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. Copies of my colleagues' notes on Harmonic Analysis were also on sale at the vending table; the price, $ 3. His must have 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 $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. 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 σ is:

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

where $i_1, i_2, \ldots, i_n$ is just a reordering of $1, 2, \ldots, n$. 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

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

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

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

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

The function composition of σ and δ, where σ, δ 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 $\iota : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ defined by $\iota(j) = j$ belongs to S_n, and is called the *identity* map.

(ii) If $\sigma \in S_n$, then $\sigma^2, \sigma^3, \ldots \in S_n$, as well (Exercise 1.2).

(iii) The functional inverse of $\sigma \in S_n$, σ^{-1}, is also in S_n. By definition $\sigma^{-1}(i) = j$ exactly when $\sigma(j) = i$. Another point of view yields that σ^{-1} is the only permutation for which $\sigma\sigma^{-1} = \iota = \sigma^{-1}\sigma$.

Example 1 *(a) If*

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

then

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

(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* $\tau = (i_1, i_2, \ldots, i_m)$, $\tau^{-1} = (i_m, i_{m-1}, \ldots, i_1)$. *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, ℓ with $\sigma^\ell = \sigma^m$. If $m < \ell$ multiply both sides by σ^{-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 $i \in \{1, 2, \ldots, n\}$, 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 $i_1, i_2, \ldots, i_k$. We claim that $\sigma(i_k) = 1_1$.

Note that, in this procedure, $i_s = \sigma^{s-1}(i_1)$ where σ^0 is defined to be ι. 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 $\tau_1 = (i_1, i_2, \ldots, i_k)$ which conforms to σ at each of $i_1, i_2, \ldots, i_k$;

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

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

$$\ldots$$

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

Choose j not among $i_1, i_2, \ldots, i_k$ (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 $\tau_2 = (j_1, j_2, \ldots, j_\ell)$ which agrees with σ on all of the numbers $j_1, j_2, \ldots, j_\ell$. We continue producing cycles $\tau_1, \tau_2, \ldots, \tau_s$ until all of the numbers $1, 2, \ldots, n$ have been exhausted. Then

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

A cycle

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

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

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

This expression is not unique since for example

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

A 2-cycle is also called a transposition.

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

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 ι can be expressed as a product of say ℓ transpositions, then ℓ is even.

So we can forget about the notation used thus far and assume that ι 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 ℓ is even. Let c be any number appearing in one of the transpositions in (†), 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 (†) by two and produce a representation of ι as a product of $\ell - 2$ transpositions. Otherwise, $(ii) - (iv)$ apply and we can rewrite † to obtain an expression of ι as a product of ℓ 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 (†) 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 (†), or rewrite (†) 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 (†); eventually leaving only ι on the left-hand side. So, ℓ 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 $r_0 > r_1 > r_2 > \cdots$. So, continuing this precess 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, ℓ.

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

$$n = q_1 m + r_1$$

$$m = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\cdots$$

$$r_{j-3} = q_{j-1} r_{j-2} + r_{j-1}$$

$$r_{j-2} = q_j r_{j-1}.$$

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

$$r_{j-1} = r_{j-3} - q_{j-1} r_{j-2}$$

$$r_{j-1} = r_{j-3} - q_{j-1}(r_{j-4} - q_{j-2} r_{j-3})$$

$$r_{j-1} = (1 + q_{j-1} q_{j-2}) r_{j-3} - q_{j-1} r_{j-4}.$$

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

$$d = u r_0 + v r_1$$

and so

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

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 $r_1 = n - q_1 m$, 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 $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is one-to-one if and only if the function σ 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 σ^{-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) σ^{-1}, δ^{-1}.

   (c) all distinct powers of σ and of δ.

   (d) the powers of σ and δ which produce σ^{-1} and δ^{-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 ρ, ρ^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 $* : G \times G \to G$. 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 $1, 2, \ldots, n$, 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 $\mathbb{Z}_{(n)} = \langle \overline{1} \rangle$ 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 $\sigma = (1, 2, \ldots, n) \in S_n$ has n distinct powers:

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

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 $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, where $\overline{i}$ denotes the congruence class of i modulo $n\mathbb{Z}$.*

Addition is performed as $\overline{i} + \overline{j} = \overline{k}$ 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, $\mathbb{Z}_p = \{ \frac{n}{m} \mid n, m \in \mathbb{Z}, p \not| m \}$ 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 $\frac{\bar{n}}{p^k}$ 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 $G_1, G_2, \ldots, G_n$ to obtain a group*

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

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

$$(g_1, g_2, \ldots, g_n) \cdot (g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n').$$

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 $a^k = a^{qm+r} = a^{qm}a^r = (a^m)^q a^r = a^r$ (in particular, $a^m = a \cdot a^{m-1} = a^{m-1} \cdot a = e$ so $a^{-1} = a^{m-1}$). Therefore,

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

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

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

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 ℓ, 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 ℓ.

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 $n > n_0 > n_1 > ...$ and since positive integers cannot

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

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 $d = (m,k)$ 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, ℓ 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 ℓ. 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 $G_1, G_2, \ldots, G_n$ we have already encountered the (cartesian) direct sum

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

On the other hand, given an abelian group G with subgroups $H_1, H_2, \ldots, H_n$, 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

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

and for any i,

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

Stickleberger Theorem: Let G be a finite abelian group. If $g \in G$ 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, $a = upa + vma = uh + ukg \in H \oplus \langle g \rangle$ 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 ℓ_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 ℓ_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 Stickleberger 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 $z_1, z_2, \ldots, z_n$ of F, and positive integers $d_1, d_2, \ldots, d_n$ such that $d_1 z_1, d_2 z_2, \ldots, d_n z_n$ generates K.

Proof:

$\diamond$

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 $N = \{(e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n) \mid g_i \in G_i\}$ 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 $\phi\colon G \to H$ is called a *homomorphism* provided

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

for all $a, b \in G$. The homomorphism ϕ is called a *monomorphism* when ϕ is One-to-one, and an *epimorphism* when ϕ is onto. A one-to-one, onto homomorphism is called an *isomorphism*. The *kernel* of ϕ 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 $\phi\colon G \to H$, there is a one-to-one correspondence between subgroups B of H and subgroups A of G containing Ker ϕ 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, Ker ϕ is a normal subgroup of G.
Proof: Exercise. $\diamond$

When there exists an isomorphism $\phi\colon G \to H$ 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 $G_1, G_2, \ldots, G_n, H_1, H_2, \ldots, H_m$ 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 is 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 φ 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. (φ is called the Euler ϕ-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 φ equal to the Euler ϕ-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 $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1, e_2, \ldots, e_k$ are positive integers. Show that $\varphi(n) = p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\cdots p_k^{e_k}(p_k-1)$.

21. Consider the *quaternion group* $\mathbb{H} = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{i}\}$ where $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{i}^2 = -1$, 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) $\phi : \mathbb{Z}_{(12)} \to \mathbb{Z}_{(5)}$
    (b) $\phi : \mathbb{Z}_{(12)} \to \mathbb{Z}_{(15)}$
    (c) $\phi : \mathbb{Z}_{(12)} \to \mathbb{Z}_{(4)}$
    (d) $\phi : \mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(4)} \to \mathbb{Z}_{(2)} \oplus \mathbb{Z}_{(5)}$
    (e) $\phi : \mathbb{Z} \to \mathbb{Z}_{(6)}$
    (f) $\phi : \mathbb{Z}_{(4)} \to \mathbb{Z}_{(12)}$

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

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

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

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

(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.

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

Example: The collection R of all 2×2 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.

An element $r \neq 0$ in a ring R is called a *zero divisor*, if $r \cdot s = 0$ for some $0 \neq s \in R$. The previous example is a ring with many zero divisors.

Example: 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*.

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

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

Commutative rings without zero-divisors are called *integral domains*. A ring for which every non-zero element is a unit is called a *division ring*. A commutative division ring is called a *field*.

Example: 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 ± 1) are units in R.

Example: 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.

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 $ac = b$.

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 well will see in our first theorem, irreducible elements are quite common-place while primes are not.

Example: 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. It follows that 6 cannot be factored into a

product of primes in R.

We say that an ideal I of R is *finitely generated* if there exist a subset $\{a_1, a_2, \ldots, a_n\}$ of I such that

$$a \in I \implies \exists\, r_1, r_2, \ldots, r_n \in R \text{ such that } a = \Sigma_{i=1}^{n} r_i a_i.$$

In this case we write

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

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

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

in which case $I = (a_1, a_2, \ldots, a_n)$. Note that for nonzero elements a, b in a domain R, $a \mid b$ if and only if $(b) \subseteq (a)$.

Definition: An integral domain R is called *noetherian* if every ideal is finitely generated.

Proposition 20 *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.

(d) A submodule of a finitely generated R-module is itself finitely generated.

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

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

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).

$(d) \rightarrow (a)$. R is generated by 1 and so is every submodule of R; i.e., every ideal of R, must be finitely generated.

$(a) \rightarrow (d)$. We know that every ideal of R is finitely generated. We induct on n to show that every submodule of a direct sum of n copies of R, which I'll write as $F = \oplus_n R$, is finitely generated. The induction is easy since if K is a submodule of F and $\pi : F \rightarrow R$ is the projection map onto the first component (i.e., $\pi(r_1, r_2, \ldots, r_n) = r_1$), then we have an exact sequence

$$0 \rightarrow H \rightarrow K \xrightarrow{f} I \rightarrow 0,$$

where f is the restriction of π to K. Since $H \leq \oplus_{n-1} R$, and $I \leq R$, by induction H and I are finitely generated. Therefore, if $x_1, x_2, \ldots, x_n$ are such that $f(x_1), f(x_2), \ldots, f(x_n)$ generate I, and $y_1, y_2, \ldots, y_m$ generate $H = Kernel\ f$, then check that $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m$ generate K.

Theorem 21 *Suppose every chain of principal ideals of R stabilizes. 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 $\{(a) \mid a$ 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.

Definition: A domain R is called a *unique factorization domain*, or UFD for short, if every nonzero, nonunit can be (uniquely) factored into a product of primes of R.

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 $q_1 q_2 \cdots q_m$, 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, $p_1 = u_1 q_1$ for some unit u_1. After canceling we obtain

$$p_2 p_3 \cdots p_n = u_1 q_2 q_3 \cdots q_m,$$

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

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

Proposition 22 *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 $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m$ occurs with a_i and b_j irreducible elements, then $n = m$ and after re-indexing $a_i = u_i b_i$ for some units $u_i \in R$.

Proof: By the remarks after the definition of UFD, it is sufficient to show, under either (a) or (b), that irreducible elements are prime.

Assuming (a), any irreducible element r is a product of primes, and so by the definition of irreducible, r must be a single prime. Assuming (b), suppose that an irreducible element s divides a product rt. Say $st' = rt$.

Factoring t', t and r into products of irreducibles, we find by the uniqueness in part (b), that s must be one of the irreducibles factors (up to unit multiple) of either r or t. That is, $s \mid r$ or $s \mid t$.

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, UFD's need not be noetherian or even seem noetherian-like.

Example 23 *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 $R[x_1 1, x_2, \ldots, x_n]$ for any number of indeterminates $x_1, x_2, \ldots, x_n$. By $R[x_1, x_2, \ldots]$ we mean the polynomials with coefficients in R that involve only finitely many of the x_j's, so it follows that $R[x_1, x_2, \ldots]$ is a UFD as well. The ideal $(x_1, x_2, \ldots)$ is obviously not finitely generated.*

As a corollary to our theorem, we can deduce the Fundamental Theorem of Arithmetic, as it relates to domains.

The classical approach to studying rings is to view them through their ideals (this is due to Dedekind).

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

$$IJ = \{x \in R \mid \exists\, n \in \mathbb{Z}^+,\ a_i \in I, b_i \in J, \text{for } i = 1, 2, \ldots, n$$

such that $x = \Sigma_{i=1}^{n} a_i b_i\}$.

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, $s = sm + sar \in M$.

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., $\alpha < \beta \Leftrightarrow J_\alpha \leq J_\beta$), 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.

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 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 M is a maximal ideal.

Definition: An integral domain R is called a *principal ideal domain*, or PID for short, if every ideal is principal (i.e., generated by a single element).

Theorem 24 *Any PID is a UFD.*

Proof: Let R be a PID. Since, obviously R is noetherian, any nonzero, nonunit can be factored into a product of irreducible elements by Theorem 2. It remains to show that any irreducible element in a PID is prime.

Let a be an irreducible element, and suppose $a \mid bc$ for some $b, c \in R$. Since a is not a unit, $(a) \neq R$ and so (a) is contained in a maximal ideal M. Write $M = (d)$. Then $a \in (d)$ implies $a = de$ for some $e \in R$, but because a is irreducible, e must be a unit. That is, $(a) = (d) = M$. Since maximal ideals are prime, $bc \in (a)$ implies $c \in (a)$ (i.e., $a \mid c$) or $b \in (a)$ (i.e., $a \mid b$).

3.3 Integral Closure

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 25 *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 $t^n = -\Sigma_{j=1}^{n-1} r_j t^j$ implying that $R[t]$ is a ring that is generated as an R-module by $1, t, \ldots, t^{n-1}$.

(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

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

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

$$AX = tX,$$

where X is the n-tuple $(t_1, t_2, \ldots, t_n)$ (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 $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$.

Here is the definition given in class describing integrally closed.

Corollary 26 *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

$$S \text{ finitely generated over } R \Rightarrow S = Rt_1 + \ldots + Rt_n$$

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

(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 27 *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

$$r^n + r_{n-1}sr^{n-1} + \cdots + s^{n-1}r_1r + s^nr_0 = 0.$$

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 $t \in R$.

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 28 *Let F be any field containing $\mathbb{Z}$. The collection of all elements $\alpha \in F$ such that α 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 α'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 $1, \alpha, \ldots, \alpha^{n-1}$ over $\mathbb{Z}$, and any $g(\beta)$ by $1, \beta, \ldots, \beta^{m-1}$ over $\mathbb{Z}$. It follows that any element in S can be generated by

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

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

$$f_0(\alpha) + f_1(\alpha)\beta + \cdots + f_k(\alpha)\beta^k = \Sigma_{i_1=0}^m f_{i_1}(\alpha)\beta^{i_1} +$$

$$\Sigma_{j=m+1}^k [f_j(\alpha) \Sigma_{i=0}^m \ell_{ij} \beta^i].$$

Likewise we can express each $f_i(\alpha)$ exclusively in terms of $1, \alpha, \ldots, \alpha^n$ 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 γ 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

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

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

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

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 α 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* α *over* $\mathbb{Z}$ is the monic polynomial of smallest positive degree in $\mathbb{Q}[x]$ having α 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 α 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 29 *Let α be in a field F containing $\mathbb{Z}$. The following are equivalent:*

(1) α is integral over $\mathbb{Z}$.

(2) α is algebraic over $\mathbb{Z}$ and the monic minimal polynomial for α is in $\mathbb{Z}[x]$.

(3) α 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 α as a root (α integral) and let $f(x) \in \mathbb{Q}[x]$ be the monic polynomial of smallest degree having α as a root (clearly, α 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 α is algebraic. If $f(x) \in \mathbb{Q}[x]$ is the monic polynomial of least degree with α 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 α as a root, then $f_0(x)/a \in \mathbb{Q}[x]$ is the monic polynomial for α 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 α as a root must be monic.

(3) $\rightarrow$ (1). Again, if $f(x) \in \mathbb{Q}[x]$ is the monic irreducible polynomial for α, 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 α is integral over $\mathbb{Z}$.

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

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

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

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

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

From this data and the previous example we find that α, β, δ are integral over $\mathbb{Z}$ while γ is not. To see how to obtain the polynomials, let us consider obtaining $k(x)$ for δ. 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 δ with x, we obtain

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

3.4 Localizations and Over-rings of R

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

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

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 $s_1, s_2 \in \mathcal{S}$, $s_1 s_2 \in \mathcal{S}$, then one can form a *localization*, $\mathcal{S}^{-1}(R)$, where

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

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

(a) J is an ideal of $\mathcal{S}^{-1}(R)$ if and only if $J = \mathcal{S}^{-1}(I) = \{\frac{a}{s} \mid s \in \mathcal{S},\ a \in I\}$, 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 $\frac{r_1}{s_1}\frac{r_2}{s_2} \in P' = \mathcal{S}^{-1}(P)$ 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 $\frac{r_1}{s_1} \in P'$.

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.

3.5 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 $P_1, P_2, \ldots, P_n$. 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 $Q_1, Q_2, \ldots, Q_m$. 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 $i = 1, 2, \ldots n$. 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 $i = 1, 2, \ldots n$, we see that $Q_{2i-1} = Q_{2i} = P_i$ for $i = 1, 2, \ldots n$. Therefore,

$$(P + Rr)^2 = P_1^2P_2^2 \cdots P_n^2 = Q_1Q_2 \cdots Q_m = P + Rr^2.$$

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,

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

Under (2), I is invertible, and so $a = \Sigma_{i=1}^n (ab_i)a_i$ for any $a \in I$, and since $ab_i \in I$ for all i, I is generated by $a_1, a_2, \ldots, a_n$. 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 $I = \{s \in S \mid s(\frac{t}{y}+S) = 0\}$, 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 $P = ann_S\, x + S$ 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 $\cap_{k=1}^{\infty} N^k = 0$. If we set $I = \cap_{k=1}^{\infty} N^k$ 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, $\cap_{k=1}^{\infty} N^k = 0$.

Let J be a proper ideal of S. Then $J \subseteq N$. Since $\cap_k(b^k) = 0$, 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,

$$r \in M \setminus P \implies r \in (M \cdot R_M) \setminus (P \cdot R_M) \ (check!)$$

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, $M_1, M_2, \ldots, M_n$ are coprime in pairs (i.e., $M_i + M_j = R$ for all $i \neq j$), the intersection can be replaced by the product:

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

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 $M = rad(J)$. 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 $M = rad(J)$. 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 31 *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 $x|h(x, y)$ 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 32 *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

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

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 $\mathbb{Z}[\sqrt{-5}]$.

3.6 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, $rad(I)$, is the ideal consisting of the elements $r \in R$ such that $r^n \in I$ for some $n \geq 1$.

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

Proposition 33 *Given an ideal $I \neq R$ of the noetherian domain R, one can say the following:*

(i) The radical of I, $rad(I)$, is the intersection of all prime ideals containing I.

(ii) There is an $n \geq 1$ such that $rad(I)^n \subseteq I$.

(iii) If I is primary, then $rad(I)$ is prime.

(iv) If $rad(I)$ is a maximal ideal, I is primary.

Item (i) prompts the phrase, *prime radical*, for $rad(I)$. **Proof:** (i). Let $J = \cap\{P \mid I \subseteq P\}$ (P will always represent a prime unless otherwise indicated). If $r \in rad(I)$, 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., $rad(I) \subseteq J$. 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 $\mathcal{S} \cap I = 0$ 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 $J \subseteq rad(I)$.

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

$$r^n = (a_1r_1+a_2r_2)^n = \Sigma_{i=0}^n c_{n,i}(a_1r_1)^i(a_2r_2)^{n-i} = \Sigma_{i=0}^n c_{n,i}(a_1^i a_2^{n-i})[r_1^i r_2^{n-i}],$$

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

(iii). Suppose $rs \in rad(I)$ for some $r, s \in R$ with $r \notin rad(I)$. By the definition of $rad(I)$, 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 $r \notin rad(I)$), implies that some power of s^n, $s^{mn} \in I$. That is, $s \in rad(I)$. Therefore, $rad(I)$ is prime.

(iv). Let I be an ideal such that $rad(I) = M$ 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

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

If we multiply this by a we obtain

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

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

Example 35 *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:*

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

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 $b \in B$

$$ann_R\, b = \{r \in R \mid rb = 0\}.$$

Of course $ann_R\, b$ may be 0 or may be R, but for certain modules B, $ann_R\, b$ 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 $0 \neq b \in B = R/I$, $ann_R\, b$ 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

$$P = ann_R\, b,$$

for some $b \in B$. With $\mathcal{A} = \{J \mid J = ann_R\, b \text{ for some } 0 \neq b \in B\}$, 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 $P = ann_R\, b$ 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 36 *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 $P' = ann_R\ r + I$ 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 $P = rad(I)$ 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 $I_1, I_2, \ldots, I_n$ 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' of 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 $\{1, 2, \ldots, n\}$ is $I = \cap_{j \in U} J_j$. So J is irreducible if J is not the irredundant intersection of two ideals J' and J''.

Theorem 37 *Let I be a proper ideal in a noetherian domain R. Then, there exists primary ideals $I_1, I_2, \ldots, I_k$ 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 $I_1, I_2, \ldots, I_n$ 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 $P_i = ann_R\, r_i + J$. 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 38 *If $I_1, I_2, \ldots, I_n$ are primary ideals whose radicals are the distinct maximal ideals $M_1, M_2, \ldots, M_n$, then*

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

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

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

for all i. To see this observe that if M is a maximal ideal containing $M_i^k + \Pi_{j \neq i} M_j^k$ 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,

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

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 $I_1 \cap I_2 \cap \cdots \cap I_n$:

$$I_1 \cap I_2 \cap \cdots \cap I_n = [I_i \cap \cap_{j \neq i} I_j](I_i + \Pi_{j \neq i} I_j) =$$

$$[I_i \cap (\Pi_{j \neq i} I_j)](I_i + \Pi_{j \neq i} I_j) = [I_i \cap (\Pi_{j \neq i} I_j)] I_i + [I_i \cap (\Pi_{j \neq i} I_j)] \Pi_{j \neq i} I_j$$
$$\subseteq I_1 I_2 \cdots I_n.$$

3.7 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 2×2 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 $deg : F[x] \to \mathbb{N}$ 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 α.

   (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 $J = \cap_{M\ max} M$.

   (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 $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. 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

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

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:

(a) $R = \mathbb{Z}[\sqrt{10}]$

(b) $R = \mathbb{Z}[\sqrt{5}]$

(c) $R = \mathbb{Z}[\sqrt{d}]$ with $d < 0$, $d \neq -1$.

(d) $R = \mathbb{Z}[\sqrt{-1}]$.

17. Show that if $\alpha \in R = \mathbb{Z}[\sqrt{d}]$ with $N(\alpha) = \pm p$, an integral prime, then α is irreducible. Must α 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 $F[x]$.

(a) $F = \mathbb{Z}_{(p)}$ for your choice of p.

(b) $F = \mathbb{Q}$.

(c) $F = \mathbb{R}$.

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.

Chapter 4

An Introduction to Module Theory

4.1 Introduction

Given an integral domain R, an abelian group M, written additively, constitutes a *left R-module* or a *left module over R* if there exists a function on sets

$$R \times M \to M;$$

with the image of the tuple (r, m) written (generically) as $r \cdot m$ - and $\forall\, r, s \in R,\ \forall\, m, n \in M$ the following properties hold:

$$r \cdot (s \cdot m) = (rs) \cdot m,$$

$$r \cdot (n + m) = r \cdot n + r \cdot m,$$

$$(r + s) \cdot m = r \cdot m + s \cdot m,$$

and

$$1 \cdot m = m.$$

In this case the function $R \times M \to M$ is called the *module action*.

If M is an R-module, a nonempty subset N of M is called a *submodule* of M if the restriction of the module action $R \times M \to M$ to $R \times N$ has image in N (i.e., N is closed with respect to the module action), and N is closed under $+$.

The ideals of R are naturally R-modules and are submodules of R. Given a natural number n we can form the direct sum of R, taken n times, as

$$\oplus_n R = \{(r_1, r_2, \ldots, r_n) \mid r_i \in R,\ i = 1, 2, \ldots, n\}.$$

More generally, given any collection of modules M_i where i belongs to the index set I, we define the *direct sum* of the M_i's to be

$$\oplus_{i \in I} M_i = \{(m_i \mid i \in I) \mid m_i \in M_i \ \forall\ i \in I, \text{ and, almost all } m_i's = 0\}.$$

The notation $(m_i \mid i \in I)$ denotes a *sequence* whose i^{th} entry for $i \in I$ is m_i.

The direct sum $\oplus_{i \in I} M_i$ of modules is again a module under the module and group actions

$$r(m_i \mid i \in I) = (rm_i \mid i \in I),$$

and

$$(m_i \mid i \in I) + (n_i \mid i \in I) = (m_i + n_i \mid i \in I).$$

A module M over an integral domain R is called *torsion-free* if

$$rm = 0 \ \Rightarrow\ r = 0 \text{ or } m = 0 \ \forall\ r \in R,\ m \in M.$$

Chapter 5

An Introduction to Galois Theory

5.1 Introduction

Perhaps one of the mostly intensely studied problems in mathematics was the issue of trying to obtain formulas, analogous to the quadratic formula, where one can express the roots of a polynomial in terms of radicals of the coefficients of the polynomial. Almost from the beginning of recorded time, there was some knowledge of obtaining solutions of quadratic equations using completion of the square and the quadratic formula. The ancient Greeks were interested in

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 abelain 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] Daniel Marcus; *Number Fields*, Springer-Verlag 1977.

[9] Eben Matlis; *Torsion-Free Modules*, University of Chicago Press, 1972.

[10] Eben Matlis; 1-*Dimensional Cohen-Macaulay Rings*, LNM 327, Springer-Verlag, 1973.

[11] Matsumura, H.; *Commutative Ring Theory*, Cambridge University Press, 1980.

[12] Rotman, Joseph J.; *An Introduction to Homological Algebra*, Academic Press, 1979.