end{aligned}$$

We then replace  $r_{j-3}$  with  $r_{j-5} - q_{j-3}r_{j-4}$  to express  $r_{j-1}$  in terms of  $r_{j-4}$  and  $r_{j-5}$ , and likewise are able to express  $d = r_{j-1}$  in terms of any pair  $r_t$  and  $r_{t-1}$  where  $t < j - 1$ . In particular, we can express

$$d = ur_0 + vr_1$$

and so

$$d = um + v(n - q_1m) = vn + (u - q_1)m.$$

From the equation  $d = vn + (u - q_1)m$ , we see that any common divisor of  $n, m$  must also divide  $d$ .

We next observe that  $d$  is a common divisor of  $n$  and  $m$ ; from the last equation of our quotient/remainder equations,  $r_{j-2} = q_{j-1}d$ , and from the second to the last  $d = r_{j-3} - q_{j-1}r_{j-2}$ ; from these we find that  $d$  divides both  $r_{j-2}$  and  $r_{j-3}$ . By  $d = (1 + q_{j-1}q_{j-2})r_{j-3} - q_{j-1}r_{j-4}$  we see that  $d$  divides  $r_{j-3}$  and  $r_{j-4}$ . Eventually we observe that  $d$  divides all of the  $r_i$ 's; in particular  $d$  divides  $r_0$  and  $r_1$ .

So,  $d$  divides  $r_0 = m$  and  $r_1 = n - q_1m$ , and so  $d$  divides  $n, m$ . Since we have already noticed that any common divisor of  $n, m$  must also divide  $d$ , we now see that  $d$  is a common divisor of  $n, m$  that is greater than or equal to any common divisor of  $n, m$ . So,  $d = r_{j-1}$  is the greatest common divisor of  $n, m$ .  $\diamond$

**Example 2** *The greatest common divisor of 225 and 360 is found as follows:*

$$360 = (1)(225) + 135$$

$$225 = (1)(135) + 90$$

$$135 = (1)(90) + 45$$

$$90 = (2)(45).$$

*So, 45 is the greatest common divisor, and*

$$45 = 135 - 90 = 135 - (225 - 135) = 2(135) - 225$$

$$= 2(360 - 225) - 225 = 2(360) - 3(225).$$

*So, the greatest common divisor 45 is obtained as a linear combination*

$$45 = 2(360) - 3(225).$$

## 1.4 Complex Numbers

A complex number is an expression

$$a + b\mathbf{i}$$

where  $\mathbf{i}$  is a symbol whose square is  $-1$ . Multiplication and addition are said to *extend linearly*:

$$(a + b\mathbf{i}) + (c + d\mathbf{i}) = (a + c) + (b + d)\mathbf{i},$$

and

$$(a + b\mathbf{i}) \cdot (c + d\mathbf{i}) = (ac - bd) + (ad + bc)\mathbf{i}.$$

The *conjugate* (or more precisely, the *complex conjugate*) of  $a + b\mathbf{i}$  is defined to be

$$\overline{a + b\mathbf{i}} = a - b\mathbf{i}.$$

The length of a complex number  $a + b\mathbf{i}$  is written as  $|a + b\mathbf{i}|$ , and is defined to be  $\overline{(a + b\mathbf{i})}(a + b\mathbf{i}) = (a + b\mathbf{i})\overline{(a + b\mathbf{i})} = a^2 + b^2$ . So,  $\frac{1}{a^2 + b^2}(a + b\mathbf{i})$  has length 1.

The multiplicative inverse of a non-zero complex number  $a + b\mathbf{i}$  is readily seen to be

$$(a + b\mathbf{i})^{-1} = \frac{1}{|a + b\mathbf{i}|} \overline{(a + b\mathbf{i})} = \frac{1}{a^2 + b^2} (a - b\mathbf{i}).$$

Using the Maclaurin series for  $e^x$ ,  $\cos x$ , and  $\sin x$ , it is easy to establish;

**Demoivre's Formula:**

$$e^{\theta\mathbf{i}} = \cos \theta + \mathbf{i} \sin \theta.$$

From what we have stated, the numbers of the form  $e^{\theta\mathbf{i}}$  are the complex numbers of length 1.

## 1.5 Exercises

1. Show that a function  $\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  is one-to-one if and only if the function  $\sigma$  is onto.
2. Assume that  $\sigma, \delta \in S_n$ .
  - (a) Show that  $\sigma \circ \delta \in S_n$ . Henceforth we write  $\sigma\delta$  for  $\sigma \circ \delta$
  - (b) Show that  $\sigma^{-1}$  exists and belongs to  $S_n$ .
3. Express the following as products of disjoint cycles, and then products of transpositions.

(a)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 8 & 6 & 4 & 7 & 5 \end{pmatrix}$$

(b)  $\delta = (5, 7, 2, 3)(3, 4, 1)(8, 6, 2)$ (c)  $\alpha = (1, 3, 5)(3, 4)(4, 5)(2, 6, 8)$ (d)  $\beta = (1, 2, 3, 4, 5, 6, 7, 8)^2$ .4. Given  $\sigma = (1, 3, 4, 5)(2, 5, 7)$  and  $\delta = (6, 5, 4)(1, 3, 2)$ , compute:(a)  $\sigma\delta$ .(b)  $\sigma^{-1}, \delta^{-1}$ .(c) all distinct powers of  $\sigma$  and of  $\delta$ .(d) the powers of  $\sigma$  and  $\delta$  which produce  $\sigma^{-1}$  and  $\delta^{-1}$  respectively.5. List all of the six elements of  $S_3$ .6. List all of the cycles in  $S_4$ .7. Write out  $A_3$  and  $A_4$ .8. How many cycles are there in  $A_4$ ?

9. Use Euclid's Algorithm to find the greatest common divisors of the following pairs of numbers, and express the greatest common divisors as linear combinations of the numbers involved.

(a) 1115, 25.

(b) 473, 86.

(c) 110, 283.

10. Show that if  $n, m$  are positive integers, and  $d$  is the greatest common divisor of  $n, m$ , then the greatest common divisor of  $m/d$  and  $n/d$  is 1. Hint: Use B. of Euclid's Division Algorithm.11. Show if  $n$  and  $m$  have greatest common divisor equal to 1, and  $n$  and  $m$  divide an integer  $k$ , then  $nm$  divides  $k$ . Hint: Use B. from Euclid's Division Algorithm.

12. Assume that  $n$  and  $m$  have greatest common divisor 1. Show, for any integer  $k$ , if  $n$  divides  $mk$ , then  $n$  divides  $k$ . Hint: Use B. from Euclid's Division Algorithm.
13. The *least common multiple* of positive integers  $n, m$  is the smallest positive integer that is divisible by both  $n$  and  $m$ . Show that the least common multiple  $k$  of  $n$  and  $m$  can be found as

$$k = nm/d,$$

where  $d$  is the greatest common divisor of  $n$  and  $m$ . Hint: Use Problem 11 and some elbow grease.

14. Find the least common multiples of the pairs of numbers from Problem 9. Hint: Use Problem 12.
15. Important to the study of groups and rings, are the numbers  $\rho = e^{(2\pi/n)\mathbf{i}}$ , where  $n$  is a positive integer. Show that each power of  $\rho$ ,  $\rho^j$ , with  $j$  an integer, satisfies  $(\rho^j)^n = 1$ , and that  $\rho^j \neq 1$  if  $0 < j < n$ .
16. How many permutations in  $S_5$  are not cycles?



# Chapter 2

## An Introduction to Group Theory

### 2.1 Introduction

The study of groups arose from attempting to extend the the quadratic formula to polynomials of higher degree. Since that time, Group Theory has been employed in a variety of diverse fields in Mathematics and the Sciences. We will offer an general presentation here, and provide numerous examples to promote the concepts.

A *binary operation* on a set  $G$  is any function  $* : G \times G \rightarrow G$ . We will write  $a * b$  for the image of  $(a, b)$  under  $*$ .

A *group* is a set  $G$  along with a binary operation  $*$  on  $G$  such that the following hold:

- (i)  $*$  is associate; i.e.,  $a * (b * c) = (a * b) * c$  for all  $a, b, c, \in G$ .
- (ii) There is an element  $e \in G$  such that  $e * a = a * e = a$  for all  $a \in G$ .
- (iii) Given  $a \in G$ , there is an element  $a' \in G$  such that  $a * a' = a' * a = e$ , where  $e$  is described in (ii).

In honor of N. H. Abel for his triumphant work in showing the general quintic is not solvable by radicals, a group  $(G, *)$  is called *abelian*

if  $a * b = b * a$  for all  $a, b \in G$ . Furthermore, it is conventional to use  $+$  for the binary operation when  $G$  is abelian, so  $a * b$  is written  $a + b$ .

When a group is specified, the underlying set  $G$  and the binary operation  $*$  must be described. In practice, we down-play references to  $*$ , and write  $ab$  for  $a * b$ , and write  $G$  instead of writing  $(G, *)$ . With this notation,  $a^{-1}$  is written for the (unique) element  $a'$  associate with  $a \in G$  described in (iii), except when the additive notation  $=$  is used for the abelian group  $G$ ; then  $-a$  represents the element from (iii). Also, because of (i), parentheses are dropped when appropriate; i.e.,  $abc$  represents  $(a * b) * c$ .

## 2.2 Standard Examples

**Example 3**  $\mathbb{Z}$  is a group under the addition of integers binary operation.

**Example 4**  $S_n$  is a group under the composition of permutations binary operation.

Once a group  $G$  has been found (selected), other groups may be found inside  $G$ .

**Example 5** If  $G$  is a group, then a subset  $H$  of  $G$  is called a subgroup, provided  $H$  is again a group under the binary operation of  $G$ . It follows that a non-empty subset  $H$  is a subgroup of  $G$  if and only if  $H$  is closed under the binary operation of  $G$  and the unary operation  $a \mapsto a^{-1}$  for  $a \in H$ .

A theorem called *Cayley's Theorem*, asserts that for any group  $G$  with  $n$  elements, if we encode  $G$  as the numbers  $1, 2, \dots, n$ , then  $G$  can be regarded as a subgroup of  $S_n$  when  $G$  is identified with its encoding.

**Example 6** Since permutation multiplication on  $A_n$  is closed and the inverse of an even permutation is even,  $A_n$  is a group under permutation multiplication by the last two examples.



**Example 7** The group  $G$  is called cyclic if  $G = \langle a \rangle$  for some  $a \in G$ . In this case, the element  $a$  is called a generator for the cyclic group  $G$ . Prototypical examples of cyclic groups are the groups  $\mathbb{Z}_{(n)} = \langle \bar{1} \rangle$  and  $\mathbb{Z} = \langle 1 \rangle$ .

**Example 8** Given a group  $G$  and an element  $a \in G$ , the subset  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$  is a subgroup of  $G$ . Here,  $a^n$  is defined recursively;  $a^0 = e$  and  $a^n = aa^{n-1}$  for positive  $n$ ; when  $n = -m$  for some positive  $m$ ,  $a^n = (a^m)^{-1}$ . The subgroup  $\langle a \rangle$  is called the cyclic subgroup generated by  $a$ .

The element  $\sigma = (1, 2, \dots, n) \in S_n$  has  $n$  distinct powers:

$$\sigma^0 = \iota, \quad \sigma, \quad \sigma^2, \quad \dots, \quad \sigma^{n-1}.$$

Also,  $\sigma^n = \iota$ . Consequently, the cyclic group  $\langle \sigma \rangle$  has order  $n$ . Thus, for every  $n$ , there is a group of order  $n$ .

**Example 9** Suppose  $G$  is a group and  $H$  is a subgroup of  $G$ . There is an equivalence relation  $\sim$  defined on  $G$ , where  $a \sim b$  if  $b^{-1}a \in H$ . The equivalence class of  $a \in G$  is called the congruence class of  $a$  modulo  $H$ . If  $\bar{a}$  denotes this congruence class, then  $\bar{a} = \{b \in G \mid b^{-1}a \in H\} = \{b \in G \mid a^{-1}b \in H\} = \{b \in G \mid b \in aH\} = aH$ .

Now assume that  $G$  is abelian (written additively). The set of congruence classes is denoted by  $G/H$  and because  $G$  is abelian,  $G/H$  is also a group in a natural manner determined by  $G$ :

$$(a + H) + (b + H) = (a + b) + H.$$

The symbol  $+$  separating  $(a + H)$  and  $(b + H)$  refers to adding the sets  $a + H$  and  $b + H$  together, and so the equality is readily checked.

Some specific applications of the previous example yield some well-known groups.

**Example 10** In the previous example, take  $G = \mathbb{Z}$  under addition and  $H = n\mathbb{Z}$ . Then  $\mathbb{Z}/n\mathbb{Z}$  is a group consisting of exactly  $n$  elements  $\bar{0}, \bar{1}, \dots, \overline{n-1}$ , where  $\bar{i}$  denotes the congruence class of  $i$  modulo  $n\mathbb{Z}$ .

Addition is performed as  $\bar{i} + \bar{j} = \bar{k}$  with  $k$  taken to be the remainder (or residue) of the sum of  $i$  and  $j$  in  $\mathbb{Z}$  when divided by  $n$ . We denote the group  $\mathbb{Z}/n\mathbb{Z}$  by  $\mathbb{Z}_{(n)}$ .

**Example 11** Given a prime  $p$ ,  $\mathbb{Z}_p = \{ \frac{n}{m} \mid n, m \in \mathbb{Z}, p \nmid m \}$  is a subgroup of  $\mathbb{Q}$ . Thus,  $\mathbb{Q}/\mathbb{Z}_p$  is a group under addition of congruence classes. This group is infinite and is denoted by  $\mathbb{Z}_{(p^\infty)}$ .

The general element of  $\mathbb{Z}_{(p^\infty)}$  can be written as  $\frac{n}{p^k}$  where  $n, k$  are integers. From this it follows that every subgroup of  $\mathbb{Z}_{(p^\infty)}$  is cyclic. Observe that  $\mathbb{Z}_{(p^\infty)}$  is not cyclic.

**Example 12** One can form the external direct product of groups  $G_1, G_2, \dots, G_n$  to obtain a group

$$G = G_1 \times G_2 \times \cdots \times G_n,$$

whose elements are the (formal) ordered  $n$ -tuples  $(g_1, g_2, \dots, g_n)$ , where  $g_j \in G_j$  for all  $j$ , and whose binary operation is given by

$$(g_1, g_2, \dots, g_n) \cdot (g'_1, g'_2, \dots, g'_n) = (g_1 g'_1, g_2 g'_2, \dots, g_n g'_n).$$

The direct product  $G$  is abelian exactly when each  $G_j$  is abelian. In this case we will use the notation

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_n,$$

and refer to  $G$  as the direct sum of the  $G_i$ 's.

## 2.3 Subgroups

We find that a nonempty subset  $H$  of a group  $G$  is a subgroup if and only if  $H$  is closed with respect to the binary operation on  $G$  and closed under the formation of inverses.

**Example 13** All subgroups of  $\mathbb{Z}_{(12)}$  can be found below;

$$\mathbb{Z}_{(12)}, \quad \{0\}, \quad \{2, 4, 6, 8, 10, 0\}, \quad \{3, 6, 9, 0\}, \quad \{4, 8, 0\}, \quad \{6, 0\}$$

**Example 14** The subgroups of  $\mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(6)}$  can be computed as follows:  
Cyclic Subgroups:

$$C_0 = \{ (0, 0) \}$$

$$C_1 = \langle(0, 1)\rangle = \{(0, 1), (0, 2), (0, 3), (0, 4), (0, 5), (0, 0)\} = \langle(0, 5)\rangle$$

$$C_2 = \langle(0, 3)\rangle = \{(0, 3), (0, 0)\}$$

$$C_3 = \langle(0, 2)\rangle = \{(0, 2), (0, 4), (0, 0)\} = \langle(0, 4)\rangle$$

$$C_4 \langle(1, 3)\rangle = \{(1, 3), (2, 0), (3, 3), (0, 0)\} = \langle(3, 3)\rangle$$

$$C_5 = \langle(2, 3)\rangle = \{(2, 3), (0, 0)\}$$

$$C_6 = \langle(1, 2)\rangle = \{(1, 2), (2, 4), (3, 0), (0, 2), (1, 4), (2, 0), (3, 2), \\ (0, 4), (1, 0), (2, 2), (3, 4), (0, 0)\} = \langle(1, 4)\rangle$$

$$C_7 = \langle(1, 5)\rangle = \{(1, 5), (2, 4), (3, 3), (0, 2), (1, 1), (2, 0), (3, 5), (0, 4), \\ (1, 3), (2, 2), (3, 1), (0, 0)\} = \langle(1, 1)\rangle = \langle(3, 1)\rangle = \langle(3, 5)\rangle$$

$$C_8 = \langle(1, 0)\rangle = \langle(3, 0)\rangle$$

$$C_9 = \langle(2, 2)\rangle = \langle(2, 4)\rangle$$

$$C_{10} = \langle(2, 1)\rangle = \langle(2, 5)\rangle$$

$$C_{11} = \langle(3, 2)\rangle = \langle(3, 4)\rangle = \langle(1, 4)\rangle = \langle(1, 2)\rangle$$

*(Isn't this fun!)*

Non-Cyclic Subgroups:

$$N_0 = \mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(6)} = \langle(1, 0), (0, 1)\rangle = \langle(3, 0), (0, 1)\rangle = \langle(1, 5), (2, 1)\rangle$$

*( $N_0$  can be obtained for example by taking any of the elements  $(a, b)$  which generate a subgroup of order 12 above, then including a single element  $(c, d)$  not in  $\langle(a, b)\rangle$ )*

$$N_1 = \langle(2, 0), (0, 3)\rangle$$

$$N_2 = \langle(1, 0), (0, 2)\rangle$$

$$N_3 = \langle(2, 0), (0, 1)\rangle$$

**Example 15** *The subgroups of  $\mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(9)}$  are as follows;*

$$\langle(0, 0)\rangle$$

$$\mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(9)}$$

$$\langle(a, b)\rangle$$

*where  $(a, b)$  belongs to  $\mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(9)}$  (Of course, as above, it may turn out that  $\langle(a, b)\rangle = \langle(c, d)\rangle$  when  $(a, b) \neq (c, d)$ ).*

## 2.4 Cosets and Counting

From Example 9, when  $H$  is a subgroup of  $G$  we have an equivalence relation

$$a \sim b \leftrightarrow b \in aH.$$

From the nature of an equivalence relation, either

$$aH = bH \quad \text{or} \quad aH \cap bH = \phi.$$

Therefore,  $G$  is the disjoint union of distinct congruence classes, the number of which is equal to the number of cosets of  $H$  in  $G$ .

Furthermore, each congruence class has the same number of elements (namely,  $|H|$ ); to see this we observe the bijection between  $aH$  and  $H$  given by:

$$ah \mapsto h = a^{-1}ah$$

The notation for the number of cosets of  $H$  in  $G$  is  $[G : H]$ ; and so we have the following important result:

**Lagrange's Theorem:** If  $H$  is a subgroup of  $G$ , then

$$|G| = |H| \cdot [G : H].$$

The *order* of an element  $a \neq e$  in a finite group  $G$  is the least positive integer  $m$  such that

$$a^m = e.$$

Notice that for any integer  $k$ , write

$$k = qm + r,$$

with  $r$  either 0 or  $0 < r < m$ . Then  $a^k = a^{qm+r} = a^{qm}a^r = (a^m)^qa^r = a^r$  (in particular,  $a^m = a \cdot a^{m-1} = a^{m-1} \cdot a = e$  so  $a^{-1} = a^{m-1}$ ). Therefore,

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} = \{a, a^2, \dots, a^m = e\}.$$

Furthermore,  $\{e, a, a^2, \dots, a^{m-1}\}$  has  $m$  distinct elements since if

$$a^i = a^j \quad \text{with} \quad i < j,$$

then

$$a^{j-i} = e,$$

contrary to the selection of  $m$ . By Lagrange's Theorem,  $m$  divides the order of  $G$ .

If  $a^\ell = e$  for some integer  $\ell$ , write  $\ell = qm + r$  as in the Quotient/Remainder Theorem. Then, as above,

$$a^\ell = e = a^{qm+r} = a^r,$$

and since  $m$  is the smallest positive integer for which  $a^m = e$ ,  $r$  must be zero. Thus,  $m$  divides  $\ell$ .

## 2.5 Cyclic Groups

The Fundamental Theorem of Arithmetic asserts that any positive integer  $n$  is uniquely expressible as a product of powers of distinct primes

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

(primes are integers with no proper divisors).

We will provide a classification of finite abelian groups; this can be established from first principals. We only require the definition of a group and a weak version of The Fundamental Theorem of Arithmetic; every positive integer  $n$  has a prime divisor. To see this, suppose  $n$  is not prime. Then

$$n = n_0 m_0$$

where  $n_0$  and  $m_0$  are both proper divisors of  $n$  (i.e., neither of them is  $n$ ). If  $n_0$  is not prime, then

$$n_0 = n_1 m_1$$

where  $n_1$  and  $m_1$  are both proper divisors of  $n_0$ . Continuing along this path, we produce  $n > n_0 > n_1 > \dots$  and since positive integers cannot

descend infinitely, at some point we obtain that  $n_i$  is prime. I.e.,  $n$  has a prime divisor. Repeating this process, we obtain

**Fundamental Theorem of Arithmetic** If  $n$  is a positive integer, then there exist primes  $q_1, q_2, \dots, q_\ell$  such that

$$n = q_1 q_2 \cdots q_\ell.$$

**Subgroups of Cyclic Groups:** Subgroups of cyclic groups are again cyclic.

**Proof:** Let  $G = \langle g \rangle$  and suppose that  $H$  is a subgroup of  $G$ . If  $g^k \in H$ , then  $g^{-k} = (g^k)^{-1} \in H$ , so either  $H = \langle e \rangle$ , or there is a least positive integer  $m$  such that  $g^m \in H$ . In the former case,  $H$  is cyclic, so assume that latter. Now suppose  $g^n \in H$ . Write

$$n = qm + r \text{ as in the Quotient/Remainder Theorem.}$$

Then  $g^n = g^{qm+r} = (g^m)^q g^r$  and so,  $g^r = (g^m)^{-q} g^n \in H$  due to the fact that  $g^m$  hence  $g^{mq}$  and  $(g^m)^{-q} \in H$  for every integer  $q$ . But  $m$  was selected as the smallest positive integer for which  $g^m \in H$ , so  $r$  cannot be positive, and therefore must be 0. Thus,  $H = \langle g^m \rangle$ .  $\diamond$

**Theorem on Orders In Cyclic Groups:** Let  $g \in G$  have order  $n$ . Then  $h = g^k$ , where  $k$  is a positive integer, has order  $n/(n, k)$  where  $(n, k)$  is the greatest common divisor of  $n$  and  $k$ .

**Proof:**

Let  $d = (n, k)$  and set  $\ell = |g^k|$ . Then

$$(g^k)^{(n/d)} = g^{(n/d)k} = g^{n(k/d)} = (g^n)^{k/d} = e^{k/d} = e.$$

By the remarks at the end of the last section,  $\ell$  must divide  $n/d$ . But

$$(g^k)^\ell = e,$$

implying that  $n$  divides  $k\ell$  (by the previous section again), and so

$$\frac{k\ell}{n} = \frac{(k/d)\ell}{n/d},$$

and  $n/d$  divides  $(k/d)\ell$ .

By Exercise 10 on page 12,  $k/d$  and  $n/d$  are relatively prime (i.e., their gcd is 1), and therefore by Exercise 12 on page 13,  $n/d$  divides  $\ell$ . Thus,  $\ell = n/d$  as claimed.  $\diamond$

**Corollary 16** *Let  $G = \langle g \rangle$  be of order  $n$ . The only subgroups of  $G$  are  $\langle h \rangle$ , where  $h = g^d$  and  $d$  divides  $n$ .*

**Proof:**

Let  $H$  be a subgroup of  $G$ . From above,  $H$  is cyclic, and so  $H = \langle g^k \rangle$ . Let  $d = (n, k)$ . From Euclid's Division Algorithm,

$$d = uk + vn$$

for some integers  $u, v$ . We claim that  $H = \langle g^d \rangle$ . First,  $g^d = g^{uk+vn} = (g^k)^u (g^n)^v = (g^k)^u$ , so that  $g^d \in H$ . Conversely, if we write  $k = ad$  for some integer  $a$ , then  $g^k = (g^d)^a \in \langle g^d \rangle$ . Thus,  $H = \langle g^d \rangle$ .  $\diamond$

**Corollary 17** *Let  $G$  be a finite group of order  $n$ . Then  $G$  is cyclic if and only if for every  $m$  dividing  $n$ ,  $G$  has an element of order  $m$ .*

**Proof:** If  $G$  is cyclic of order  $n$  and  $m$  divides  $n$ , then set  $k = n/m$ , so that  $H = \langle g^k \rangle$  has order  $n/(n, k) = \frac{n}{n/m} = m$  by the Theorem on Orders in Cyclic Groups. Conversely, if for every  $m$  dividing  $n$ ,  $G$  has an element of order  $m$ , then  $G$  must have an element of order  $n$ . I.e.,  $G$  is cyclic.

$\diamond$

Using the examples we can construct endless finite abelian groups

$$G = \mathbb{Z}_{(n_1)} \oplus \mathbb{Z}_{(n_2)} \oplus \cdots \oplus \mathbb{Z}_{(n_k)}.$$

It turns out that all abelian groups (up to renaming the elements) can be obtained in this way.

## 2.6 Abelian Groups

Given groups  $G_1, G_2, \dots, G_n$  we have already encountered the (cartesian) direct sum

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i\}.$$

On the other hand, given an abelian group  $G$  with subgroups  $H_1, H_2, \dots, H_n$ , we say that  $G$  is the *direct sum* of the  $H_i$ 's and write  $G = H_1 \oplus H_2 \oplus \cdots \oplus H_n$  provided

$$G = \sum_{j=1}^n H_j = \{g \in G \mid g = h_1 + h_2 + \cdots + h_n \text{ where } h_i \in H_i \text{ for all } i\},$$

and for any  $i$ ,

$$H_i \cap \sum_{j \neq i} H_j = 0.$$

**Stickelberger Theorem:** Let  $G$  be a finite abelian group. If  $0 \neq g \in G$  is an element of maximal order, then  $G = \langle g \rangle \oplus H$  for some subgroup  $H$  of  $G$ .

**Proof:** Let  $H$  be a subgroup of  $G$  maximal with respect to  $H \cap \langle g \rangle = 0$  (as always,  $0$  serves many purposes; here  $0$  denotes the subgroup of  $G$  containing only the additive identity). Since  $G$  is finite,  $H$  is easy to find. In order to show that  $G$  is the direct sum of  $H$  and  $\langle g \rangle$  we must show that any  $a \in G$  can be written as  $kg + h$  for some integer  $k$  and some  $h \in H$ .

There is an integer  $m$  such that  $ma \in H \oplus \langle g \rangle$  (in fact,  $ma = 0$  for some  $m$ ). From the opening remarks of this section,  $m$  has a prime divisor,  $p$  say. We wish to show that  $ma \in H$  implies  $a \in H$ . Factoring  $m$  as  $pm'$ , if we show that  $pm'a \in H$  implies  $m'a \in H$ , then we can repeat this argument again with  $m'a$  instead of  $ma$  and eventually deduce that  $a \in H$ .

Thus, it suffices to argue the implication

$$pa \in H \oplus \langle g \rangle \Rightarrow a \in H \oplus \langle g \rangle.$$

We now forget about the above use of the letter  $m$ , and concern ourselves with  $p$ . Write  $pa = h + kg$  for some integer  $k$ .



First, we may as well assume that  $p$  divides  $m = |a|$ . For if  $p$  does not divide  $m$ , then  $up + vm = 1$  for some integers  $u, v$  by Euclid's Algorithm. But then,  $a = upa + vma = uh + uk g \in H \oplus \langle g \rangle$  as desired.

Now we show that  $p$  divides  $n = |g|$ . If not, then  $b = (m/p)a$  is an element of order  $p$  by the Theorem on Orders of Cyclic Groups, and so,

$$\langle b \rangle \cap \langle g \rangle = 0$$

(by Lagrange's Theorem). This implies,  $b+g \in \langle b \rangle \oplus \langle g \rangle$  is an element of order  $pn$ , the least common multiple of the orders of  $b$  and  $g$  (Exercise 9); this contradicts  $g$  having maximal order.

We have reduced to the situation that  $p$  divides both  $|g|$  and  $|a|$ . To see that  $p$  divides  $k$ , write  $m = p^i m'$  and  $n = p^j n'$  where  $p$  does not divide  $n'$ , or  $m'$ . Then  $m'a$  has order  $p^i$  and  $p^j g$  has order  $n'$ . By Lagrange's Theorem,  $\langle m'a \rangle \cap \langle p^j g \rangle = 0$  and therefore  $m'a + p^j g$  has order equal to the least common multiple of  $|m'a|$ , and  $|p^j g|$  which is  $p^i n'$ .

But  $pa \in H \oplus \langle g \rangle$  has order equal to the  $lcm\{|h|, |kg|\}$  and since  $p^j$  divides  $|kg|$ ,  $p^{j+1}$  divides  $m$ . But then  $i \geq j + 1$  so  $m'a + p^j g$  has order at least  $pn$ , a contradiction.

Write  $k = pk'$  and consider  $c = a - k'g$  and  $H' = H + \langle c \rangle$ . If  $H' = H$  then we conclude  $a \in H \oplus \langle g \rangle$ . Otherwise,  $H' \cap \langle g \rangle \neq 0$  by the choice of  $H$ ; say,  $k_0 g = h_0 + \ell_0 c \neq 0$ . If  $p$  divides  $\ell_0$ , then  $\ell_0 = p\ell'_0$ , and so  $0 \neq k_0 g = h_0 + \ell'_0 h \in H$ ; which is contrary to  $\langle g \rangle \cap H = 0$ . So,  $p$  does not divide  $\ell_0$  and  $up + v\ell_0 = 1$  for some integers  $u, v$ . Therefore,  $a = upa + v\ell_0 a = upa + v\ell_0 c + v\ell_0 k'g = h + kg + v(k_0 g - h_0) + v\ell_0 k'g \in H \oplus \langle g \rangle$  as needed.  $\diamond$

**Corollary 18** *Any finite abelian group  $G$  is a direct sum of cyclic groups. Moreover, the cyclic groups can be taken to have primary order.*

## 2.7 Stacked Basis Theorem

The last corollary is a version of the Fundamental Theorem for Finite Abelian Groups; namely that every finite abelian group is a direct sum of cyclic groups. Although the proof relies solely on the Frobenius

and Sticklerberger Theorem which was proven in the late 1800's, most textbooks prefer to use the following theorem to prove the Fundamental Theorem.

**Stacked Basis Theorem:** Let  $F = \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$  ( $n$  copies) and suppose that  $K$  is a subgroup of  $F$  such that  $mF \subseteq K$  for some integer  $m$ . Then, there is a generating set  $z_1, z_2, \dots, z_n$  of  $F$ , and positive integers  $d_1, d_2, \dots, d_n$  such that  $d_1z_1, d_2z_2, \dots, d_nz_n$  generates  $K$ .

**Proof:**

◇

## 2.8 Normal Subgroups and Homomorphisms

When considering a direct product

$$G = G_1 \times G_2 \times \cdots \times G_n,$$

for any  $i$ , the subgroup  $N = \{(e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_n) \mid g_i \in G_i\}$  of  $G$  satisfies the condition

$$gNg^{-1} = N.$$

Subgroups enjoying this property are said to be *normal* and play an elemental role in the study of groups.

**Proposition 19** *The following conditions are equivalent for a subgroup  $H$  of a group  $G$ :*

- (1)  $gHg^{-1} = H$  for all  $g \in G$ .
- (2)  $G/H$  is a group under the induced coset operation.
- (3) Every left coset is a right coset.

**Proof:** (1) is equivalent to  $gH = Hg$  for every  $g \in G$ , so (3) follows from (1). Conversely, if  $aH = Hb$ , then  $Ha \cap Hb \neq \emptyset$  implying that  $aH = Ha$  for every  $a \in G$ , so (1) follows from (3). Condition (2)

implies  $(gH)(g^{-1}H) = H$  and so  $gHg^{-1} \subseteq H$  for all  $g \in G$ . So,  $H = g^{-1}gHg^{-1}g \subseteq g^{-1}Hg$  for all  $g \in H$  and (1) follows from (2). Condition (2) follows from (1) by the computation  $(aH)(bH) = abHb^{-1}bH = abH$ .  $\diamond$

Given groups  $G$  and  $H$ , a function  $\phi: G \rightarrow H$  is called a *homomorphism* provided

$$\phi(ab) = \phi(a)\phi(b),$$

for all  $a, b \in G$ . The homomorphism  $\phi$  is called a *monomorphism* when  $\phi$  is One-to-one, and an *epimorphism* when  $\phi$  is onto. A one-to-one, onto homomorphism is called an *isomorphism*. The *kernel* of  $\phi$  is defined as

$$\text{Ker } \phi = \{g \in G \mid \phi(g) = e_H\},$$

where  $e_H$  is the identity element of  $H$ .

**Correspondence Theorem:** Given an epimorphism  $\phi: G \rightarrow H$ , there is a one-to-one correspondence between subgroups  $B$  of  $H$  and subgroups  $A$  of  $G$  containing  $\text{Ker } \phi$  given by

$$B \mapsto \phi^{-1}(B)$$

and

$$A \mapsto \phi(A).$$

Moreover, normal subgroups are sent to normal subgroups under this correspondence. In particular,  $\text{Ker } \phi$  is a normal subgroup of  $G$ .

**Proof:** Exercise.  $\diamond$

When there exists an isomorphism  $\phi: G \rightarrow H$  we write  $G \cong H$ .

**Fundamental Theorem For Finite Abelian Groups:** Any finite abelian group is the finite direct sum of cyclic groups of primary orders. Furthermore, if  $G_1 \oplus G_2 \oplus \cdots \oplus G_n \cong H_1 \oplus H_2 \oplus \cdots \oplus H_m$  with  $G_1, G_2, \dots, G_n, H_1, H_2, \dots, H_m$  cyclic of primary orders, then  $n = m$  and after reindexing  $G_j \cong H_j$  for all  $j$ .

## 2.9 Exercises

1. It is possible to find all groups of a given order by examining the possible binary operation tables. For example, there is only one possibility for a group of order 2:

*	e	a
e	e	a
a	a	e

Using  $ab = ac \rightarrow b = c$  and  $ca = ba \rightarrow b = c$  for all  $a, b, c$  in the group, find all groups of orders 3, 4, and 5 (apart from relabeling).

2. Let  $H$  be a subgroup of a finite group  $G$ . If  $[G : H] = 2$ , show that  $H$  is a normal subgroup of  $G$ .
3. What are the elements of maximal order in a direct product of finite cyclic groups  $C_1 \times C_2 \times \cdots \times C_k$ ?
4. (a) Show that  $\mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(2)}$  is not cyclic, so it has a different structure than  $\mathbb{Z}_{(4)}$ .  
 (b) Show that  $\mathbb{Z}_{(n)} \oplus \mathbb{Z}_{(m)}$  is cyclic if and only if  $m, n$  are relatively prime (i.e., their gcd is 1).
5. Show that for every positive natural number  $n$ , there is a group of order  $n$ .
6. Let  $g$  belong to a finite group  $G$ , and let  $m$  be the least positive integer such that  $g^m = 1$ . We call  $m$  is the *order of  $g$  in  $G$* . Show that  $m = |\langle g \rangle|$  and that  $m$  divides  $|G|$ .
7. List all abelian groups of order 24. Do not list isomorphic groups. Do the same for  $p^3$ ,  $p^4$ , and  $p^5$ .
8. If  $G$  is a finite abelian group, then  $G$  has an element of order  $p$  for every  $p$  dividing  $|G|$ .

9.  $(a, b) \in A \times B$  has order  $[n, m]$  (the lcm of  $m, n$ ) where  $n$  is the order of  $a \in A$  and  $m$  is the order of  $b \in B$ .
10. The largest order of an element in  $\mathbb{Z}_{(n)} \oplus \mathbb{Z}_{(m)}$  is  $[n, m]$ .
11.  $d = (n, m)$  if and only if  $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ .
12.  $\ell = [n, m]$  if and only if  $n\mathbb{Z} \cap m\mathbb{Z} = \ell\mathbb{Z}$ .
13. Can you describe all groups of order 3? Order 4? Order 5? Order 6? Order 7?
14. Use Lagrange's Theorem to argue that every group of order  $p$  is cyclic.
15. Let  $G$  be a group of even order. Show that  $G$  has an element  $a \neq e$  such that  $a^2 = e$ .
16. Find all generators for  $\mathbb{Z}_{(12)}$ ? Do the same for  $\mathbb{Z}_{(24)}$ .
17. Let  $\varphi$  be defined on the positive integers by setting  $\varphi(n)$  equal to the number of positive integers less than or equal to  $n$  that are relatively prime to  $n$ . ( $\varphi$  is called the Euler  $\phi$ -function). Show that  $\varphi(p^e) = p^{e-1}(p-1)$  for any prime  $p$ . Hint: Count the number of positive integers less than or equal to  $p^e$  that are not relatively prime to  $p^e$ .
18. How many generators does  $\mathbb{Z}_{(n)}$  have?
19. With  $\varphi$  equal to the Euler  $\phi$ -function, show that  $\varphi(nm) = \varphi(n)\varphi(m)$  if  $m$  and  $n$  are relatively prime.
20. Suppose that  $n$  can be factored into  $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$  where  $p_1, p_2, \dots, p_k$  are distinct primes and  $e_1, e_2, \dots, e_k$  are positive integers. Show that  $\varphi(n) = p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1) \cdots p_k^{e_k-1}(p_k-1)$ .
21. Consider the *quaternion group*  $\mathbb{H} = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$  where  $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ , and  $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$ ,  $\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$ , and  $\mathbf{ki} = \mathbf{j} = -\mathbf{ik}$ . Show that every subgroup of  $\mathbb{H}$  is normal but that  $\mathbb{H}$  is not abelian. Note also that every proper subgroup of  $\mathbb{H}$  is abelian as well.

22. Write down the cyclic group that represents the given factor group:

- (a)  $\mathbb{Z}_{(4)}/\langle 2 \rangle$
- (b)  $\mathbb{Z}_{(8)}/\langle 3 \rangle$
- (c)  $\mathbb{Z}_{(18)}/\langle 3 \rangle$
- (d)  $\mathbb{Z}_{(24)}/\langle 6 \rangle$
- (e)  $\mathbb{Z}_{(125)}/\langle 10 \rangle$
- (f)  $\mathbb{Z}_{(72)}/\langle 18 \rangle$

23. Classify the groups below according to the Fundamental Theorem for Finite Abelian Groups:

- (a)  $(\mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(4)})/\langle (0, 1) \rangle$
- (b)  $(\mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(4)})/\langle (1, 0) \rangle$
- (c)  $(\mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(4)})/\langle (0, 2) \rangle$
- (d)  $(\mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(8)})/\langle (1, 2) \rangle$
- (e)  $(\mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(8)})/\langle (1, 2, 4) \rangle$
- (f)  $(\mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(4)})/H$ , where  $H = \{(0, 0), (2, 0), (0, 2), (2, 2)\}$

24. Give an example of a nonzero homomorphism, if one exists. If no such homomorphism exists, state this.

- (a)  $\phi : \mathbb{Z}_{(12)} \rightarrow \mathbb{Z}_{(5)}$
- (b)  $\phi : \mathbb{Z}_{(12)} \rightarrow \mathbb{Z}_{(15)}$
- (c)  $\phi : \mathbb{Z}_{(12)} \rightarrow \mathbb{Z}_{(4)}$
- (d)  $\phi : \mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(4)} \rightarrow \mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(5)}$
- (e)  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_{(6)}$
- (f)  $\phi : \mathbb{Z}_{(4)} \rightarrow \mathbb{Z}_{(12)}$

25. Give a proper normal subgroup of the given group, if one exists. If no such normal subgroup exists, state this.

- (a)  $S_3$
- (b)  $A_3$
- (c)  $\mathbb{Z}_{(13)}$
- (d)  $\mathbb{Z}_{(12)}$
- (e)  $S_4$
- (f) For  $G$  equal to the subgroup of  $S_5$  generated by the cycle  $(1, 2, 3, 4, 5) \in S_5$ .
- (g)  $\mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(2)}$

26. State Lagrange's Theorem, and use the theorem as an aid to find all of the cosets of the given  $H$  in the associated  $G$ :

- (a)  $H = A_3$  in  $G = S_3$
- (b)  $H = \langle 3 \rangle$  in  $G = \mathbb{Z}_{(12)}$
- (c)  $H = \langle (1, 2) \rangle$  in  $G = \mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(4)}$
- (d)  $H = \langle (1, 2) \rangle$  in  $G = S_3$
- (e)  $H = \{(0, 0), (2, 0), (0, 2), (2, 2)\}$  in  $G = \mathbb{Z}_{(4)} \oplus \mathbb{Z}_{(4)}$
- (f)  $H = \langle 6 \rangle$  in  $G = \mathbb{Z}_{(15)}$





# Chapter 3

## An Introduction to Commutative Rings

### 3.1 Introduction

We provide the concept of a *ring* and an introduction to the theory of these objects. It is our interest to mainly present rings from an historical perspective. For example, before there was the general definition of a ring, there were the rings inside the field of complex numbers. The rings for which each nonzero element  $r \neq 0$  has a multiplicative inverse,  $\frac{1}{r}$  are called fields. The fields inside  $\mathbb{C}$  that are finite dimensional over  $\mathbb{Q}$  are called algebraic number fields, and form the foundation for Algebraic Number Theory, an area of Mathematics that is the conjunction of Number Theory and Commutative Ring Theory. Subrings of Algebraic Number Fields are the Classical rings due to Dedekind, and were developed in the mid to late 1800's. Such rings are called Algebraic Number Rings.

Generally, a *ring* consists of a set  $R$  with two binary operations,  $+$  and  $\cdot$ , defined on  $R$  such that

- (i) There is a element denoted by  $1 \in R$  such that

$$1 \cdot r = r \cdot 1 = r \quad \text{for all } r \in R.$$

- (ii)  $R$  is an abelian group under the binary operation  $+$ .

(iii) The distributive laws hold: for every  $r, s, t \in R$ ,

$$r \cdot (s + t) = r \cdot s + r \cdot t \quad \text{and} \quad (r + s) \cdot t = r \cdot t + s \cdot t.$$

(iv) The binary operation  $\cdot$  is associative: for every  $r, s, t \in R$ ,

$$(r \cdot s) \cdot t = r \cdot (s \cdot t).$$

If  $R$  is a ring with the additional property that  $r \cdot s = s \cdot r$  for every  $r, s \in R$ , then  $R$  (together with the two binary operations) is called a *commutative ring*. A commutative ring  $R$  such that for each  $0 \neq r \in R$ , there exists an  $s \in R$  for which

$$r \cdot s = s \cdot r = 1,$$

is called a *field*. If  $D$  is a ring such that for each  $0 \neq d \in D$ , there exists an  $b \in R$  for which  $d \cdot b = b \cdot d = 1$ , yet  $D$  is not commutative, then  $D$  is called a *division ring*. So, a commutative division ring is a field.

**Example 20** Under the usual binary operations,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{Z}_{(n)}$  are commutative rings.

**Example 21** The field of complex numbers  $\mathbb{C}$  consists of expressions of the form

$$a + b\mathbf{i},$$

where  $a, b \in \mathbb{R}$ , and  $\mathbf{i}$  is a symbol whose square is  $-1$ ;

$$\mathbf{i}^2 = -1.$$

It is a straightforward computation to show that  $\mathbb{C}$  is a field under the binary operations:

$$(a+b\mathbf{i})(c+d\mathbf{i}) = (ac-bd)+(ad+cb)\mathbf{i} \quad \text{and} \quad (a+b\mathbf{i})+(c+d\mathbf{i}) = (a+c)+(b+d)\mathbf{i},$$

with  $(a+b\mathbf{i})(c+d\mathbf{i}) = (c+d\mathbf{i})(a+b\mathbf{i})$ . Furthermore, if  $a+b\mathbf{i} \neq 0$ , then  $(a+b\mathbf{i})\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\mathbf{i}\right) = 1$ , so that  $\mathbb{C}$  is a field.

**Example:**

An element  $r$  of  $R$  is called a *left divisor of zero* if there exists an  $s \in R$  such that

$$r \cdot s = 0.$$

This makes  $s$  a *right divisor of zero*.

Commutative rings without zero-divisors are called *integral domains*. Some call a ring with no (left or right) divisors of zero, a *domain*, however, here we are building our Ring Theory on commutative rings, so a domain just means a commutative ring with no zero divisors; i.e., integral domain and domain are synonymous below. A non-commutative ring for which every non-zero element is a unit is a *division ring*.

**Example 22** *If  $d$  is any square-free integer, then*

$$R = \mathbb{Z}[\sqrt{d}] = \{n + m\sqrt{d} \mid n, m \in \mathbb{Z}\}$$

*is an integral domain under the standard operations. None of the elements from  $\mathbb{Z}$  (except  $\pm 1$ ) are units in  $R$ . On the other hand, when  $m \geq 2$ ,  $R$  has infinitely units of the form  $a + b\sqrt{m}$  with  $a, b$  both nonzero. Conversely, when  $m \leq -2$ ,  $\pm 1$  are the only units of  $R$ .*

**Example 23** *If  $d$  is any square-free integer, then*

$$F = \mathbb{Q}[\sqrt{d}] = \{n + m\sqrt{d} \mid n, m \in \mathbb{Q}\}$$

*is an field under the standard operations. We will generalize this in the next section.*

**Example 24** The collection  $R$  of all  $2 \times 2$  matrices with entries in  $\mathbb{R}$ ;

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with  $a, b, c, d \in \mathbb{R}$ , forms a non-commutative ring under the standard matrix multiplication and addition.

For example, if

$$A = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix}$$

then for

$$B = \begin{pmatrix} a & 0 \\ -1 & 0 \end{pmatrix},$$

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

The previous example is a ring with many zero divisors.

**Example 25** Let  $\mathbb{H}$  be the collection of elements of the form

$$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

where  $a, b, c, d \in \mathbb{R}$  and  $\mathbf{i}, \mathbf{j}$ , and  $\mathbf{k}$  behave as described in Exercise 2.1. Addition and multiplication extend linearly to make  $\mathbb{H}$  a non-commutative ring without zero divisors. The ring  $\mathbb{H}$  is called the ring of Hamiltonian Quaternions. Furthermore,  $\mathbb{H}$  is a division ring.

**Example 26** Let  $R = \mathbb{Z}[\sqrt{2}, \sqrt{3}]$ , which consists of all expressions of the form;

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

with  $a, b, c, d \in \mathbb{Z}$ . Since  $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$  are integrally independent,  $R^+$  is free abelian of rank 4.

Therefore, the integral Hamiltonian Quaternions  $\mathbf{Q}$ , the  $2 \times 2$  matrix ring over  $\mathbb{Z}$ ,  $Mat_{2 \times 2}(\mathbb{Z})$ , and the subring of  $\mathbb{C}$ ,  $R = \mathbb{Z}[\sqrt{2}, \sqrt{3}]$ , are all rings whose additive group structures are the same (free, abelian, of rank 4); two of which are noncommutative  $\mathbf{Q}$ , and  $Mat_{2 \times 2}(\mathbb{Z})$ . Of these two noncommutative rings,  $\mathbf{Q}$  is the only one that has no divisors of zero. A similar ring was established in [8] as a counter-example to a

conjecture of Eben Matlis. The statement of Matlis is rather technical so it will not be presented here.

**Example 27** Let  $S = \mathbb{Z}_2[\sqrt{5}, \sqrt{13}]$  where  $\mathbb{Z}_2$  is the collection of rationals  $\frac{a}{b}$  where  $a, b \in \mathbb{Z}$  are such that  $2 \nmid b$ .

**Definition:** An element  $r$  of  $R$  is called a *unit* if there exists an  $s \in R$  such that

$$r \cdot s = s \cdot r = 1.$$

We will get the ball rolling with a general result, but a result that requires very little background.

## 3.2 The Fundamental Theorem of Arithmetic

In this section  $R$  is an integral domain. Given  $a, b \in R$ , we say that  $a$  *divides*  $b$  in  $R$ , and write  $a \mid b$ , if there exists a  $c \in R$  such that  $ac = b$ . While the notion of an *ideal* in a ring can be elusive, we only need the most basic of types.

A subset of  $R$  consisting of all multiples of a given  $a \in R$  is called a *principal ideal* of  $R$ . Specifically, for  $a \in R$ , the subset  $I$  of  $R$  for which

$$b \in I \iff b = ra, \text{ for some } r \in R,$$

is called a principal ideal, or, the principal ideal generated by  $a$ . The notation

$$I = (a) = Ra,$$

is used interchangeably.

From the remark above concerning divisibility, if  $I = Ra$  and  $J = Rb$ , then

$$I \subseteq J \iff b \mid a.$$

Mimicking the state of affairs for the integers,

**Definition:** A domain  $R$  is called a *unique factorization domain*, or the acronym UFD for short, if any nonzero, nonunit  $r$  can be factored as a product

$$r = s_1 s_2 \cdots s_n,$$

for primes  $s_1, s_2, \dots, s_n$  of  $R$ .

**Definition:** Let  $R$  be an integral domain.

An element  $a \in R$  that is not a unit is called *irreducible*, if  $a = bc$  for some  $b, c \in R$  can only occur when  $c$  or  $b$  is a unit in  $R$ .

An element  $a \in R$  that is not a unit is called *prime*, if  $a \mid (bc)$  for some  $c, b \in R$ , implies  $a \mid b$  or  $a \mid c$ .

Prime elements are irreducible; if  $p$  is prime and  $p = ab$  for some  $a, b \in R$ , then  $p \mid ab$  and so  $p \mid a$  or  $p \mid b$ . If  $p \mid a$ , then  $pc = a$  and so  $p = ab = pcb$  implying  $1 = bc$ . Likewise, if  $p \mid b$ , then  $a$  is a unit. However, as we will see in our first theorem, irreducible elements are quite common-place while primes are not.

The uniqueness will be proven when needed.

**Example 28** As we will see shortly, the domain  $R = \mathbb{Z}[\sqrt{10}]$  affords that every non-zero, non-unit can be factored into a product of irreducible elements, and

$$6 = 2 \cdot 3 = -(4 + \sqrt{10})(4 - \sqrt{10}).$$

But none of  $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$  divides the other elements so these elements are not prime (the concepts will be formalized in a subsequent section, but ultimately the verification will be relegated to the Exercises). It follows that 6 cannot be factored into a product of primes in  $R$ .

**Theorem 29** *Suppose every chain of principal ideals of  $R$  stabilizes; i.e., if*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

*are principal ideals, then at some point (meaning there exists an index  $m$ ),*

$$I_m = I_n, \quad \forall n \geq m.$$

*Then, any nonzero nonunit in  $R$  is a product of irreducible elements.*

**Proof:** Suppose some nonzero, nonunit in  $R$  is not a product of irreducible elements. Let  $\mathcal{I}$  be the collection of all principal ideals  $\{(a) \mid a \text{ is not a product of irreducible elements}\}$ . Any chain in  $\mathcal{I}$ ;

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots,$$

must stabilize (by hypothesis) meaning that for some index  $m$ ,  $(a_j) = (a_m)$  for all  $j \geq m$ . Therefore,  $\mathcal{I}$  contains a maximal element, call it  $(a)$ .

We cannot have  $a$  irreducible by the description of  $\mathcal{I}$ , so there exist element  $b, c \in R$ , both non-units, such that  $a = bc$ . But then  $(a)$  is properly contained in both  $(b)$  and  $(c)$ , and so by the choice of  $(a)$ , both  $b$  and  $c$  are products of irreducible elements. But  $a = bc$  so  $a$  is a product of irreducible elements. This contradiction shows that  $\mathcal{I}$  must be nonempty.  $\diamond$

The uniqueness is provided for free (Mathematicians speak of "paying a price" for a particular hypothesis) for if

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m,$$

with  $p_i, q_j$  primes, then  $p_1$  divides  $q_1q_2 \cdots q_m$ , and so by the obvious (correct) extrapolation,  $p_1$  divides some  $q_j$ , which after re-indexing we assume to be  $q_1$ . Since  $q_1$  is irreducible,  $p_1 = u_1q_1$  for some unit  $u_1$ . After canceling we obtain

$$p_2p_3 \cdots p_n = u_1q_2q_3 \cdots q_m,$$

and by induction we obtain  $n = m$ , and after re-indexing,  $p_i = u_iq_i$  for some unit  $u_i \in R$ .

**Theorem 30** *The following are equivalent for an integral domain  $R$ :*

- (a)  $R$  is a UFD.
- (b) (i) Every non-zero, nonunit of  $R$  can be factored into a product of irreducible elements, and
  - (ii) If  $a_1a_2 \cdots a_n = b_1b_2 \cdots b_m$  occurs with  $a_i$  and  $b_j$  irreducible elements, then  $n = m$  and after re-indexing  $a_i = u_ib_i$  for some units  $u_i \in R$ .
- (c) Every non-zero, non-unit is a product irreducibles, and irreducibles are prime.
- (d) Any monotonically increasing chain of principal ideals stabilizes, and, irreducible coincides with prime.

**Proof:** (a)  $\rightarrow$  (d). Since

$$Ra \subseteq Rb \iff b \mid a,$$

the principal ideals containing  $Ra$  correspond to the divisors  $b$  of  $a$ . When  $R$  is a UFD, and

$$a = p_1p_2 \cdots p_n$$

with  $p_j$  prime, up to a unit multiple, the divisors of  $a$  are precisely  $\prod_{j \in N} p_j$  where  $N$  is a subset of  $\{1, 2, \dots, n\}$ . Therefore, there are only finitely many divisors of  $a$ , and hence principal ideals containing  $Ra$ . We surmise that chains of principal ideals

$$Ra \subseteq Ra_2 \subseteq Ra_3 \subseteq \cdots,$$



must be finite.

Also, if  $r$  is irreducible, then  $r$  is a product of primes. But  $r$  cannot have more than 1 prime due to irreducibility, and so  $r$  must be a single prime.

( $d$ )  $\rightarrow$  ( $c$ ) Done.

( $c$ )  $\rightarrow$  ( $b$ ). Evidently ( $b$ ) ( $i$ ) follows from ( $c$ ). Since irreducibles are primes, the argument just prior to the statement of this theorem shows that uniqueness is assured.

( $b$ )  $\rightarrow$  ( $a$ ). Since ( $b$ ) implies that irreducibles are prime, ( $a$ ) follows immediately from ( $b$ ).  $\diamond$

Uniqueness is not assured, in general, for factorizations into irreducibles.

**Definition:** Given a commutative ring  $R$ , an ideal  $I$  of  $R$  is a subset that is closed under the additive structure and ring multiplication of  $R$ , i.e.,

$$I^+ \text{ is an abelian group, and } rI = Ir \subseteq I, \forall r \in R.$$

If each ideal of  $R$  is principal, then  $R$  is called a Principal Ideal Domain, or PID for brevity, if  $R$  is an integral domain for which the ideals of  $R$  are precisely the ideals  $(a) = Ra$  for some  $a \in R$ . As a corollary to our theorem, we can deduce the Fundamental Theorem of Arithmetic, as it relates to domains. A technique for Mathematical Research is to take a property known to be true for the integers, and examine the domains supporting the property stated *mutatis mutandis* (a bit of Cocktail Latin, as Prof. Ullery would say!).

**Corollary 31** *If  $R$  is a PID, then  $R$  must be a UFD as well.*

**Proof:** First let

$$Ra_1 \subseteq Ra_2 \subseteq \dots$$

be a chain of principal ideals. Set  $I = \cup_j Ra_j$ . It is easy to check that  $I$  is an ideal, so from the hypothesis,  $I = Ra$  for some  $a \in I$ . Because  $I = \cup_j Ra_j$ , there is some index  $n$  such that  $a \in Ra_n$ . Then  $Ra \subseteq Ra_n \subseteq Ra$  from which we conclude that  $I = Ra = Ra_n = Ra_m$  for all  $m \geq n$ .

Now let  $r$  be irreducible and set  $I = Rr$ . Note that

$$(r) \subseteq (s) \iff s \mid r,$$

and because  $r$  is irreducible,  $I$  is a maximal ideal ( $I \neq R$  because  $r$  is not a unit!). So,  $R/I$  is a commutative ring with no proper ideals, and therefore must be a field (Exercise 42). Say  $r \mid st$ . Then  $(s+I)(t+I) = 0+I$  and since  $R/I$  is a field, either  $s+I = 0$  (i.e.,  $s \in (r)$ ) or  $t+I = 0$  (i.e.,  $t \in (r)$ ). Then,  $r \mid s$  or  $r \mid t$  as needed. Irreducibles are prime.  $\diamond$

A word of caution here: By Theorem 2 and its converse (Exercise 6.),  $R$  is a UFD if and only if every proper chain of principal ideals is finite. However, UFDs need not be noetherian or even seem noetherian-like (see the next section for the definition of noetherian).

**Example 32** *It is an exercise at the end of the section that when  $R$  is a UFD, then so is  $R[x]$ . Repeating, so is  $(R[x])[y] = R[x, y]$ , and so is  $R[x_1, x_2, \dots, x_n]$  for any number of indeterminates  $x_1, x_2, \dots, x_n$ . By  $R[x_1, x_2, \dots]$  we mean the polynomials with coefficients in  $R$  that involve only finitely many of the  $x_j$ 's, so it follows that  $R[x_1, x_2, \dots]$  is a UFD as well. The ideal  $(x_1, x_2, \dots)$  is obviously not finitely generated.*

Evidently, UFDs imply that any two nonzero, nonunits possess a *greatest common divisor* (without a notion of "greatest", we say that the greatest common divisor of  $a, b \in R$  is an element  $d$  such that  $d \mid a$ ,  $d \mid b$ , and if  $c \mid a$  and  $c \mid b$ , then  $c \mid d$ ).

**Example 33** *If  $R$  is a UFD, and  $a, b \in R$  are nonzero, nonunits, then the gcd  $(a, b)$  and the lcm  $[a, b]$  exists. In fact, write*

$$a = up_1^{e_1} p_2^{e_2} \cdots p_j^{e_j} \quad \text{and} \quad b = vp_1^{f_1} p_2^{f_2} \cdots p_j^{f_j},$$

where  $u, v$  are units,  $p_1, p_2, \dots, p_j$  are primes, and  $e_i, f_i \geq 0$  for all  $i$ .  
Then

$$(a, b) = se_1^{m_1} p_2^{m_2} \cdots p_j^{m_j} \quad \text{and} \quad [a, b] = te_1^{M_1} p_2^{M_2} \cdots p_j^{M_j},$$

where  $s, t$  are units,  $m_i = \min\{e_i, f_i\}$ , and  $M_i = \max\{e_i, f_i\}$  for  $i = 1, 2, \dots, j$ . Furthermore,

$$(a, b) \cdot [a, b] = a \cdot b.$$

It is known, but perhaps not well-known, that

**Example 34** Let  $R$  be a domain. Then, the *g.c.d.* exists for any pair of elements of  $R \iff Rc \cap Rd = Rd$ . That is, the intersection of principal ideals is principal.

Thus, a UFD has the property that the intersection of principal ideals is principal, further establishing a similarity between PIDs and UFDs.

**Proof:**

A sketch of this is the following; if  $d$  is the *g.c.d.* of  $a$ , and  $b$ , then  $d \in Ra \cap Rb$ . Furthermore, if  $c \in Ra \cap Rb$ , then  $c \mid a$  and  $c \mid b$ , and so  $c \mid d$ ; meaning  $c \in Rd$ . That is,  $Ra \cap Rb = Rd$ . Conversely, if  $Rd = Ra \cap Rb$ , then  $d$  satisfies the definition of the *g.c.d.* of  $a, b$ .

◇

Ostensibly, if *g.c.d.s* exist, then  $[a, b] = ab/(a, b) = (a/(a, b))b = a(b/(a, b))$ , where  $[a, b]$  (and  $(a, b)$ ) is the *l.c.m.* (respectively, *g.c.d.*) of  $a, b$ . Conversely, if the *l.c.m.* of  $a, b$  exists,  $[a, b]$ , then the *g.c.d.*  $(a, b) = (ab)/[a, b]$  exists as well.

### 3.3 The Classical Rings

The Fundamental Theorem of Algebra asserts that any polynomial with complex coefficients, has a complex root. An equivalent statement is, there is no finite dimensional field extension of  $\mathbb{C}$ , the field of complex numbers. Yet another, any polynomial  $g(z) = c_n z^n + c_{n-1} z^{n-1} + \cdots + c_0 \in \mathbb{C}[z]$  can be factored as

$$g(z) = c_n(z - \alpha_1)(z - \alpha_2) \cdots (z - \alpha_n), \text{ for some } \alpha_j \in \mathbb{C} \quad \forall 1 \leq j \leq n.$$

A complex number  $\alpha$  is called *algebraic* if there is a polynomial  $f(x) = a_n x^n + \cdots + a_1 x + a_0$  whose coefficients  $a_0, a_1, \dots, a_n$  lie in  $\mathbb{Q}$ , such that  $f(\alpha) = 0$ . Equivalently, if  $\alpha$  is a root to a polynomial  $g(x) = k_n x^n + \cdots + k_1 x + k_0$  where the coefficients  $k_0, k_1, \dots, k_n$  are integers. We call  $\alpha$  integral, if  $\alpha$  is a root to a monic polynomial  $h(x) = x^n + k_{n-1} x^{n-1} + \cdots + k_0$  with  $k_{n-1}, \dots, k_1, k_0$  integers. Evidently, integral elements are algebraic, but not conversely.

Say  $F$  is an algebraic number field. Such fields are of the form of

$$F = \mathbb{Q}[\alpha]$$

where  $\alpha \in \mathbb{C}$  is algebraic. However, the standard proof of this has a scope that requires time beyond what we have to offer at this point.

The Classical Rings of Dedekind are called *Number Rings*. Those are the rings  $R$  inside an algebraic number field  $F$ , that consists of all elements in  $F$  that are integral. We call  $R$  the *integral closure* of  $\mathbb{Z}$  inside  $F$  (i.e., the set of all elements that are in  $F$  and are roots to some monic polynomial with integer coefficients). For Number Rings, the additive structure is free abelian; that is,

$$R^+ \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$

Such rings are also called maximal  $\mathbb{Z}$ -orders. So, the number ring  $R$  in  $F$  is a  $\mathbb{Z}$ -order that are maximal (in fact the largest of all  $\mathbb{Z}$ -orders, inside  $F$ ). Since  $R$  contains all elements integral over  $\mathbb{Z}$  inside  $F$ , it follows that  $R$  contains every element in  $F$  that is integral, and as such, is a maximal  $\mathbb{Z}$ -order. Necessarily, the maximal order  $R$  has the following properties:

- (i) There is no ring inside  $F$  that is finitely generated over  $\mathbb{Z}$ , and contains  $R$  except  $R$ ;
- (ii)  $R$  is called Dedekind (i.e., every proper ideal of  $R$  is a product of maximal (prime) ideals of  $R$ );

While the following is not hard, it appears pulled out of the air. For now, we can offer two justifications, which we feel are interesting in their own right:

**Proposition 35** *If  $\alpha$  is algebraic, then  $F = \mathbb{Q}[\alpha]$  is a field.*

**Proof:**

We will present two disparate proofs, the purpose is to shine light on the different approaches.

- (1) Since  $F$  is finite dimensional over  $\mathbb{Q}$ , this monotonically decreasing sequence of subspaces of  $F$  must stabilize. This means that for some positive integer  $n$ ,  $F\beta^n = F\beta^{n+1}$ .

Write  $\beta^n = \gamma\beta^{n+1}$  for some  $\gamma \in F$ . Then, performing a little algebra,  $\beta^n(1 - \gamma\beta) = 0$ . We know that for any two numbers  $r, t$  in  $\mathbb{C}$ ,  $rt = 0$  only when  $r = 0$  or  $t = 0$ . Therefore, since  $\beta \neq 0$ ,  $\beta^n \neq 0$ , and by the remarks just made, we deduce that  $1 - \gamma\beta = 0$ , so that  $\gamma\beta = 1$ .

- (2) Here is another proof that  $F$  is a field. One would say that it is short, though writing it all down is not so short. There is a very old algorithm called Euclid's Division Algorithm. Of course it was stated for the integers; and it asserts, if  $m, n$  are integers, then there are integers  $u, v$  such that

$$un + vm = d,$$

where  $d$  is the greatest common divisor of  $n, m$ . Knowing how to divide elements from  $\mathbb{Q}[x]$ , the same can be said here. Specifically, given  $f(x), g(x) \in \mathbb{Q}[x]$ , there exists  $u(x), v(x) \in \mathbb{Q}[x]$  such that

$$u(x)f(x) + v(x)g(x) = d(x),$$

where  $d(x)$  is the greatest common divisor of  $g(x), f(x)$  (i.e., the polynomial of greatest degree which divides both  $f(x), g(x)$ ).

If  $f(x)$  is the irreducible polynomial for  $\alpha$ , and  $g(x) \in \mathbb{Q}[x]$  is such that  $g(\alpha)$  is a given element of  $F = \mathbb{Q}[\alpha]$ , then the degree of  $g(x)$  is less than the degree of  $f(x)$ . And so,  $g(x), f(x)$  can have no factors in common. Thus

$$u(x)f(x) + v(x)g(x) = 1,$$

and so

$$v(\alpha)g(\alpha) = 1,$$

showing that  $F$  is a field.

◇

Note, therefore, that for an algebraic  $\alpha$ , and any polynomial expression

$$b_\ell \alpha^\ell + b_{\ell-1} \alpha^{\ell-1} + \cdots + b_0$$

in  $\alpha$ , that is not zero, there exists a polynomial expression

$$c_k \alpha^k + c_{k-1} \alpha^{k-1} + \cdots + c_0$$

such that the product of the two expressions is 1. I.e.,

$$(b_\ell \alpha^\ell + b_{\ell-1} \alpha^{\ell-1} + \cdots + b_0)^{-1} = c_k \alpha^k + c_{k-1} \alpha^{k-1} + \cdots + c_0.$$

**Example 36** *The classical rings of Dedekind, are obtained by taking the integral elements residing in  $\mathbb{Q}[\alpha]$ , where  $\alpha \in \mathbb{C}$  is algebraic. It turns out that such rings have additive group structure that is free abelian. That is, if  $R$  is the collection of integral elements in  $F = \mathbb{Q}[\alpha]$ , then*

$$R^+ \cong \mathbb{Z}\mathbf{e}_1 + \cdots + \mathbb{Z}\mathbf{e}_n,$$

where  $\alpha$  has degree  $n$ , and  $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n$  are integrally independent, in that

$$m_1 \mathbf{e}_1 + m_2 \mathbf{e}_2 + \cdots + m_n \mathbf{e}_n = 0$$

precisely when  $m_1 = m_2 = \cdots = m_n = 0$ .

It is a small computation in showing that for an algebraic  $\alpha$ , there exists an integral  $\beta$  for which

$$\mathbb{Q}[\alpha] = \mathbb{Q}[\beta].$$

In fact, there is an integer  $a \neq 0$ , so that  $a\alpha$  is integral, and necessarily,  $\mathbb{Q}[\alpha] = \mathbb{Q}[a\alpha]$ . We will leave this as an exercise.

The point is, when  $\beta$  is integral,  $\mathbb{Z}[\beta]$  is a ring whose additive group structure is free abelian. However, this ring  $\mathbb{Z}[\beta]$ , is not necessarily the ring of Dedekind.

**Example 37** *When  $m$  is a square-free integer,  $\mathbb{Z}[\sqrt{m}]$  is a ring, with free abelian group structure, of rank 2. However, the ring of Dedekind can be shown to be dependent upon the congruence of  $m$  modulo 4. The ring of integral elements in  $\mathbb{Q}[\sqrt{m}]$  is;*

$$\mathbb{Z}[\sqrt{m}], \text{ precisely when } m \equiv 2, 3 \pmod{4},$$

and is

$$\mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right], \text{ exactly when } m \equiv 1 \pmod{4}.$$

$$\text{In the latter case, } \mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right] = \left\{ \frac{a + b\sqrt{m}}{2} \mid a \equiv b \pmod{2} \right\}.$$

The integral elements in an Algebraic Number Field  $\mathbb{Q}[\alpha]$  is called a Number Ring. These Number Rings are Dedekind in the sense that every ideal is a product of prime ideals. More about that later.

### 3.4 Valuations of Quadratic Number Rings

The obvious technique employed by all of us (admit it, you seek the easy way too!), is to take a ring, say, and through some identification, assign

a simpler numerical correspondence of the given ring. As quoted from J. B. Fraleigh, never underestimate something that counts something (or a grammatical improvement of this misquote). Perhaps a generalization is, never underestimate an integral formula that describes a theoretical condition. While there are more general assignments than the one given next, it will serve our purpose as an exemplar. These valuations will allow us to view examples more easily, such as prime, or irreducible elements, units, and the structure of the Number Rings.

**Example 38** Let  $R$  be the ring  $\mathbb{Z}[\sqrt{m}]$  as above. Define the value

$$\mathbf{v} : R^* \rightarrow \mathbb{N}, \text{ where } R^* = R \setminus 0,$$

by  $\mathbf{v}(a + b\sqrt{m}) = a^2 - b^2m$ . Then

- (1)  $\mathbf{v}$  is multiplicative (in that  $\mathbf{v}(\alpha\beta) = \mathbf{v}(\alpha)\mathbf{v}(\beta)$  for  $\alpha, \beta \in R$ .)
- (2)  $\mathbf{v}(\alpha) = \pm 1 \iff \alpha$  is a unit in  $R$ .
- (3) If  $\mathbf{v}(\alpha) = p$  for some integral prime  $p$ , then  $\alpha$  is irreducible in  $R$ .
- (4) If  $m \leq -2$ , then the only units of  $R$  are  $\pm 1$ ; if  $m = -1$ , then  $R$  has 4 units; if  $m \geq 2$ , then  $R$  has infinitely many units (the proof of this gets harder as  $m$  grows) - verify this for  $m = 2, 3, 4, 5, 6$ .

**Proof:** The proofs of these facts are relegated to the exercises.  $\diamond$

Keeping with the valuation theme, we have the following:

Besides the integers, there is a general collection of PIDs called *Euclidean Domains*. These are domains that have a measurement associated with them; in particular, the degree associated with polynomials. As was the case for the valuation on Number Rings, there is a more general notion which we examine here.

**Definition:** A Euclidean domain is an integral domain  $R$  for which there exists a function

$$\nu : R^* \rightarrow \mathbb{N},$$



with the property that given  $a, b \in R$ , there exists  $q, r \in R$ , for which

$$b = q \cdot a + r, \text{ and either } r = 0 \text{ or } \nu(r) < \nu(a).$$

Loosely put, we can divide  $b$  by  $a$  and either  $a$  divides  $b$  with quotient  $q$ , or,  $a$  divides  $b$  with quotient  $q$  and remainder  $r$  having smaller value (or size) than  $a$ .

**Example 39**  $R = \mathbb{Z}$  is Euclidean with  $\nu(n) = |n|$ .

**Example 40** Given a field  $F$ ,  $R = F[x]$  is Euclidean with  $\nu(f(x)) = \text{degree } f(x)$ . One can easily perform long division of one polynomial  $f(x)$  by  $g(x)$  and the remainder is either 0 or has smaller degree than  $g(x)$ .

**Example 41** In order to fit the definition of Euclidean, the value that we look at for the quadratic Number Ring inside  $\mathbb{Q}[\sqrt{m}]$  is defined to be  $\nu = |\mathbf{v}|$ . That is,  $\nu(a + b\sqrt{m}) = |a^2 - mb^2|$ . It turns out that among the Number rings, the Euclidean domains with this prescribed  $\nu$ -value are precisely the Number Rings corresponding to  $m = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$ .

The History of this work is quite extensive and involves many talented Mathematicians. The development of this could easily serve as a 1-semester, senior/graduate level course. Recall that when  $m \equiv 1 \pmod{4}$ , the Number Ring is actually  $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ . After all this interesting work has been amassed, it still remains open as to which of the Number Rings are Euclidean under a different value. (Surely, we can see that showing that an  $R$  fails to be Euclidean under a given value, is easier than showing, under no circumstances, is  $R$  Euclidean.)

In and of itself, this result is magnificent, but an ancillary fact established is that in case of the real Number Rings  $m \geq 2$ , the following was shown:

**Example 42** Let  $R$  be the Number Ring in  $\mathbb{Q}[\sqrt{m}]$  with  $m \geq 2$ . The following are equivalent:

- (1)  $R$  is a UFD.
- (2)  $R$  is a PID.
- (3)  $R$  is Euclidean.

**Remark:** It was proven under the Generalised Riemann Hypothesis, that, of the Real Number Ring  $R$ , inside  $\mathbb{Q}[\sqrt{m}]$ ,  $m \geq 2$ , that  $R$  is a PID if and only if  $R$  is Euclidean under the norm put forth above,  $\nu(a + b\sqrt{m})$  or  $\nu(\frac{a+b\sqrt{m}}{2})$  as the case may be, insures the Number Ring is Euclidean. GRH was removed subsequently in [9]. The equivalence of (1) and (2) is contained in [10].

**Example 43** The Number Ring in  $\mathbb{Q}[\sqrt{-19}]$  is  $R = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ , which is a PID that is not Euclidean, so the result in the previous example, relies upon  $m \geq 2$ . To prove this it is enough to show that each maximal ideal is principal. Furthermore, a maximal ideal is necessarily of the form  $P = (p, \alpha)$  where  $\alpha \in R$  has  $p$ ,  $p$  an integral prime. But,  $p = \alpha \cdot \bar{\alpha} \in P$ , once  $\alpha \in P$ , so  $P$  is necessarily principally generated.

In this last example, the Number Ring associated with  $m \equiv 1 \pmod{4}$  is  $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ , and so the correct valuation  $\nu$  is  $\nu(\frac{a+b\sqrt{m}}{2}) = \frac{a+b\sqrt{m}}{2} \frac{a-b\sqrt{m}}{2} = \frac{a^2 - mb^2}{4}$ , or to mimic the Euclidean definition,  $\nu(\frac{a+b\sqrt{m}}{2}) = |\frac{a^2 - mb^2}{4}|$  (See Exercise 41). Let us show how the proof of the statement above might proceed.

**Example 44** Let  $m = 3$ . We will show that the Number Ring  $R = \mathbb{Z}[\sqrt{3}]$  is Euclidean. We have  $\nu(a + b\sqrt{3}) = |a^2 - 3b^2|$  where  $a, b \in \mathbb{Z}$ . Given  $\alpha = a + b\sqrt{3}$ , and  $\beta = c + d\sqrt{3}$  inside  $R$ ; Consider

$$\alpha \cdot \beta^{-1} = (a + b\sqrt{3})(c - d\sqrt{3}) / (c^2 - 3d^2).$$

Since this is an expression of a rational plus a rational multiple of  $\sqrt{m}$ , we can certainly write this expression as  $\gamma \in R$  plus  $u+v\sqrt{m}$  where  $u, v$  are less than  $\frac{1}{2}$  in absolute value. The norm of this latter expression is  $|u^2 - 3v^2|$  which, in turn, is less than or equal to  $|\frac{3}{4}|$ . Therefore

$$\alpha = \gamma \cdot \beta + \rho \cdot \beta,$$

with  $\rho = 0$ , or  $\mathbf{v}(\rho) \leq \frac{3}{4}\beta < \beta$ .

The previous example works for  $m = 2$  as well as any negative  $m$ . Perhaps, to gain some respect for the problem, you may attempt to extend the result in the previous example when  $m = 5$  say! The remaining cases, have involved many great mathematicians, and is impressive in its depth and collective discovery.

**Example 45** As asserted before, the domain  $R = \mathbb{Z}[\sqrt{10}]$  affords that every non-zero, non-unit can be factored into a product of irreducible elements. However,  $R$  is not a UFD because the maximal ideal

$$P = R2 + R(4 + \sqrt{10})$$

is not principal. (Observe,  $R/2R$  has order 4, and thus,  $R/P$  has order 2.) Since PID coincides with UFD for the number ring  $R$  inside  $\mathbb{Q}[\sqrt{10}]$ ,  $R$  is not a UFD.

Alternately, we can show that 6 cannot be a product of primes

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

We will argue that 2, 3,  $4 + \sqrt{10}$ ,  $4 - \sqrt{10}$  are irreducible (hence prime, assuming that  $\mathbb{Z}[\sqrt{10}]$  is a UFD).

The case for 2 will be made here, the case for the remaining elements will be left as an exercise. Perhaps our approach is not the most elegant, but none-the-less, here it is, and it is quick. Suppose  $2 = \alpha\beta$ , neither of  $\alpha, \beta$  are units, and  $\alpha = a + b\sqrt{10}$ . Then the norm of  $\alpha\beta = 2$  yields

$$a^2 - 10b^2 = 2.$$

Whatcha gunna du? Well, look at congruences modulo 5, of course! Now,  $a$  is even,  $2k = a$ , and  $|\alpha| = a^2 - 10b^2 = 2$ . So, modulo 5,

$$a^2 = 2(2k^2) \equiv 2 \pmod{5}, \text{ or } 2k^2 \equiv 1 \pmod{5}$$

But, check it, the only squares modulo 5 are  $\pm 1$ , while we are presented with

$$k^2 \equiv 3 \pmod{5}.$$

This is impossible, and so 2 is irreducible.

Now, if  $P = R\delta$ , then  $2 = \delta\gamma$  and  $a + \sqrt{10} = \delta\mu$ . However, 2, and  $4 + \sqrt{10}$  are irreducible, so the only conceivable way is with  $\delta$  - a unit. But  $P \neq R$  because  $R/P$  has order 2.

### 3.5 Ideals in a Commutative Ring

**Definition:** An integral domain  $R$  is called *noetherian* if every ideal is finitely generated. That is, there exists

$$\exists a_1, a_2, \dots, a_n \in I \text{ such that } I = Ra_1 + Ra_2 + \dots + Ra_n.$$

**Example 46** Let  $F$  be an Algebraic Number Field  $\mathbb{Q}[\alpha]$  and  $R$  be the Number Ring inside of  $F$ . Recall, that  $R^+$  is free abelian, meaning

$$R^+ \cong \mathbb{Z}\mathbf{e}_1 \oplus \mathbb{Z}\mathbf{e}_2 \oplus \dots \oplus \mathbb{Z}\mathbf{e}_n,$$

for some integrally independent  $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n \in R$ . Let  $I \neq 0$  be an ideal of  $R$ ; if  $0 \neq \delta \in I$ , then  $m\delta^{-1} \in R$  since  $\delta^{-1} \in \mathbb{Q}[\alpha]$ , and  $F^+/R^+$  only has elements of finite order. But then,  $m1 = m\delta^{-1}\delta \in I$ , and so,  $mR \subseteq I \subseteq R$ . Then  $I^+/mR^+$  is contained in the finite group  $R^+/mR^+$ , and so,  $I^+/mR^+$  is finite. Thus,

$$I^+ \cong Ra_1 + Ra_2 + \dots + Ra_k + Rm\mathbf{e}_1 + Rm\mathbf{e}_2 + \dots + Rm\mathbf{e}_n$$

is finitely generated (here;  $I^+/mR^+ = \{a_1, a_2, \dots, a_k\}$ ). Therefore, all of the Number Rings are noetherian. (Surprising?)

In case  $I$  is an ideal of  $R$  that is *finitely generated*, we often write

$$I = (a_1, a_2, \dots, a_n).$$

Conversely, given  $a_1, a_2, \dots, a_n \in R$  we can define an ideal  $I$  by asserting

$$a \in I \Leftrightarrow \exists r_1, r_2, \dots, r_n \in R \text{ such that } a = \sum_{i=1}^n r_i a_i,$$

in which case  $I = (a_1, a_2, \dots, a_n)$ .

While examples of noetherian, and also non-noetherian domains abound, we found that

$$R = \mathbb{Z}[x_1, x_2, \dots] \text{ with infinitely indeterminates } x_1, x_2, \dots,$$

is non-noetherian. It is called the *Hilbert Basis Theorem* that if  $R$  is noetherian, then so is  $R[x_1, x_2, \dots, x_n]$  for any finite collection of indeterminates.

**Proposition 47** *The following are equivalent on an integral domain  $R$ :*

- (a)  $R$  is noetherian.
- (b) If  $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$  are ideals of  $R$ , then there is an index  $m$  such that  $n \geq m$  implies  $I_m = I_n$ .
- (c) Any nonempty collection of ideals has a maximal member.

**Proof:** (a)  $\rightarrow$  (b). Given such a chain of ideals, set  $I = \cup_n I_n$ . Since the ideals  $I_1, I_2, \dots$  form a chain,  $I$  is again an ideal (check this!). But  $I$  is finitely generated, so there exists a finite generating set  $a_1, \dots, a_n$ . For each  $i$ , there is an index  $m_i$  such that  $a_i \in I_{m_i}$ . Let

$$m = \max\{m_1, m_2, \dots, m_n\}.$$

Then each  $a_j \in I_m$  and so  $I = I_m$ .

(b)  $\rightarrow$  (c). Let  $\mathcal{I}$  be any nonempty collection of ideals. Choose  $I_1 \in \mathcal{I}$ . If  $I_1$  is not maximal among all ideals in  $\mathcal{I}$ , choose  $I_2 \in \mathcal{I}$  that properly contains  $I_1$ . Proceeding like this, in order that (b) is not violated, this process must stop, and it terminates in selecting an ideal that is not smaller than any other ideal of  $\mathcal{I}$ .

(c)  $\rightarrow$  (a). Given an ideal  $I$ , let  $\mathcal{I}$  be the set of all finitely generated ideals  $J$  such that  $J \subseteq I$ .  $\mathcal{I}$  has a maximal member  $J$ , and if  $J \neq I$  there is an element  $a \in I \setminus J$  so that  $J \subseteq J + (a) \subseteq I$ , in contradiction to (c).  $\diamond$

Given a ring  $R$ , a subset  $S$  of  $R$  is called a subring, provided  $S$  is a ring under the operations  $+$ ,  $\cdot$  that make  $R$  a ring. Simply put,  $S$  is a subring precisely when

$$r + s \text{ and } rs$$

belong to  $S$  whenever  $r, s \in S$ .

Let  $P$  and  $M$  be ideals of a commutative ring  $R$ . Then

- ( $\rho$ )  $P$  is a prime ideal if and only if  $ab \in P$  implies  $a \in P$  or  $b \in P$

- ( $\mu$ )  $M$  is a maximal ideal if and only if for any ideal  $M \subseteq J \subseteq R$ , either  $J = M$  or  $J = R$ .

There are definitions of maximal and prime that are analogous. By Exercise 23.,  $P$  is prime if and only if  $R/P$  is an integral domain; and,  $M$  is maximal if and only if  $R/M$  is a field.

It follows that maximal ideals are prime, but the converse is not valid.

**Example 48** *Let  $M$  be an ideal of  $R$ ,  $M \neq R$ . Then  $M = (r)$  for some irreducible element  $r$  if and only if  $(r)$  is maximal among all principal ideals of  $R$ . Hence, if  $R$  is a PID, then an ideal  $M$  is maximal if and only if  $M = (r)$  for some irreducible element  $r$ .*

**Definition:** If  $I$  and  $J$  are ideals of  $R$ , then by  $I \cdot J$  we mean

$$I \cdot J = \{ a_0b_0 + a_1b_1 + \cdots + a_kb_k \mid k \in \mathbb{N}, a_j \in I, b_j \in J, \text{ for all } j \}.$$

Then,  $I \cdot J$  is again an ideal of  $R$ , but an element of  $I \cdot J$  need not be of the form of  $ab$  where  $a \in I$ , and  $b \in J$ .

**Example 49** *There exists an integral domain  $R$ , such that each finitely ideal is principal. Yet, not every ideal is principal. For example, if  $\mathbb{A}$  is the ring of all integral elements in  $\mathbb{C}$ , then  $\mathbb{A}$  is Bezout (i.e., each finitely generated ideal of  $\mathbb{A}$  is principal), but there exists non principal ideals of  $\mathbb{A}$ . [Proof is rather lengthy, and will not be under-taken here.]*

**Definition:** Let  $P$  and  $M$  be ideals of the integral domain  $R$ , with  $P, M \neq R$ .

- $P$  is said to be a *prime* ideal, if for any  $r, s \in R$ ,  $rs \in P$  implies  $r \in P$  or  $s \in P$ .

- $M$  is said to be a *maximal* ideal, if for any ideal  $J$  containing  $M$ , either  $J = M$  or  $J = R$ .

There is an arithmetic that we can perform on ideals. Given ideals  $I$  and  $J$ , define the addition of the two ideals as

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

and the multiplication as

$$c \in IJ \iff c = \sum_j a_j b_j \quad a_j \in I, b_j \in J.$$

Certainly  $IJ$  contains  $ab$  where  $a \in I$  and  $b \in J$  but the set  $\{ab \mid a \in I, b \in J\}$  is not usually closed under  $+$  and will not be an ideal in those cases. Later we will consider multiplicative ideal theory.

We will make several observations:

Observation: An ideal  $P \neq R$  is prime if and only if for any ideals  $I, J$  of  $R$  with  $IJ \subseteq P$ , either  $I \subseteq P$  or  $J \subseteq P$ .

**Proof:** If  $P$  is prime and the ideals  $I, J$  are given, with  $IJ \subseteq P$  while  $J$  and  $I$  are both not contained in  $P$ , then let  $a \in J \setminus P$  and  $b \in I \setminus P$ . Then  $ab \in P$  but  $a, b \notin P$ , a contradiction. Conversely, if  $ab \in P$ , then  $(a)(b) = (ab) \subseteq P$  implies  $a \in (a) \subseteq P$  or  $b \in (b) \subseteq P$ , so the ideal-theoretic property leads to the elemental property.

Observation: An ideal  $M \neq R$  is maximal if and only if for any  $r \in R \setminus M$ ,  $M + (r) = R$ .

**Proof:** If  $M$  is maximal and  $r \in R \setminus M$ , then  $M + (r)$  is an ideal properly containing  $M$ . Hence  $M + (r) = R$ . Conversely, if  $M$  satisfies  $M + (r) = R$  for any  $r \in R \setminus M$ , and  $J$  is an ideal containing  $M$ , then either  $J = M$ , or there exists  $r \in J \setminus M$ . In the latter case,  $R = M + (r) \subseteq J \subseteq R$ , and so  $J = R$ .

Observation: Maximal ideals are prime.



**Proof:** If  $rs \in M$  and  $r \notin M$ , then  $M + (r) = R$  and so  $m + ar = 1$  for some  $m \in M$  and  $a \in R$ . Then,  $s = sm + sar \in M$ .  $\diamond$

**Observations:** Every ideal  $I$  unequal to  $R$  is contained in some maximal ideal  $M$ .

**Proof:** Consider the set  $\mathcal{M}$  of all ideals  $J$  such that  $I \subseteq J$  and  $J \neq R$ . Then  $I \in \mathcal{M}$  so  $\mathcal{M}$  is nonempty. If  $\{J_\alpha\}_{\alpha < \lambda}$  is a chain of elements from  $\mathcal{M}$  (i.e.,  $\alpha < \beta \Leftrightarrow J_\alpha \subseteq J_\beta$ ), then set  $J = \cup_{\alpha < \lambda} J_\alpha$ . It is easy to see that  $J \in \mathcal{M}$ . Therefore, by Zorn's Lemma,  $\mathcal{M}$  contains a maximal element  $M$ . If  $J$  is an ideal that contains  $M$  and  $J \neq R$ , then  $J \in \mathcal{M}$  and so  $J$  must be equal to  $M$  by the choice of  $M$ . Thus,  $M$  is a maximal ideal of  $R$ .  $\diamond$

The following are easy exercises:

Show:  $P$  is prime if and only if  $R/P$  is an integral domain.

Show:  $M$  is maximal if and only if  $R/M$  is a field.

Show: Finite integral domains are fields, so if  $P$  is a prime ideal such that  $R/P$  is finite, then  $P$  is a maximal ideal.

## 3.6 The Integral Closure Revisited

When we study domains, a primary tool is the *integral closure* of the domain, and to use it we need to develop it. If we just wish to characterize Dedekind domains, we can be satisfied with a simpler description of the integrally closed property, one that is readily usable. So, we need to balance the two objectives. (That is, the definitions we consider now will be towards a more general perspective in order to accommodate the homework, rather than the definition of integral closure given in

class for the purpose of proving our Dedekind domains theorem).

**Definition:** An element  $t \in Q$  will be said to be *integral over*  $R$  if there is a finitely generated (as an  $R$ -module) over-ring  $S$  of  $R$  inside  $Q$  which contains  $t$ . Given a domain  $R$ , an over-ring  $S$  of  $R$  in the quotient field  $Q$  is said to be *integral over*  $R$ , if every  $t \in S$  is integral over  $R$ . If every element in  $Q$  that is integral over  $R$  belongs to  $R$ , then we say that  $R$  is *integrally closed*.

**Proposition 50** *The following are equivalent for an integral domain  $R$  and an element  $t$  in a field  $F$  containing  $R$ :*

- (1)  $t$  is integral over  $R$ .
- (2)  $R[t]$  is a (module) finitely generated over-ring of  $R$ .
- (3) There is a polynomial  $f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$  such that  $f(t) = 0$ .

**Proof:** (2)  $\rightarrow$  (1) is obvious. (3)  $\rightarrow$  (2) is easy because  $t^n = -\sum_{j=1}^{n-1} r_j t^j$  implying that  $R[t]$  is a ring that is generated as an  $R$ -module by  $1, t, \dots, t^{n-1}$ .

(1)  $\rightarrow$  (3). Let  $S$  be a subring of  $F$  containing  $R$  and  $t$  such that  $S = Rt_1 + Rt_2 + \cdots + Rt_n$ . For each  $i$  there exists  $r_{ij} \in R$  with  $j$  running from 1 to  $n$ , such that

$$t \cdot t_i = \sum_{j=1}^n r_{ij} t_j.$$

Let  $A$  be the  $n \times n$  matrix whose  $i, j^{\text{th}}$  entry is  $r_{ij}$ . Then, we can rephrase the above equation as the matrix equation

$$AX = tX,$$

where  $X$  is the  $n$ -tuple  $(t_1, t_2, \dots, t_n)$  (actually, stand  $X$  up to multiply). Or, in the other familiar form

$$(A - tI)X = 0,$$

where  $I$  is the  $n \times n$  identity matrix.

If we let  $x$  be an indeterminate, then the determinant of  $A - xI$  (computed using cofactor expansion for example), is a monic polynomial of degree  $n$ , for which  $t$  is a root. This works the same way it always has in undergraduate linear algebra. Therefore,  $t$  is a root to  $\det(A - xI)$ , which as you may recall, is equal to  $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ .

◇

Here is the definition given in class describing integrally closed.

**Corollary 51** *The noetherian domain  $R$  is integrally closed if and only if whenever  $S$  is an over-ring of  $R$ ,  $S^{-1} = \emptyset$ .*

**Proof:** This is due to the fact that  $S^{-1} \neq 0$  (i.e.,  $S$  is a fractional over-ring) if and only if  $S$  is finitely generated:

$0 \neq t \in S^{-1} \Rightarrow tS \subseteq R \Rightarrow S \cong tS$  is a (finitely generated) ideal of  $R$ ,

and

$S$  finitely generated over  $R \Rightarrow S = Rt_1 + \cdots + Rt_n$

for some  $t_j \in Q \Rightarrow rS \subseteq R$  for some  $0 \neq r \in R$

(clear the denominators of the  $t_j$ 's). ◇

Some well-known examples of integrally closed domains are the rings we have just finished studying.

**Example 52** *If  $R$  is a UFD, then  $R$  is integrally closed.*

**Proof:** Suppose  $t = r/s \in Q$  is integral over  $R$ . We can assume that  $r/s$  is in lowest form so that the  $\gcd(r, s) = 1$  ( $r, s$  do not share a prime factor). By the proposition above,  $t$  is a root to some  $x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$ , and so plugging in  $t$  and clearing the powers of  $s$  from the denominators we have

$$r^n + r_{n-1}sr^{n-1} + \cdots + s^{n-1}r_1r + s^n r_0 = 0.$$

But then

$$s(r_{n-1}r^{n-1} + \cdots + s^{n-2}r_1r + s^{n-1}r_0) = -r^n,$$

and so any prime factor of  $s$  must divide  $r$  as well. By design,  $s$  does not share any primes with  $r$ , so  $s$  must be a unit, implying  $t \in R$ .  $\diamond$

A way to create examples of integrally closed domains is to take the widely-understood domain  $\mathbb{Z}$ , and a field containing  $\mathbb{Z}$ , and compute the "integral closure" of  $\mathbb{Z}$  inside the field.

**Example 53** *Let  $F$  be any field containing  $\mathbb{Z}$ . The collection of all elements  $\alpha \in F$  such that  $\alpha$  is a root to some monic polynomial in  $\mathbb{Z}[x]$  is integrally closed, and is called the integral closure of  $\mathbb{Z}$  in  $F$ .*

**Proof:** Let  $R$  be the collection of all the  $\alpha$ 's just described. As in the proof of the proposition,  $\alpha \in R$  if and only if the ring  $\mathbb{Z}[\alpha]$  is finitely generated as an abelian group. If  $\alpha, \beta \in R$ , then  $\alpha\beta$ , and  $\alpha + \beta$  both belong to  $S = \mathbb{Z}[\alpha, \beta] = (\mathbb{Z}[\alpha])[\beta]$ .

Something in  $S$  looks like

$$f_0(\alpha) + f_1(\alpha)\beta + \cdots + f_k(\alpha)\beta^k$$

for some  $f_j(x) \in \mathbb{Z}[x]$ . But  $\alpha, \beta \in R$  implies that there exists integers  $n$  and  $m$  such that any  $f(\alpha)$  can be generated by  $1, \alpha, \dots, \alpha^{n-1}$  over  $\mathbb{Z}$ , and any  $g(\beta)$  by  $1, \beta, \dots, \beta^{m-1}$  over  $\mathbb{Z}$ . It follows that any element in  $S$  can be generated by

$$1, \alpha^i\beta^j, \quad i < n, \quad j < m.$$

For example, for  $j > m$ , one can write  $\beta^j = \sum_{i=0}^m \ell_{ij}\beta^i$ , so that

$$\begin{aligned} f_0(\alpha) + f_1(\alpha)\beta + \cdots + f_k(\alpha)\beta^k &= \sum_{i_1=0}^m f_{i_1}(\alpha)\beta^{i_1} + \\ &\quad \sum_{j=m+1}^k [f_j(\alpha)\sum_{i=0}^m \ell_{ij}\beta^i]. \end{aligned}$$

Likewise we can express each  $f_i(\alpha)$  exclusively in terms of  $1, \alpha, \dots, \alpha^n$  using integer coefficients. Thus,  $S$  is finitely generated and so  $R$  is a subring of  $F$ .

If  $\gamma \in F$  is integral over  $R$ , then  $\gamma$  is a root to some  $x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$ . But  $\mathbb{Z}[r_j]$  is finitely generated for each  $j$ , from which it follows as above that

$$\mathbb{Z}[r_1, r_2, \dots, r_{n-1}]$$

is finitely generated over  $\mathbb{Z}$  as well. Hence

$$\mathbb{Z}[r_1, r_2, \dots, r_{n-1}, \gamma]$$

is finitely generated over  $\mathbb{Z}$  too and so  $\gamma \in R$  to begin with. That is,  $R$  is integrally closed.

Recall that an element  $\alpha$  of a field  $F$  containing  $\mathbb{Z}$  is called *algebraic over  $\mathbb{Z}$*  if there exists

$$0 \neq f(x) \in \mathbb{Z}[x] \text{ such that } f(\alpha) = 0.$$

In this case, the *minimal polynomial for  $\alpha$  over  $\mathbb{Z}$*  is the monic polynomial of smallest positive degree in  $\mathbb{Q}[x]$  having  $\alpha$  as a root. Note, if

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

has  $\alpha$  as a root, with  $a_n \neq 0$ , then so does

$$g(x) = x^n + b_{n-1} x^{n-1} + \cdots + b_0,$$

where  $b_j = a_j/a_n$ . While there are infinitely many choices for  $f(x)$ , recall that the monic  $g(x)$  is unique provided we are considering the polynomials of smallest degree. Furthermore, it is an easy exercise using long division to show that

$$h(x) \in \mathbb{Q}[x] \text{ with } h(\alpha) = 0 \iff g(x) \mid h(x) \text{ in } \mathbb{Q}[x].$$

◇

**Example 54** *Let  $\alpha$  be in a field  $F$  containing  $\mathbb{Z}$ . The following are equivalent:*

- (1)  $\alpha$  is integral over  $\mathbb{Z}$ .
- (2)  $\alpha$  is algebraic over  $\mathbb{Z}$  and the monic minimal polynomial for  $\alpha$  is in  $\mathbb{Z}[x]$ .
- (3)  $\alpha$  is algebraic but is not the root of some polynomial in  $\mathbb{Z}[x]$  with leading coefficient greater than 1 while the coefficients are relatively prime.

**Proof:** (1)  $\rightarrow$  (2) is a proof given in class (essentially). Let  $g(x) \in \mathbb{Z}[x]$  be the monic polynomial of smallest degree having  $\alpha$  as a root ( $\alpha$  integral) and let  $f(x) \in \mathbb{Q}[x]$  be the monic polynomial of smallest degree having  $\alpha$  as a root (clearly,  $\alpha$  is algebraic over  $\mathbb{Z}$ ). Performing long division, we can factor  $g(x) = f(x)h(x)$  for some monic polynomial  $h(x) \in \mathbb{Q}[x]$ .

There are positive integers  $m$  and  $n$  such that  $nf(x), mh(x) \in \mathbb{Z}[x]$ , and the gcd's of the coefficients of  $nf(x)$  and also of  $mh(x)$  are both 1 (for example, choose only the smallest  $n$  that will make  $nf(x) \in \mathbb{Z}[x]$ ). Then  $mng(x) = (nf(x))(mh(x))$ . Suppose there is a prime  $p$  dividing  $n$ . Considering the polynomials "mod  $p$ ", we obtain

$$0 = \overline{mng(x)} = \overline{nf(x)} \cdot \overline{mh(x)}.$$

(What we mean is that the coefficients of the polynomials are reduced modulo  $p$ , which is signified by the bar over the polynomials; formally, we have a ring epimorphism from  $\mathbb{Z}[x] \rightarrow \mathbb{Z}[x]/p\mathbb{Z}[x]$  given by  $y(x) \mapsto y(x) + p\mathbb{Z}[x]$ , and the isomorphism  $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$  affords the reduction of the coefficients).

But  $\mathbb{Z}_p[x]$  is an integral domain, and  $\overline{nf(x)} \cdot \overline{mh(x)} = 0$  implies either  $\overline{nf(x)} = 0$  or  $\overline{mh(x)} = 0$ . Neither is possible since the coefficients of  $nf(x)$  and of  $mh(x)$  are relatively prime. Therefore,  $m = 1$  and  $g(x) = f(x) \in \mathbb{Z}[x]$ .

(2)  $\rightarrow$  (3). For the moment just assume that  $\alpha$  is algebraic. If  $f(x) \in \mathbb{Q}[x]$  is the monic polynomial of least degree with  $\alpha$  as a root, then for some integer  $n$ ,  $nf(x)$  has the gcd of its coefficients equal to 1. Conversely, if  $f_0(x)$  is a polynomial of least degree in  $\mathbb{Z}[x]$  with the gcd of its coefficients equal to 1 and  $\alpha$  as a root, then  $f_0(x)/a \in \mathbb{Q}[x]$

is the monic polynomial for  $\alpha$  of least degree where  $a$  is the coefficient of the highest power of  $x$  in  $f_0(x)$ . It follows that, under the full force of (2),  $a$  has to be 1. Thus, every polynomial in  $\mathbb{Z}[x]$  with the gcd of its coefficients equal to 1 and having  $\alpha$  as a root must be monic.

(3)  $\rightarrow$  (1). Again, if  $f(x) \in \mathbb{Q}[x]$  is the monic irreducible polynomial for  $\alpha$ , and  $f(x) \notin \mathbb{Z}[x]$ , then we could multiply by an  $n > 1$  to obtain a polynomial  $nf(x) \in \mathbb{Z}[x]$  such that the gcd of the coefficients is 1. We conclude that  $f(x) \in \mathbb{Z}[x]$  and  $\alpha$  is integral over  $\mathbb{Z}$ .

◇

**Example 55** For example, the following algebraic elements are roots to the given polynomials:

$$\alpha = \sqrt{2 + \sqrt{3}} \iff f(x) = x^4 - 4x^2 + 1,$$

$$\beta = \sqrt[3]{2 + 3\sqrt{5}} \iff g(x) = x^6 - 4x^3 - 41,$$

$$\gamma = \sqrt{2 + \sqrt{3/5}} \iff h(x) = 5x^4 - 20x^2 + 17,$$

$$\delta = (\sqrt{2} + \sqrt{3}) / (\sqrt{1 + \sqrt{2}}) \iff k(x) = x^8 - 60x^6 + 134x^4 + 60x^2 + 1.$$

From this data and the previous example we find that  $\alpha, \beta, \delta$  are integral over  $\mathbb{Z}$  while  $\gamma$  is not. To see how to obtain the polynomials, let us consider obtaining  $k(x)$  for  $\delta$ . Square both sides and eliminate the denominator:

$$\delta^2(1 + 2 + 2\sqrt{2}) = 2 + 3 + 2\sqrt{6};$$

(legally) remove the square-root on the  $\sqrt{6}$  term:

$$(\delta^2(3 + 2\sqrt{2}) - 5)^2 = 4(6) = 24;$$

or;

$$(\delta^4(3 + 2\sqrt{2})^2 - 2(5)\delta^2(3 + 2\sqrt{2}) + 25 = 24;$$

or;

$$(\delta^4(9 + 8 + 12\sqrt{2}) - 20\delta^2\sqrt{2} = -1 + 30\delta^2;$$

isolate the remaining square-root;

$$\sqrt{2}(12\delta^4 - 20\delta^2) = -1 + 30\delta^2 - 17\delta^4;$$

square both sides;

$$2(144\delta^8 + 400\delta^4 - 480\delta^6) = 1 + 900\delta^4 + (17)^2\delta^8 - 1020\delta^6 - 60\delta^2 + 34x^4;$$

and since  $17^2 = 288 + 1 = 2(144) + 1$ , when we replace  $\delta$  with  $x$ , we obtain

$$k(x) = x^8 - 60x^6 + 134x^4 - 60x^2 + 1.$$

### 3.7 Localizations and Over-rings of $R$

**Definition:** If  $P$  is a prime ideal in an integral domain  $R$ , then

$$R_P = \left\{ \frac{r}{s} \mid r \in R, s \in R \setminus P \right\},$$

is an over-ring of  $R$  (inside  $Q$ ), called the *localization of  $R$  at  $P$* .

More generally, if  $\mathcal{S}$  is a nonempty *multiplicatively closed* subset of  $R$  that does not contain 0; that is,  $\mathcal{S} \neq \emptyset$ ,  $0 \notin \mathcal{S}$  and for every  $s_1, s_2 \in \mathcal{S}$ ,  $s_1s_2 \in \mathcal{S}$ , then one can form a *localization*,  $\mathcal{S}^{-1}(R)$ , where

$$\mathcal{S}^{-1}(R) = \left\{ \frac{r}{s} \mid s \in \mathcal{S}, r \in R \right\}.$$

Using the principal that  $\mathcal{S}$  is multiplicatively closed, we see immediately that  $\mathcal{S}^{-1}(R)$  is an over-ring of  $R$  (regard  $r \in R$  as  $\frac{sr}{s}$  where  $s \in \mathcal{S}$ ).

In the case of the localization of  $R$  at a prime  $P$ ,  $\mathcal{S}$  is taken to be  $R \setminus P$ . In one instance below we form a localization that is not at a prime ideal so we must consider the broader notion of localization,  $\mathcal{S}^{-1}(R)$  (though it is no harder).

**Proposition 56** *Let  $\mathcal{S}$  be a multiplicatively closed subset of  $R$ .*

- (a)  *$J$  is an ideal of  $\mathcal{S}^{-1}(R)$  if and only if  $J = \mathcal{S}^{-1}(I) = \left\{ \frac{a}{s} \mid s \in \mathcal{S}, a \in I \right\}$ , for some ideal  $I$  of  $R$ .*



(b)  $P'$  is a prime ideal of  $\mathcal{S}^{-1}(R)$  if and only if  $P' = \mathcal{S}^{-1}(P) = \{\frac{a}{s} \mid s \in \mathcal{S}, a \in P\}$ , for some prime ideal  $P$  of  $R$  such that  $P \cap \mathcal{S} = \emptyset$ .

**Proof:** (a). Given an ideal  $J$  of  $\mathcal{S}^{-1}(R)$ , we will consider  $I = R \cap J$ . If  $b \in J$ , then  $sb \in R \cap J = I$  for some  $s \in \mathcal{S}$ , so that  $b = \frac{sb}{s} \in \mathcal{S}^{-1}(I)$ . On the other hand,  $I \subseteq J$  implies that  $\mathcal{S}^{-1}(R)I = \mathcal{S}^{-1}(I) \subseteq J$ . Therefore,  $J = \mathcal{S}^{-1}(I)$ . Conversely,  $\mathcal{S}^{-1}(I) = \mathcal{S}^{-1}(R)I$  is an ideal of  $\mathcal{S}^{-1}(R)$  when  $I$  is an ideal of  $R$ , so the proof of (a) is complete.

(b). From (a) we note that  $P' = \mathcal{S}^{-1}(P)$  where  $P = P' \cap R$ . With this notation, we will show that

$$P' \text{ is prime in } \mathcal{S}^{-1}(R) \iff P \text{ is prime in } R \text{ with } P \cap \mathcal{S} = \emptyset.$$

If  $P'$  is prime in  $\mathcal{S}^{-1}(R)$ , then for any  $r_1, r_2$  in  $R$  (in particular),  $r_1 r_2 \in P'$  implies  $r_1 r_2 \in P' \cap R = P$ . We are given that  $r_1 \in P'$  (hence  $r_1 \in P' \cap R = P$ ) or  $r_2 \in P'$  (hence  $r_2 \in P' \cap R = P$ ), and because  $1 \notin P'$ ,  $1 \notin P$  so  $P$  is prime.

Conversely, if  $P = P' \cap R$  is a prime ideal of  $R$  with  $P \cap \mathcal{S} = \emptyset$ , then first of all,  $1 \notin P'$ , so  $P' \neq \mathcal{S}^{-1}(R)$ . If  $\frac{r_1 r_2}{s_1 s_2} \in P' = \mathcal{S}^{-1}(P)$  for some  $r_1, r_2 \in R$  and  $s_1, s_2 \in \mathcal{S}$ , then, multiplying by  $s_1 s_2$ ,  $r_1 r_2 \in P' \cap R = P$ , implies  $r_1 \in P \subseteq P'$  or  $r_2 \in P \subseteq P'$ . Hence  $\frac{r_1}{s_1} \in P' = \mathcal{S}^{-1}(P)$  or  $\frac{r_2}{s_2} \in P'$ .

Do you wonder which domains have the property that every overring  $S$  of  $R$  in  $Q$  must be a localization? This is what commutative ring theorists do, and the next section provides a partial answer.

## 3.8 Dedekind Domains

**Characterization of Dedekind Domains** The following are equivalent for an integral domain  $R$  that is not a field.

- (1)  $R$  is Dedekind (i.e., every proper ideal is a product of prime ideals).
- (2) Every nonzero ideal is invertible.
- (3)  $R$  is noetherian, every nonzero prime ideal is maximal, and  $R$  is integrally closed.

- (4)  $R$  is noetherian and for every maximal ideal  $M$  of  $R$ ,  $R_M$  is a local PID.

**Proof:**

(1)  $\rightarrow$  (2). Observe that a product of ideals  $I_1 I_2 \cdots I_n$  is invertible if and only if each  $I_j$  is invertible. Therefore, it is sufficient to show that every nonzero prime ideal is invertible. Let  $P$  be a nonzero prime ideal of  $R$ . Given  $0 \neq a \in P$ , by (1), we can write  $Ra = P_1 P_2 \cdots P_n$ . By the preceding remark, each  $P_j$  is invertible.

Since  $P_1 P_2 \cdots P_n = Ra \subseteq P$  and  $P$  is prime,  $P$  contains one of the invertible primes  $P_j$  (for some  $j$ ). In order to show that  $P$  is invertible, it is sufficient to show that  $P_j$  is maximal. Therefore, we have reduced the problem to showing that every invertible prime ideal is maximal, so without loss of generality, let  $P$  be an invertible prime (in other words, forget all the previous uses of letters).

In order to show that  $P$  is maximal we must show that if  $r \in R \setminus P$ , then  $P + Rr = R$ . Suppose that  $P + Rr \neq R$ . Then, by (1),  $P + Rr = P_1 P_2 \cdots P_n$  for some prime ideals  $P_1, P_2, \dots, P_n$ . Since  $r \notin P$ ,  $r^2 \notin P$  as well and we can write  $P + Rr^2 = Q_1 Q_2 \cdots Q_m$  for some prime ideals  $Q_1, Q_2, \dots, Q_m$ . Each  $P_j$  contains  $P_1 P_2 \cdots P_n$  and therefore must contain  $P$ . Likewise,  $Q_i$  contains  $P$  for all  $i$ . Hence, we can factor modulo  $P$ :

$$(P + Rr)/P = \bar{P}_1 \bar{P}_2 \cdots \bar{P}_n,$$

and

$$(P + Rr^2)/P = \bar{Q}_1 \bar{Q}_2 \cdots \bar{Q}_m,$$

where  $\bar{P}_j = P_j/P$ ,  $\bar{R} = R/P$ , and  $\bar{Q}_i = Q_i/P$ . Furthermore,

$$((P + Rr)/P)^2 = (P + Rr^2)/P,$$

so that

$$\bar{P}_1^2 \bar{P}_2^2 \cdots \bar{P}_n^2 = \bar{Q}_1 \bar{Q}_2 \cdots \bar{Q}_m.$$

Each  $\bar{P}_j$  and  $\bar{Q}_i$  is a prime ideal in the integral domain  $R/P$ ; for instance,  $\bar{R}/\bar{P}_j = (R/P)/(P_j/P) = R/P_j$  is an integral domain. Additionally, each  $\bar{P}_j$  and  $\bar{Q}_i$  is invertible because  $(P + Rr)/P$  and  $(P + Rr^2)/P$  are principal ideals of  $\bar{R}$  (the general element in  $(P + Rr^2)/P$  for example is the coset  $sr^2 + P$  for some  $s \in R$ ).

We can prove by induction on  $m$  that  $2n = m$  and after re-indexing,  $\bar{Q}_{2i-1} = \bar{Q}_{2i} = \bar{P}_i$  for  $i = 1, 2, \dots, n$ . We will show how reduction of the index works. Among each  $\bar{P}_i$  and  $\bar{Q}_j$ , choose one that is minimal with respect to containment. If it is a  $\bar{P}_i$ , then reorder so that  $i = 1$ . Then  $\bar{P}_1$  contains  $\bar{Q}_1\bar{Q}_2 \cdots \bar{Q}_m$  and hence must contain some  $\bar{Q}_j$  since  $\bar{P}_1$  is a prime ideal. Reorder so that  $j = 1$ , then cancel

$$\bar{P}_1\bar{P}_2^2 \cdots \bar{P}_n^2 = \bar{Q}_2 \cdots \bar{Q}_m.$$

If the original minimal prime was chosen as some  $\bar{Q}_j$ , reorder so that  $j = 1$ , and as before  $\bar{Q}_1$ , must contain some  $\bar{P}_i$ , which we take to be  $\bar{P}_1$ . Again, we cancel to obtain

$$\bar{P}_1\bar{P}_2^2 \cdots \bar{P}_n^2 = \bar{Q}_2 \cdots \bar{Q}_m.$$

In either case, induction applies (or, we can just repeat the argument as many times as necessary).

From  $\bar{Q}_{2i-1} = \bar{Q}_{2i} = \bar{P}_i$  for  $i = 1, 2, \dots, n$ , we see that  $Q_{2i-1} = Q_{2i} = P_i$  for  $i = 1, 2, \dots, n$ . Therefore,

$$(P + Rr)^2 = P_1^2 P_2^2 \cdots P_n^2 = Q_1 Q_2 \cdots Q_m = P + Rr^2.$$

So,  $P \subseteq P + Rr^2 = P^2 + Rr^2 + Pr$ . Given  $p \in P$ , write  $p = p_2 + sr^2 + p_1r$ , so that  $sr^2 = p - p_2 - p_1r \in P$ . Since  $r^2$  does not belong to the prime ideal  $P$ ,  $s \in P$  and so  $P \subseteq P + Pr^2 + Pr = P^2 + Pr = P(P + Rr)$ . But since  $P$  is invertible,  $R = P^{-1}P \subseteq P^{-1}P(P + Rr) = P + Rr \subseteq R$ . This contradiction, shows that indeed  $P + Rr = R$  (from the start) and therefore  $P$  is maximal as claimed.

(2)  $\rightarrow$  (3). For any proper ideal  $I$ ,

$$I^{-1}I = R \iff \sum_{i=1}^n b_i a_i = 1 \text{ for some } b_i \in I^{-1}, a_i \in I.$$

Under (2),  $I$  is invertible, and so  $a = \sum_{i=1}^n (ab_i)a_i$  for any  $a \in I$ , and since  $ab_i \in I$  for all  $i$ ,  $I$  is generated by  $a_1, a_2, \dots, a_n$ . I.e.,  $R$  is noetherian.

If  $P$  is a nonzero prime ideal, then  $P$  is contained in a maximal ideal  $M$ . Since  $M$  is invertible,  $M^{-1}P \subseteq R$ , and  $M(M^{-1}P) \subseteq P$ . Since  $P$  is prime, either  $M^{-1}P \subseteq P$  or  $M \subseteq P$ . If the former were to hold,  $M^{-1}P \subseteq P$ , then  $P$  invertible implies  $M^{-1} = M^{-1}PP^{-1} \subseteq PP^{-1} = R$ . But forming inverses is order reversing and  $M \subseteq R$  (so  $M^{-1} \supseteq$

$R$ ). Taken together, we have  $M^{-1} = R$ , from which  $MM^{-1} = M$ ; a contradiction. Therefore, the latter case holds;  $P = M$ .

Suppose  $S$  is a fractional over-ring of  $R$  in the quotient field  $Q$ ;  $R \subseteq S$  implies  $S^{-1} \subseteq R$  is an ideal and by (2),  $(S^{-1})^{-1}S^{-1} = R$ . But  $S$  is a ring, and  $(S^{-1})^{-1}S^{-1} = R$  is an  $S$ -module, so  $S \cdot R \subseteq R$ , and  $S = R$ .

(3)  $\rightarrow$  (4). Recall that  $R_M = \{\frac{r}{s} \mid r, s \in R, s \notin M\}$ . By Proposition 11, the ideals of  $S = R_M$  are *extended*; i.e., the ideals of  $S$  must be of the form  $I \cdot R_M = \{\frac{r}{s} \mid r \in I, s \in R \setminus M\}$  for some ideal  $I$  of  $R$ . Furthermore, the prime ideals of  $S = R_M$  are of the form  $P \cdot R_M$  where  $P$  is a prime ideal contained in  $M$ . Therefore, from (3), every ideal of  $S$  is finitely generated (since the ideals of  $R$  are finitely generated), with 0 and  $N = M \cdot R_M$  as the only prime ideals of  $S$ .

We will first show that the maximal ideal of  $S$  is principal. By homework problem number 2 from the current set, it suffices to show that  $N$  is invertible (relative to  $S$ ). But, in a manner applied earlier,  $N^{-1} = \{t \in Q \mid tN \subseteq S\}$ , contains  $S$ , and so  $N \subseteq N^{-1}N \subseteq S$ . If  $N^{-1}N = N$ , then  $N^{-1}N^{-1}N = N^{-1}N = N$ , implying that  $N^{-1}N^{-1} = N^{-1}$ ; i.e.,  $T = N^{-1}$  is a fractional over-ring of  $S$ . But, we claim that  $S$  is integrally closed; a property inherited from  $R$ .

If  $S[t]$  is an over-ring of  $S$ , then there exists an equation  $t^n + s_{n-1}t^{n-1} + \cdots + s_0 = 0$  where  $s_j \in S$  and  $n \geq 1$ . Let  $r \in R \setminus M$  be such that  $rs_j \in R$  for all  $j$ . Then  $r^n(t^n + s_{n-1}t^{n-1} + \cdots + s_0) = (rt)^n + rs_{n-1}(rt)^{n-1} + \cdots + r^n s_0 = 0$ , implying that  $rt$  is integral over  $R$ . Therefore,  $rt = a \in R$  and consequently  $t = ar^{-1} \in S$ . Therefore,  $S$  is integrally closed by Proposition 6, and so  $N^{-1} = S$ .

We will show in this paragraph that  $N^{-1}$  is in fact unequal to  $S$ . Fix  $0 \neq y \in N$  and consider the cyclic  $S$ -module

$$C = \langle \frac{1}{y} + S \rangle$$

inside  $Q/S$ . Observe that  $C \neq 0$ , because  $N$  does not contain a unit of  $S$ . The collection  $\mathcal{I}$  of all ideals  $I$  of  $S$  such that  $I = \{s \in S \mid s(\frac{1}{y} + S) = 0\}$ , for some fixed  $t \in S$  such that  $\frac{t}{y} \notin S$ . Since  $S$  is noetherian, unions of chained ideals of  $S$  stabilize and so  $\mathcal{I}$  contains maximal members. Let  $P$  be maximal in  $\mathcal{I}$ , say  $P = \text{ann}_S x + S$  for some  $x = \frac{t}{y} \in Q \setminus S$

where  $t \in S$ , and suppose  $rs \in P$ , for some  $r, s \in S$  with  $r \notin P$ . Then,  $r(x+S) \neq 0$  but  $(P+(s))(rx+S) = 0$ . This implies  $P = P+(s)$  and so  $s \in P$  and  $P$  is prime. But  $P \neq 0$  since  $0 \neq Sy \in \mathcal{I}$ , therefore  $P = N$ . That is, there exists an element  $q = \frac{t}{y} \in Q \setminus S$  such that  $Nq \in S$  and so  $q \in N^{-1} \setminus S$ .

Therefore,  $N^{-1}N = S$  is the only possibility, and since  $S$  is local, by homework problem 2,  $N$  must be principal. Write  $N = (b)$  for some  $b \in S$ . Now,  $S$  is a noetherian domain with principal maximal ideal  $N = (b)$  and  $N$  and  $0$  are the only primes. We need to show that  $S$  is a PID.

Our first claim is that  $\bigcap_{k=1}^{\infty} N^k = 0$ . If we set  $I = \bigcap_{k=1}^{\infty} N^k$  then clearly  $bI = I$ : check that if  $a = bc$ , then  $a \in (b^n)$  if and only if  $c \in (b^{n-1})$ ; so  $a \in (b^n)$  for all  $n$  if and only if  $c \in (b^n)$  for all  $n$ . Thus,  $\frac{1}{b}I = I$ , and  $I$  is an ideal in  $S[\frac{1}{b}] = Q$ . To see that  $S[\frac{1}{b}] = Q$  observe that  $S[\frac{1}{b}]$  is a localization of  $S$  using the set  $\{b^j\}_{j=1}^{\infty}$ , and by Proposition 11,  $S[\frac{1}{b}]$  has no prime ideals save  $0$ ; consequently,  $S[\frac{1}{b}]$  must be a field; and consequently, the field  $Q$ . But having  $I$  a module over  $Q$  can only happen when  $I = 0$ . Thus,  $\bigcap_{k=1}^{\infty} N^k = 0$ .

Let  $J$  be a proper ideal of  $S$ . Then  $J \subseteq N$ . Since  $\bigcap_k (b^k) = 0$ , there is a least positive integer such that  $J \subseteq (b^k)$  but  $J$  is not contained in  $(b^{k+1})$ . If  $a \in J \setminus (b^{k+1})$ , write  $a = ub^k$  where  $u \in R$ . Then, obviously,  $u \notin (b)$ , implying that  $u$  is a unit (since  $S$  is local with maximal ideal  $(b)$ ). Therefore,  $J = (b^k)$  and  $S$  is a PID.

(4)  $\rightarrow$  (1). Let  $P$  be a prime ideal of  $R$  that is contained in a maximal ideal  $M$ ,  $P \neq M$ . Then, from Proposition 11,  $P \cdot R_M$  is a prime ideal in the ring  $R_M$ . But,  $R_M$  is a local PID so the only prime ideals are  $0$  and  $M \cdot R_M$ . Also,

$$r \in M \setminus P \implies r \in (M \cdot R_M) \setminus (P \cdot R_M) \quad (\text{check!})$$

and so  $P$  must be zero. Hence any nonzero prime ideal of  $R$  is maximal.

By the Primary Decomposition Theorem (to follow), every ideal  $I \neq 0$  has a (reduced) primary decomposition:

$$I = I_1 \cap I_2 \cap \cdots \cap I_n,$$

where the  $I_j$ 's are primary ideals associated with distinct primes (maximal ideals)  $M_j$ 's. When the radicals,  $M_1, M_2, \dots, M_n$  are coprime in

pairs (i.e.,  $M_i + M_j = R$  for all  $i \neq j$ ), the intersection can be replaced by the product:

$$I = I_1 \cdot I_2 \cdots I_n \quad (\text{see Corollary 11 below}).$$

Once we show that the primary ideal  $I_j$  must be equal to  $M_j^{n_j}$  for some positive integer  $n_j$ , the proof will be complete.

Let  $J$  be any nonzero primary ideal and let  $M = \text{rad}(J)$ . Note that  $M$  is a maximal ideal. Since  $R_M$  is a local PID,  $J \cdot R_M = M^n \cdot R_M$  for some positive integer  $n$ . We claim that  $J = M^n$ . Note, that  $M^n$  too is primary by Proposition 14.

We claim that because  $J$  is primary,

$$J = R \cap (J \cdot R_M),$$

where  $M = \text{rad}(J)$ . Once this has been established we can show too that  $M^n = R \cap (M^n \cdot R_M)$ , since  $M^n$  is primary with radical  $M$  as well. This leads to

$$J = R \cap (J \cdot R_M) = R \cap (M^n \cdot R_M) = M^n,$$

as desired.

Clearly,  $J \subseteq R \cap (J \cdot R_M)$ . Suppose  $a \in R \cap (J \cdot R_M) \setminus J$ . Then, for some  $r \in R \setminus M$ ,  $ra \in J$ . But  $J$  is primary and  $a \notin J$  implies  $r^m \in J$  for some  $m \geq 1$ . However,  $r \notin M$  implies  $r^m \notin M$  for any  $m$  since  $M$  is prime; a contradiction. Therefore, a primary ideal must be  $M^n$  for some maximal ideal  $M$  and integer  $n$ , completing the proof.

Dedekind domains have ample structure with which we can discover the wonders of ring theory. Many of the assertions that were made during the course of the proof no longer hold once we leave the structure of Dedekind domains.

**Example 57** Let  $R = F[x, y]$  where  $F$  is a field. The quotient field  $Q$  of  $R$  is then  $F(x, y) = \{ f(x, y)/g(x, y) \mid f(x, y), g(x, y) \in R, g(x, y) \neq 0 \}$ . The ideal generated by  $x$  and  $y$ ,  $M = (x, y)$ , is maximal. But if  $q(x, y) \in M^{-1}$ , then  $q(x, y) \cdot x \in R$  implies  $q(x, y) = \frac{h(x, y)}{x}$  (recall that  $R$  is a UFD). But then  $q(x, y) \cdot y \in R$ , implies  $x \mid h(x, y)$  so that  $q(x, y) \in R$ . That is,

$$M^{-1} = R,$$

unlike the case when the domain is noetherian such that every nonzero prime ideal is maximal.

A class of domains receiving the most attention these days is the class of Prüfer domains. A domain is called Prüfer if every finitely generated ideal is invertible. There are numerous examples of non-noetherian Prüfer domains. Also, it can be shown that a maximal ideal  $M$  of a Prüfer domain is infinitely generated if and only if  $M^2 = M$ , and there are many example of such rings.

**Example 58** *The following conditions are equivalent for an integral domain  $R$ :*

- (1)  $R$  is Prüfer.
- (2) For all ideals  $I, J, K$  of  $R$ ,  $I(J \cap K) = (IJ) \cap (IK)$ .
- (3) For all ideals  $I, J, K$  of  $R$ ,  $I \cap (J + K) = (I \cap J) + (I \cap K)$ .
- (4) Every over-ring  $S$  of  $R$  in  $Q$  is Prüfer.
- (5) For every prime ideal  $P$  of  $R$ ,  $R/P$  is Prüfer.

It can be shown for a Dedekind domain  $R$ , that every over-ring  $S$  of  $R$  in  $Q$  is of the form

$$S = \bigcap_{M \in \mathcal{M}} R_M,$$

where  $\mathcal{M}$  is a collection of maximal ideals of  $R$ , and  $S$  is like-wise Dedekind.

### EXERCISES of SECTION 3:

1. A domain  $R$  is called a *divisorial* domain if every proper ideal  $I$  satisfies  $(I^{-1})^{-1} = I$ .
  - (i) Show that Dedekind domains are divisorial.
  - (ii) If  $R$  is divisorial and  $M$  is a maximal ideal of  $R$ , show that  $M^{-1}/R \cong R/M$ .
2. (i) Show that a PID is Dedekind.

- (ii) Show that if every maximal ideal in a Dedekind domain  $R$  is principal, then  $R$  is a PID.
- (iii) Find Dedekind domain that is not a PID. Hint: consider  $\mathbb{Z}[\sqrt{-5}]$ .

### 3.9 Primary Decompositions of Ideals

We have seen that any ideal in a PID is a product of primary ideals (i.e., powers of a prime ideal). In order to establish this for more general domains, we need to weaken the definition of primary.

**Definition:** An ideal  $I$  of an integral domain  $R$  is called *primary*, if  $I \neq R$  and whenever  $rs \in I$  with  $r \notin I$ , there is an  $n \geq 1$  such that  $s^n \in I$ .

**Definition:** The *radical of an ideal*  $I$ ,  $\text{rad}(I)$ , is the ideal consisting of the elements  $r \in R$  such that  $r^n \in I$  for some  $n \geq 1$ .

Sometimes  $\text{rad}(I)$  is called the *nilradical* of  $I$ , and sometimes it is written as  $\sqrt{I}$ .

**Proposition 59** *Given an ideal  $I \neq R$  of the noetherian domain  $R$ , one can say the following:*

- (i) *The radical of  $I$ ,  $\text{rad}(I)$ , is the intersection of all prime ideals containing  $I$ .*
- (ii) *There is an  $n \geq 1$  such that  $\text{rad}(I)^n \subseteq I$ .*
- (iii) *If  $I$  is primary, then  $\text{rad}(I)$  is prime.*
- (iv) *If  $\text{rad}(I)$  is a maximal ideal,  $I$  is primary.*

Item (i) prompts the phrase, *prime radical*, for  $\text{rad}(I)$ . **Proof:** (i). Let  $J = \bigcap \{P \mid I \subseteq P\}$  ( $P$  will always represent a prime unless otherwise indicated). If  $r \in \text{rad}(I)$ , then  $r^n \in I$  for some  $n \geq 1$ . But then, for any  $P \supseteq I$ ,  $r^n \in P$  and since  $P$  is prime,  $r \in P$ . I.e.,  $\text{rad}(I) \subseteq J$ . Conversely, if  $r \in J$ , but  $r^n \notin I$  for any  $n$ , then consider the situation with the multiplicatively closed set  $\mathcal{S} = \{r^n\}_{n=1}^{\infty}$ . We have  $\mathcal{S} \cap I = \emptyset$  and so  $\mathcal{S}^{-1}(I)$  is a proper ideal of  $\mathcal{S}^{-1}(R)$ . However, there are no primes



in  $\mathcal{S}^{-1}(R)$  containing  $\mathcal{S}^{-1}(I)$  since  $r$  belongs to every  $P$  containing  $I$ ; a contradiction. Thus,  $r^n \in I$  for some  $n$  and  $J \subseteq \text{rad}(I)$ .

(ii). Since  $R$  is noetherian,  $\text{rad}(I)$  is finitely generated; say  $\text{rad}(I)$  is generated by  $r_1, r_2, \dots, r_k$ . For each  $j$  there exists an  $n_j$  such that  $r_j^{n_j} \in I$ . Set  $n = \sum_j n_j$ . Given  $r = \sum_j a_j r_j \in \text{rad}(I)$ , we will convince ourselves that  $r^n \in I$  by considering the case of two  $r_j$ 's:

$$r^n = (a_1 r_1 + a_2 r_2)^n = \sum_{i=0}^n c_{n,i} (a_1 r_1)^i (a_2 r_2)^{n-i} = \sum_{i=0}^n c_{n,i} (a_1^i a_2^{n-i}) [r_1^i r_2^{n-i}],$$

where  $c_{n,i}$  is the (integral) number of combinations of  $n$  things taken  $i$  at a time without regard to order. Observe that when  $i < n_1$ ,  $n-i > n_2$  and so  $r_2^{n-i} \in I$  and when  $i \geq n_1$ ,  $r_1^i \in I$ . Thus

$$r^n \in I.$$

That is,  $\text{rad}(I)^n \subseteq I$ . The case when  $k > 2$  is analogous, one must use the multinomial expansion formula rather than the binomial expansion formula.

(iii). Suppose  $rs \in \text{rad}(I)$  for some  $r, s \in R$  with  $r \notin \text{rad}(I)$ . By the definition of  $\text{rad}(I)$ , there is an  $n \geq 1$  such that  $r^n s^n = (rs)^n \in I$ . But  $I$  is primary, and  $r^n \notin I$  (since  $r \notin \text{rad}(I)$ ), implies that some power of  $s^n$ ,  $s^{mn} \in I$ . That is,  $s \in \text{rad}(I)$ . Therefore,  $\text{rad}(I)$  is prime.

(iv). Let  $I$  be an ideal such that  $\text{rad}(I) = M$  is maximal and suppose that  $ab \in I$ , with  $a \notin I$ . By (ii), there is an  $n \geq 1$  such that  $M^n \subseteq I$ , so if we show that  $b \in M$ , then we will have  $b^n \in I$ . Suppose  $b \notin M$ . Then  $M + (b) = R$ . Consider

$$(M + (b))^n = M^n + bM^{n-1} + \dots + b^{n-1}M + (b^n) = R.$$

If we multiply this by  $a$  we obtain

$$aM^n + (ab)M^{n-1} + \dots + (ab^{n-1})M + (ab^n) = aR.$$

But the left-hand-side is contained in  $I$  while the right-hand-side is not; a contradiction. Thus,  $b \in M$  and so  $b^n \in I$  as required for a primary ideal.

**Corollary 60** *If  $J$  is a primary ideal in a noetherian domain and  $P = \text{rad}(J)$ , then for some positive integer  $n$ ,  $P^n \subseteq J$ .*

**Example 61** Let  $R = F[x, y]$  where  $F$  is a field, and observe that  $M = (x, y)$  is a maximal ideal of  $R$ . Then each of the ideals given below is primary with radical  $M$ :

$$(x^2, y), (x^2, y^2), (x^2, y^3), (x^3, y^3), \dots$$

Observe that a power of  $M$  is primary but does not appear in this list. Check for  $M$  or  $M^2 = (x^2, xy, y^2)$  for example.

Given any module  $B$ , we can consider the *annihilator ideal* associated with an element  $b \in B$

$$\text{ann}_R b = \{r \in R \mid rb = 0\}.$$

Of course  $\text{ann}_R b$  may be 0 or may be  $R$ , but for certain modules  $B$ ,  $\text{ann}_R b$  will always be a proper ideal when  $b \neq 0$ . For example, when  $B = R/I$  for a proper ideal  $I$  of  $R$ . Then, for any  $0 \neq b \in B = R/I$ ,  $\text{ann}_R b$  is a proper ideal, properly containing  $I$ .

Let us restrict ourselves to torsion (or bounded modules  $B$ ), and assume that for any  $b \in B$  there exists an  $0 \neq r \in R$  such that  $rb = 0$ . The *associated primes* of  $B$  are the prime ideals  $P$  of  $R$  such that

$$P = \text{ann}_R b,$$

for some  $b \in B$ . With  $\mathcal{A} = \{J \mid J = \text{ann}_R b \text{ for some } 0 \neq b \in B\}$ , the maximal elements in  $\mathcal{A}$  are associated primes of  $B$ .

To see this, let  $P$  be a maximal element in  $\mathcal{A}$  and write  $P = \text{ann}_R b$  for some  $b \in B$ . If  $rs \in P$  but  $r \notin P$ , then  $rb \neq 0$ , but

$$(P + (s)) \cdot rb \subseteq Pb = 0.$$

Thus,  $(s) \subseteq P$ , and  $P$  is prime.

**Proposition 62** Let  $I$  be a proper ideal of the noetherian domain  $R$ . Then  $R/I$  has a single associated prime  $P$  if and only if  $I$  is primary with radical  $P$ .

**Proof:** Assume that  $I$  is primary with radical  $P$ , and let  $P'$  be an associated prime of the (bounded) module  $R/I$  ( $a \cdot R/I = 0$  for some

(any) nonzero  $a \in I$ ). Say  $P' = \text{ann}_R r + I$  for some  $r \in R \setminus I$ , and observe that  $I \subseteq P'$ . Suppose there exists an  $a \in P' \setminus P$ . Then  $ar \in I$  and  $r \notin I$  implies  $a^n \in I \subseteq P$  for some  $n$ , and because  $P$  is prime  $a \in P$ ; i.e.,  $P' \subseteq P$ . But  $I$  contains a power of its radical  $P$ , so  $P^m \subseteq I \subseteq P'$  implies  $P = P'$ .

Conversely, suppose  $R/I$  has the lone associate prime  $P$ . Note that  $P \supseteq I$ . Suppose  $rs \in I$  with  $r \notin I$ . Then  $b = r + I \neq 0$  and the annihilator of  $b$  is contained in a maximal element in the set of all annihilators of  $R/I$ . I.e.,  $P(r+I) = 0$  and also  $(P+(s))(r+I) = 0$ . To complete the proof it is enough to show that every prime  $P'$  containing  $I$ , contains  $P$  (for then  $P = \text{rad}(I)$  by Proposition 14, and by Corollary 15,  $s^n \in P^n \subseteq I$  as needed).

Suppose there exists an  $a \in P \setminus P'$ . Since  $I \subseteq P'$ ,  $a \notin I$  and so  $a + I \neq 0$ . But then  $P$  is the unique maximal annihilator, and so  $Pa \subseteq I \subseteq P'$ . In particular,  $a^2 \in P'$ ; a contradiction. Thus  $P \subseteq P'$  and the proof is complete.

There are a lot of different proofs of the result that every ideal has a *primary decomposition*, that is, for any proper ideal  $I$ , there exist primary ideals  $I_1, I_2, \dots, I_n$  such that

$$I = I_1 \cap I_2 \cap \cdots \cap I_n.$$

We opt for the direct approach, though this is not the traditional approach.

An ideal  $J$  that is different from  $R$  is called *irreducible*, if  $J = J' \cap J''$  for some ideals  $J', J''$ , implies one of  $J'$  or  $J''$  must be  $J$  (sound familiar?). An intersection  $I = J_1 \cap J_2 \cap \cdots \cap J_n$  is called *irredundant* if for no proper subset  $U$  of  $\{1, 2, \dots, n\}$  is  $I = \bigcap_{j \in U} J_j$ . So  $J$  is irreducible if  $J$  is not the irredundant intersection of two ideals  $J'$  and  $J''$ .

**Theorem 63** *Let  $I$  be a proper ideal in a noetherian domain  $R$ . Then, there exists primary ideals  $I_1, I_2, \dots, I_k$  such that*

$$I = I_1 \cap I_2 \cap \cdots \cap I_k.$$

**Proof:** We claim that any proper ideal  $I$  can be expressed as

$$I = I_1 \cap I_2 \cap \cdots \cap I_k,$$

where the ideals  $I_1, I_2, \dots, I_n$  are irreducible. Perhaps you can do this yourselves? While this is straightforward, we can shorten the process by using a slight technique.

If some proper ideal is not a finite intersection of irreducible ideals, then let  $\mathcal{I}$  be the nonempty collection of all such ideals. Since  $R$  is noetherian,  $\mathcal{I}$  contains a maximal member, call it  $J$ , by Proposition 1. Every ideal properly containing  $J$  must be an intersection of irreducibles.

If  $J$  is irreducible, then  $J$  is an intersection of irreducibles. Otherwise,  $J = J_1 \cap J_2$  with  $J_1, J_2$  both properly containing  $J$ . But then  $J_1, J_2$  are intersections of irreducibles, and so is  $J = J_1 \cap J_2$ ; a contradiction. Therefore  $\mathcal{I}$  is empty.

It remains to show that irreducible ideals are primary. Let  $J$  be an irreducible ideal and consider  $R/J$ . If  $R/J$  has two associated prime,  $P_1$  and  $P_2$ , then there exist elements  $r_1, r_2 \in R$  such that  $P_i = \text{ann}_R r_i + J$ . Note that this last condition implies that for  $J_i = Rr_i + J$ ,  $J_i/J \cong R/P_i$  for  $i = 1, 2$ . Since  $J_1, J_2$  properly contain  $J$ ,  $J_1 \cap J_2 = J$  is impossible. Let  $x \in J_1 \cap J_2$  but  $x \notin J$ . The element  $x + J_1$  corresponds to a nonzero element  $r + P_1$  in  $R/P_1$ . But  $P_2(x + J) = 0$  implies that  $P_2$  annihilates  $r + P_1$  and so  $P_2 r \subseteq P_1$ . This is impossible because  $r \notin P_1$  and  $P_2$  and  $P_1$  are distinct primes. Thus,  $R/J$  has only 1 associated prime and by Proposition 17,  $J$  is primary.

**Corollary 64** *If  $I_1, I_2, \dots, I_n$  are primary ideals whose radicals are the distinct maximal ideals  $M_1, M_2, \dots, M_n$ , then*

$$I_1 \cap I_2 \cap \dots \cap I_n = I_1 \cdot I_2 \cdot \dots \cdot I_n.$$

**Proof:** Each of the primary ideals  $I_j$  contains a power of their radical  $M_j$  by Corollary 8, so there exists a  $k \geq 1$  such that  $M_j^k \subseteq I_j$  for all  $j$ . Note that

$$M_i^k + \prod_{j \neq i} M_j^k = R$$

for all  $i$ . To see this observe that if  $M$  is a maximal ideal containing  $M_i^k + \prod_{j \neq i} M_j^k$  then  $M$  contains  $M_i$  and  $M$  contains some  $M_j$  with  $j \neq i$  (since  $M$  is prime), which is impossible. It follows that for any  $i$ ,

$$I_i + \prod_{j \neq i} I_j = R.$$

We have  $I_1 I_2 \cdots I_n \subseteq I_1 \cap I_2 \cap \cdots \cap I_n$ , and we can go the other way by induction on  $n$ . The inductive step is handled by multiplying both sides of the above equation by  $I_1 \cap I_2 \cap \cdots \cap I_n$ :

$$\begin{aligned} I_1 \cap I_2 \cap \cdots \cap I_n &= [I_i \cap \cap_{j \neq i} I_j](I_i + \prod_{j \neq i} I_j) = \\ [I_i \cap (\prod_{j \neq i} I_j)](I_i + \prod_{j \neq i} I_j) &= [I_i \cap (\prod_{j \neq i} I_j)]I_i + [I_i \cap (\prod_{j \neq i} I_j)]\prod_{j \neq i} I_j \\ &\subseteq I_1 I_2 \cdots I_n. \end{aligned}$$

### 3.10 Exercises

1. Show that any non-zero element  $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$  in the ring of Hamiltonian Quaternions  $\mathbb{H}$  has a multiplicative inverse in  $\mathbb{H}$ .
2. Determine all zero-divisors in the ring  $R$  of all  $2 \times 2$  matrices whose entries lie in  $\mathbb{R}$ .
3. (a) Determine all zero-divisors in  $\mathbb{Z}_{(n)}$ .  
 (b) Determine all units in  $\mathbb{Z}_{(n)}$ .  
 (c) Conclude that any non-zero element of  $\mathbb{Z}_{(n)}$  is either a zero-divisor or is a unit.
4. Give an example of a ring  $R$  and a non-zero element  $r \in R$  for which  $r$  is neither a zero-divisor nor a unit.
5. Show that if  $F$  is a field, then  $R = F[x]$  is a PID. Hint: use the degree function  $\deg : F[x] \rightarrow \mathbb{N}$  and the division algorithm in  $F[x]$  to show that if  $f(x) \neq 0$  is an ideal of smallest degree in an ideal  $I \neq 0$ , that  $I = (f(x))$ .
6. Suppose  $\alpha \in \mathbb{C}$  is the root to a monic polynomial  $f(x) \in \mathbb{Z}[x]$ , and put  $R = \mathbb{Z}[\alpha]$ ; the collection of all polynomials in  $\mathbb{Z}$  evaluated at  $\alpha$ .  
 (a) Show that  $R$  is an integral domain that is finitely generated over  $\mathbb{Z}$ .

- (b) Argue that the quotient field of  $R$  is  $\mathbb{Q}[\alpha]$ , and that for any  $\beta \in R$ , there exists an integer  $k \neq 0$  such that  $k\beta^{-1} \in R$ .
- (c) Using (b), argue that any nonzero ideal of  $R$  contains an integer, and so  $R/I$  is finite.
- (d) Using (c) conclude that  $R$  is a noetherian domain such that every non-zero prime ideal is maximal.
7. Let  $R$  be a UFD with quotient field  $Q$ , and let  $f(x) \in R[x]$ .
- (a) Show that there is an element  $r \in R$  and a polynomial  $g(x) \in R[x]$ , such that  $f(x) = rg(x)$  and the gcd of the coefficients of  $g(x)$  is 1. ( $r$  is called the *content of  $f$*  and we write  $c(f) = r$ ).
- (b) Show that if  $f(x) = g(x)h(x)$  with  $g(x), h(x) \in Q[x]$ , then there exists polynomials  $g_1(x), h_1(x) \in R[x]$  each having content 1 such that  $ag(x) = g_1(x)$  and  $bh(x) = h_1(x)$ , and  $abf(x) = g_1(x)h_1(x)$ , for some nonzero  $a, b \in R$ .
- (c) With the notation of part (b), show that if  $c(f) = 1$ , that  $ab = 1$ .
- (d) Conclude that  $f(x) \in R[x]$  is irreducible in  $R[x]$  if and only if  $f(x)$  is irreducible in  $Q[x]$ .
8. Let  $R$  be a UFD. Using Problem 3. show that  $R[x]$  is a UFD.
9. The intersection of all maximal ideals of  $R$  is called the *Jacobson radical* of  $R$ . Suppose  $J = \bigcap_M \text{max} M$ .
- (a) Show that  $a \in J$  if and only if for every  $r \in R$ ,  $1 + ra$  is a unit. Hint:  $\Rightarrow ra \in J$  for every  $r \in R$ , and so  $1 + ra$  must be a unit.  $\Leftarrow a \notin M$  for some  $M$  implies  $M + (a) = R$  and  $1 - ra \in M$  for some  $r \in R$ .
- (b) Deduce a version of Nakayama's Lemma: If  $K$  is a finitely generated module, that is,  $K = Rx_1 + Rx_2 + \cdots + Rx_n$ , such that  $JK = K$ , then  $K = 0$ . Hint: Assume  $n$  is the minimal number of generators required to generate  $K$ ; write  $x_1 = a_1x_1 + \cdots + a_nx_n \in JK = K$  with  $a_j \in J$  for all  $j$ . Invert  $1 - a_1$ .

- (c) Prove **Nakayama's Lemma**: Let  $B$  be a finitely generated module, and let  $A$  be a submodule such that  $B = A + JB$ . Then  $B = A$ . Hint:  $K = B/A$  is finitely generated and satisfies  $K = JK$ .
10. The *Hilbert Basis Theorem* asserts that if  $R$  is noetherian, then so is  $R[x]$ . Assuming  $R$  is a noetherian domain, show that  $R[x]$  is noetherian. Hint: If  $J$  is an ideal in  $R[x]$ , let  $I_n$  be the ideal of elements that occur as coefficients of  $x^n$  in some polynomial in  $J$ . Observe that  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ . Use this to pick generators for  $J$ .
11. Show that any non-zero element of  $F = \mathbb{Q}[\sqrt{d}]$  is a unit.
12. Let  $R = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$  with  $d$  a square-free integer.

(a) Show that the function

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

defined by  $N(a + b\sqrt{d}) = a^2 - db^2$ , is multiplicative in that  $N(\alpha\beta) = N(\alpha)N(\beta)$  for any  $\alpha, \beta \in R$ .

- (b) Show that  $0 \neq a + b\sqrt{d} \in R$  is a unit of  $R$  if and only if  $N(a + b\sqrt{d}) = \pm 1$ .
13. This exercise examines the ring  $R = \mathbb{Z}[\sqrt{10}]$ .
- (a) Show that  $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$  are all non-units.
- (b) Show that  $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$  are all irreducible. Hint: Use  $N$  as defined in Exercise 3.12.
- (c) From
- $$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$$
- deduce that 2 is not a unit multiple of either  $4 + \sqrt{10}$ , or  $4 - \sqrt{10}$ .
14. Show that  $R = \mathbb{Z}[\sqrt{10}]$  is not a UFD. Hint: use Exercise 13.

15. Regarding  $R = \mathbb{Z}[\sqrt{-5}]$ , show that the ideal  $I = (2, 1 + \sqrt{-5})$  is not principal.
16. Determine the number of units in the respective rings:
- $R = \mathbb{Z}[\sqrt{10}]$
  - $R = \mathbb{Z}[\sqrt{5}]$
  - $R = \mathbb{Z}[\sqrt{d}]$  with  $d < 0$ ,  $d \neq -1$ .
  - $R = \mathbb{Z}[\sqrt{-1}]$ .
17. Show that if  $\alpha \in R = \mathbb{Z}[\sqrt{d}]$  with  $N(\alpha) = \pm p$ , an integral prime, then  $\alpha$  is irreducible. Must  $\alpha$  be prime in  $R$ ?
18. Show that if  $F$  is a field, then every irreducible element of  $R = F[x]$  is prime.
19. Let  $F$  be a field and  $f(x) \in F[x]$  have degree 2 or 3. Show that  $f(x)$  is irreducible if and only if  $f(x)$  has no roots in  $F$ .
20. For the following fields, find at least 3 irreducibles in  $F[x]$ .
- $F = \mathbb{Z}_{(p)}$  for your choice of  $p$ .
  - $F = \mathbb{Q}$ .
  - $F = \mathbb{R}$ .

21. Given  $n$  and  $m$ , express

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \text{ and } m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

where  $e_i, f_i$  are non negative integers (but may be zero). Show that the greatest common divisor  $(n, m)$  and least common multiple  $[n, m]$  of  $m, n$  are given by

$$(n, m) = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} \text{ and } [n, m] = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$$

where  $s_i$  is the minimum of  $e_i, f_i$  and  $t_j$  is the maximum of  $e_j, f_j$ .

22. A non-empty  $I \subseteq R$  is an ideal if and only if the cosets  $R/I = \{ r + I \mid r \in R \}$  forms a ring under the inherited operations  $r + I + s + I = (r + s) + I$  and  $(r + I)(s + I) = (rs) + I$ .



23. Let  $J$  be an ideal in a commutative ring  $R$ .
- (a)  $J$  is prime if and only if  $R/J$  is an integral domain.
  - (b)  $J$  is maximal if and only if  $R/J$  is a field.
24. An *Algebraic Number Field* is a field  $F$  that is finite dimensional over  $\mathbb{Q}$ . Prove that  $F$  is an algebraic number field if and only if  $F = \mathbb{Q}[\alpha]$  where  $\alpha \in \mathbb{C}$  is a root to a polynomial  $f(x) \in \mathbb{Q}[x]$ .
25. A *Number Ring* is the integral closure of  $\mathbb{Z}$  inside an algebraic number field. Show that a number ring  $R$  is free as an abelian group.
26. Let  $R$  be a Dedekind domain. Show that  $R$  is a PID if and only if  $R$  is a UFD.
27. Address the issues of which of the following are integral, algebraic, or transcendental.
- (a)  $\sqrt[n]{q}$  for some integer  $n$  and rational  $q \in \mathbb{Q} \setminus \mathbb{Z}$ .
  - (b)  $\sqrt[n]{m}$  for some integers  $n$  and  $m$ .
  - (c)  $e$
  - (d)  $\pi$
  - (e)  $\frac{1+\sqrt{d}}{2}$  where  $d$  is an integer. [Hint: Depends upon the congruence class of  $d$  modulo 4]
  - (f) If  $\alpha$  is algebraic, then for some integer  $n \neq 0$ ,  $n\alpha$  is integral.
  - (g) If  $\alpha$  is transcendental, then for every integer  $n \neq 0$ ,  $n\alpha$  is transcendental.
28. Determine the degrees of the algebraic elements listed below:
- (a)  $e^{\pi i/3}$
  - (b)  $e^{2\pi i/p}$
  - (c)  $\alpha = \sqrt{6} - \sqrt{9}$
  - (d)  $\beta = i + \sqrt{2}$ , and verify that  $\mathbb{Q}[i, \sqrt{2}] = \mathbb{Q}[\sqrt{2} + i]$
  - (e)  $\gamma = \sqrt{2} + \sqrt{3}$ , and conclude that  $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$

(f)  $\delta = \sqrt[3]{2} + \sqrt{3}$  has degree 6 and  $\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}] = \mathbb{Q}[\sqrt[3]{2} + \sqrt{3}]$

29. Assume that  $d$  is a square-free integer. Verify that  $\mathbb{Z}[\sqrt{d}]$  is a ring consisting of

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

when  $d \equiv 2, 3 \pmod{4}$ . When  $d \equiv 1 \pmod{4}$ , then

$$\mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right] = \left\{a + b\frac{1 + \sqrt{d}}{2} \mid a, b \in \mathbb{Z}\right\}.$$

30. Assume  $F$  is a field. Show that if  $f(x) \in F[x]$  is a polynomial of degree 2 or 3, then  $f(x)$  is irreducible if and only if  $f(x)$  has no roots.

31. Suppose that  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$  is such that

(a) for some prime  $p$ ,  $p \mid a_k \forall k \leq n-1$ ,  $p \nmid a_n$  and (b)  $p^2 \nmid a_0$

then  $f(x)$  is irreducible over  $\mathbb{Q}$ .

32. Verify that the polynomials are irreducible.

(a)  $f(x) = x^3 - x^2 - x + 3$

(b)  $g(x) = x^2 + x + 1$

(c)  $h(x) = 21x^5 - 14x^3 + 10x + 6$  is irreducible by Eisenstein's Criterion.

(d)  $f(x) = 25x^5 - 9x^4 - 3x^2 - 12$  is irreducible by Eisenstein's Criterion.

(e)  $g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$  is irreducible by Eisenstein's Criterion.

33. Find all zeros of  $f(x) = 6x^4 + 17x^3 + 7x^2 + x - 10$  in  $\mathbb{Q}$ .

34. Let  $f(x) \in F[x]$ . Then,  $\alpha \in F$  is a root to  $f(x)$  if and only if,  $f(x) = g(x)(x - \alpha)$  for some  $g(x) \in F[x]$ .

35. Let  $R = \mathbb{Z}[\sqrt{m}]$  and define  $\nu : R \rightarrow \mathbb{Z}$  defined by

$$\nu(a + b\sqrt{m}) = (a + b\sqrt{m}) \cdot (a - b\sqrt{m}) = a^2 - mb^2.$$

Show that  $\nu$  is multiplicative; that is,

$$\nu((a + b\sqrt{m}) \cdot (c + d\sqrt{m})) = \nu(a + b\sqrt{m}) \cdot \nu(c + d\sqrt{m}).$$

36. Show that when  $m \equiv 1 \pmod{4}$ ,

$$\mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right] = \left\{ a + b\frac{1 + \sqrt{m}}{2} \mid a, b \in \mathbb{Z} \right\} = \left\{ \frac{a + b\sqrt{m}}{2} \mid a \equiv b \pmod{2} \right\}.$$

Recall, the first equality is the statement that  $\frac{1 + \sqrt{m}}{2}$  is integral, and can be assumed.

37. Assume that  $R = \mathbb{Z}[\sqrt{m}]$ . Use 1. to show that  $a + b\sqrt{m} \in R$  is a unit  $\iff \nu(a + b\sqrt{m}) = \pm 1$ .

38. Show that if  $m < -1$ , then  $R = \mathbb{Z}[\sqrt{m}]$  has only the units  $\pm 1$ .

39. For  $m = -1$ , find the 4 units of  $R = \mathbb{Z}[\sqrt{m}]$ .

40. If  $m \geq 2$ , then  $R = \mathbb{Z}[\sqrt{m}]$  has infinitely many units. Verify this for  $m = 2, 3, 5, 6$ .

41. In case  $m \equiv 1 \pmod{4}$ , the Number Ring (as noted) is  $\mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right]$ . According the Exercise 36,  $\mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right] = \left\{ \frac{a + b\sqrt{m}}{2} \mid a \equiv b \pmod{2} \right\}$ . We use this characterization of the Number Ring, to show that

$$\mathbf{v} : \left\{ \frac{a + b\sqrt{m}}{2} \mid a, b \in \mathbb{Z}, \text{ and } a \equiv b \pmod{2} \right\}^* \rightarrow \mathbb{N},$$

defined as  $\mathbf{v}\left(\frac{a + b\sqrt{m}}{2}\right) = \frac{a^2 - mb^2}{2}$  is an integer and is multiplicative. Hence,  $\frac{a + b\sqrt{m}}{2}$  is a unit  $\iff \mathbf{v}\left(\frac{a + b\sqrt{m}}{2}\right) = \pm 1$ . (Aside: The statements concerning  $\mathbb{Z}[\sqrt{m}]$  hold here as well.)

42. Let  $S$  be a commutative ring with no proper ideals. Then  $S$  is a field.

43. For the Number Ring  $\mathbb{Z}[\sqrt{10}]$ , show  $2, 3, 4 + \sqrt{10}$ , and  $4 - \sqrt{10}$  are pairwise non-associate irreducibles. Further, the ideal  $P = (2, 4 + \sqrt{10}) = R2 + R(4 + \sqrt{10})$  is not principal.
44. Let  $S$  be a finite integral domain. Then  $S$  is a field. Conclude that if  $P$  is a maximal ideal of an integral domain  $R$  such that  $R/P$  is finite, then  $P$  is a maximal ideal of  $R$ .
45. Let  $M, M \neq R$ , be an ideal of an integral domain  $R$ . Then  $M = (r)$  for some irreducible element  $r$  if and only if  $M$  is maximal among all principal ideals of  $R$ . Hence, if  $R$  is a PID, then an ideal  $M$  is maximal if and only if  $M = (r)$  for some irreducible element  $r$ .

# Bibliography

- [1] Arnold, David M.; *Finite Rank Torsion-Free Abelian Groups and Rings*, LNM 931, Springer-Verlag, 1982.
- [2] Reinhold Baer, Abelian groups without elements of finite order, *Duke Math. J.* 3 (1934), 68-122.
- [3] M. C. R. Butler, A class of torsion-free abelian groups of finite rank, *Proc. London Math. Soc.* (3) 15 (1965), 680-698.
- [4] M. C. R. Butler, Torsion-free modules and diagrams of vector spaces, *Proc. London Math. Soc.* (3) 18 (1968), 635-652.
- [5] Laszlo Fuchs; *Infinite Abelian Groups, Volume I*, Academic Press 1970.
- [6] Laszlo Fuchs; *Infinite Abelian Groups, Volume II*, Academic Press 1973.
- [7] H. Pat Goeters; On number rings and a problem of P. Hill, *Comm. in Alg.* 23 (10), (1995), 3677-3683.
- [8] H. Pat Goeters; Reflexive rings and subrings of a product of Dedekind domains, *Journal of Pure and Applied Algebra* **137** (1999) 237-252.
- [9] Harper, Malcome, Murtry, M. Ram, Euclidean rings of algebraic integers, *Canad. J. Math.* Vol. 56 (1), 2004 pp. 71-76
- [10] Daniel Marcus; *Number Fields*, Springer-Verlag 1977.

- [11] Eben Matlis; *Torsion-Free Modules*, University of Chicago Press, 1972.
- [12] Eben Matlis; *1-Dimensional Cohen-Macaulay Rings*, LNM 327, Springer-Verlag, 1973.
- [13] Matsumura, H.; *Commutative Ring Theory*, Cambridge University Press, 1980.
- [14] Rotman, Joseph J.; *An Introduction to Homological Algebra*, Academic Press, 1979.