Algebra

Jim Coykendall

March 2, 2011

Chapter 1

Basic Basics

The notation $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ refer to the natural numbers, the integers, the rational numbers, the real numbers and the complex numbers respectively.

The following theorem is the famous (and quite useful) Euclidean algorithm.

Theorem 1.0.1. *Let $m, n \in \mathbb{Z}$ be integers with $n \neq 0$. Then we can find integers q and r such that*

$$m = qn + r$$

with $0 \leq r < n$.

Our next definition is not the best in the general sense (as we will observe when we get to ring theory) but it is correct and utilitarian for use in the integers.

Definition 1.0.2. *We say that a positive integer p is prime if the only (positive) factors of p are itself and 1.*

A useful consequence of the existence of the Euclidean algorithm is the famous Fundamental Theorem of Arithmetic:

Theorem 1.0.3. *Any integer $n > 1$ can be decomposed (uniquely) into a product of prime integers.*

We now define the related concepts of greatest common divisor (gcd) and least common multiple (lcm).

Definition 1.0.4. *Let $m, n \in \mathbb{Z}$ both be positive. We define the $gcd(n, m) = d$ to be a common divisor of m and n such that if b is another common divisor of m and n then b divides d*

Definition 1.0.5. *Let $m, n \in \mathbb{Z}$ both be positive. We define the $lcm(n, m) = L$ to be a common multiple of m and n such that if k is another common multiple of m and n then L divides k*

Both gcds and lcms exist for pairs of positive integers (and the concepts can be extended to encompass airs of nonzero integers). This fact is a consequence of the Euclidean algorithm (either directly or through the Fundamental Theorem of Arithmetic). The following result shows that the two concepts are intimately related.

Proposition 1.0.6. *Let m and n be positive integers and let $L = lcm(m, n)$ and $d = gcd(m, n)$. Then $dL = mn$.*

Proof. Since d divides both m and n, $\frac{mn}{d}$ is a common multiple of m and n and hence L divides $\frac{mn}{d}$ and hence dL divides mn. Write $L = km = jn$ and it is easy to see that $\gcd(k, j) = 1$ (otherwise L is not the least common multiple). Also we can write $m = dm'$ and $n = dn'$ with $\gcd(m', n') = 1$. We obtain

$$km' = jn'.$$

Since m' and n' are relatively prime, this implies that n' divides k (verify). Hence we have that $L = km = kdm' = k'n'dm' = k'nm'$. Hence we have that $dL = k'mn \geq mn$. So we have that dL divides mn and $dL \geq mn$ and so we have equality. □

Chapter 2

Groups: A First Look

2.1 Basics and Definitions

Definition 2.1.1. *Let S be a nonempty set equipped with a binary operation $S \times S \longrightarrow S$ which is associative (that is, $a(bc) = (ab)c$ for all $a, b, c \in S$) is called a* **semigroup**.

Definition 2.1.2. *A semigroup, M, which also possesses an element, e (referred to as an identity) such that $em = me = m$ for all m/inM is called a* **monoid**.

Definition 2.1.3. *A monoid, G with the property that for all $x \in G$, there is an element $y \in G$ such that $xy = yx = e$ is called a* **group**.

Loosely speaking, a group is a set with an associative binary operation that also has an identity and inverses. If the cardinality of the set underlying the group G is finite, we say that G is a **finite group**. The next terminology is important enough to justify its own definition.

Definition 2.1.4. *If G is a group such that $xy = yx$ for all $x, y \in G$, we say that G is an* **abelian** *group.*

We remark that analogous terminology is sometimes employed for semigroups and monoids as well.

Example 2.1.5. *1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all groups under addition.*

2. *Continuous funtions on the interval $[0, 1]$, $C[0, 1]$, is a group under addition.*

3. *All of the above examples are monoids under multiplication.*

4. *Symmetries of an $n-$gon form a finite, nonabelian (if $n > 2$) group.*

5. *$S_n := \{f : \{1, 2, \cdots, n\} \longrightarrow \{1, 2, \cdots, n\} | f$ is bijective$\}$ forms a finite group of order $n!$.*

Example 2.1.6. *Consider the subset of the integers modulo n ($\mathbb{Z}_n$) consisting of integers m such that the $gcd(n, m) = 1$. This set is denoted by $U(\mathbb{Z}_n)$ and forms a finite group under multiplication.*

Example 2.1.7. *We define two rational numbers to be equivalent if their difference is an integer. That is $a \sim b \iff a - b \in \mathbb{Z}$. Verify that this is an equivalence realtion and that the set of equivalence classes (denoted by $\mathbb{Q}/\mathbb{Z}$) forms an infinite abelian group with the addition rule given by $\overline{a} + \overline{b} = \overline{a+b}$ (where $\overline{x}$ denotes the equivalence class of x).*

Proposition 2.1.8. *Let G be a group*

a) $e \in G$ *is unique.*

b) $\forall x \in G, x^{-1}$ *is unique.*

c) $(x^{-1})^{-1} = x \quad \forall \in G.$

d) $(xy)^{-1} = y^{-1}x^{-1} \quad \forall x, y \in G.$

Definition 2.1.9. *Let G be a group.*

a) The order of G ($|G|$)is the cardinality of the set underlying G.

b) If $x \in G$, then the order of the element X (written $|x|$ or $\circ(x)$ is the smallest positive integer n such that $x^n = e$ (if no such n exists, we say that $\circ(x) = \infty$).

c) The exponent of G, $exp(G)$ is the smallest positive integer m such that $x^m = e$ for all $x \in G$ (if no such m exists, we say that $exp(G) = \infty$).

2.2 Some Important Examples: Dihedral, Symmetric, Matrix Groups and the Quaternions

We first look at the dihedral group. This group clearly has at its heart a geometric definition that is based on symmetry. Let $n \geq 2$ be an integer; we consider all of the possible symmetries of the $n-$gon (the case $n = 2$ deserves special degenerate attention).

The dihedral group of on the $n-$gon (which we denote by D_n) is the group of all $2n$ symmetries on a regular $n-$gon. We define it formally in terms of generators and relations as follows.

Theorem 2.2.1. *The group set $D_n = \{x, y | x^n = e = y^2, y^{-1}xy = x^{-1}\}$ forms a group of order $2n$.*

The group defined by the generators and relations above is called the dihedral group of order $2n$.

Another important group is the symmetric group alluded to before.

Theorem 2.2.2. *The set of bijective functions from a set of n objects to itself forms a group under multiplication called the symmetric group (on n letters) of order n!.*

Remark 2.2.3. *Note that S_n coincides with D_m if and only if $n = m = 3$. Also D_n (resp. S_n is abelian if and only if $n = 2$). Also note that D_n is contained in S_n (whatever that means at this point).*

Example 2.2.4. *Do some computations with cyclic notation. Observe that disjoint cycles commute and that every element of S_n can be written as a product of disjoint cycles (and can be written as a product of transpositions).*

Matrices also offer a rich supply of groups.

Definition 2.2.5. *Let $\mathbb{F}$ be a field. We define*

a) $GL_n(\mathbb{F}) = \{M \in Mat_n(\mathbb{F}) | det(M) \neq 0\}$

b) $SL_n(\mathbb{F}) = \{M \in Mat_n(\mathbb{F}) | det(M) = 1\}$

Theorem 2.2.6. *If $|\mathbb{F}| = q < \infty$ then $|GL_n(\mathbb{F})| = \prod_{i=0}^{n-1}(q^n - q^i)$.*

Proof. Use linear independence and counting. □

The quaternions are an interesting group that tends to rear its head quite often.

Definition 2.2.7. *The quaternion group Q_8 is generated by the elements i, j, k with the relations $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j$.*

Example 2.2.8. *Write Q_8 as a subgroup of $SL_2(\mathbb{C})$.*

2.3 Morphisms and Subgroups

Definition 2.3.1. *Let G and H be groups (monoids, semigroups). A function $f : G \longrightarrow H$ is a* **homomorphism** *if*

$$f(xy) = f(x)f(y) \quad \forall x, y \in G.$$

There are types of homomorphisms worth noting.

Definition 2.3.2. *Let $f : G \longrightarrow H$ be a homomorphism. If f is 1-1, we say that f is a monomorphism or injective. If f is onto we say that f is an epimorphism or surjective. If f is both 1-1 and onto, we say that f is an isomorphism. If $H = G$ we say that f is an endomorphism and if $H = G$ and f is an isomorphism, we say that f is an automorphism.*

Example 2.3.3. *The function $f(x) = \ln(x)$ is a homomorphism from the multiplicative group of positive reals to the additive group of the reals. In the same fashion, $g(x) = e^x$ is a function from the additive group of reals the multiplicative groups of ositive reals.*

Example 2.3.4. *a)* $\mathbb{Z} \longrightarrow \mathbb{Z}_n$

b) $A \longrightarrow A$ *via* $a \longrightarrow a^{-1}$ *when* A *is abelian (or more generally* $a \longrightarrow a^n$*).*

c) $\phi_x(y) = x^{-1}yx$

Definition 2.3.5. *Let* G *be a group and* H *a nonempty subset of* G *that is itself a group. We say that* H *is a subgroup of* G *(*$H < G$*).*

Example 2.3.6. *What are the subgroups of* S_3*,* $\mathbb{Z}$*,* $\mathbb{Q}$*? Note that if* $k \leq n$ *then* S_k *is a subgroup of* S_n*. Is the same true if we replace* S *by* D*? Note, however, that* $D_n < S_n$*.*

Here is a useful result for determining subgroups.

Proposition 2.3.7. $H < G$ *is a subgroup if and only if for all* $x, y \in H$*,* $xy^{-1} \in H$*.*

Here we will define some important subgroups that will come up over and over.

Proposition 2.3.8. *Let* $f : G \longrightarrow H$ *be a homomorphism of groups and let* A *be a subset of* G*.*

a) $ker(f) = \{x \in G | f(x) = e_H\}$ *is a subgroup of* G*.*

b) $im(f) = \{f(x) | x \in G\}$ *is a subgroup of* H*.*

c) $Z(G) = \{z \in G | zg = gz, \forall g \in G\}$ *is a subgroup of* G *(and is called the* **center***.*

d) $C_G(A) = \{g \in G | ga = ag, \forall g \in G \text{ and } \forall a \in A\}$ *(the centralizer of* A *in* G*) is a subgroup of* G*.*

e) $N_G(A) = \{g \in G | g^{-1}Ag = A\}$ *(the normalizer of* A *in* G*) is a subgroup of* G*.*

Proof. Exercise. □

Here are some elementary properties of homomorphisms.

Theorem 2.3.9. *Let* $f : G \longrightarrow H$ *be a homomorphism of groups.*

a) $f(e_G) = e_H$*.*

b) $f(x^n) = (f(x))^n$*.*

c) f *is 1-1* $\iff$ $ker(f) = e_G$*.*

d) f *is onto* $\iff$ $im(f) = H$*.*

e) f *is an isomorphism* $\iff \exists g : H \longrightarrow G$ *such that* $gf = 1_G$ *and* $fg = 1_H$*.*

Proof. Easy. □

Definition 2.3.10. *Let* $\cdots \longrightarrow G_n \xrightarrow{f_n} G_{n+1} \xrightarrow{f_{n+1}} G_{n+2} \longrightarrow \cdots$ *be a sequence of groups and group homomorphisms. We say that the sequence is* **exact at** G_n *if* $ker(f_{n+1}) = im(f_n)$*. The sequence is exact if it exact at* G_n *for all* n*.*

Proposition 2.3.11. *Let* G *be a group and* $\{H_i\}_{i\in\Lambda}$ *be a family of subgroups of* G*. Then* $\bigcap_{i\in\Lambda} H_i$ *is also a subgroup of* G*.*

Proof. Easy. □

Definition 2.3.12. *Let* G *be a group and* X *a subset of* G*. We define the subgroup generated by* X *to be*

$$\langle X\rangle = \bigcap_{X\subseteq H:\ a\ subgroup} H$$

It should be noted that from a computational point of view, the subgroup generated by X is merely composed or all"words" composed from X. Also, even though the intersection of groups is a group, the union is not in general. We define $H \vee K$ to be the "join" or the group generated by the union of the sets H and K.

EXERCISES:

1. Let G be a finite group of order n. Show that any element of G is of finite order and show the exponent of G is bounded by n.
2. Show that the order of any element in S_n is bounded above by $e^{\frac{n}{e}}$.
3. Show that any group of exponent 2 is abelian.
4. Show that any finite group generated by two element of order 2 is dihedral.
5. Show that that the semigroup G is a group if and only if G possesses a left identity and every element of G has a left inverse (what if one of the "lefts" is replaced by "right"?)
6. Let G be a group, show that $\mathrm{Aut}(G)$ is a group under function composition.
7. Show that $\mathbb{Z}$ is isomorphic to all of its nonidentity subgroups.
8. Show that A is an abelian group if and only if the map $f(a) = a^{-1}$ is an automorphism of A.
9. Show that Q_8 is a subgroup of $SL_2(\mathbb{C})$ generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Show that Q_8 is not isomorphic to D_4 (and can you find both of these groups on the Rubik's cube)?

10. Compute $\mathrm{Aut}(\mathbb{Z})$, $\mathrm{Aut}(\mathbb{Z}_6)$, $\mathrm{Aut}(\mathbb{Z}_8)$, and $\mathrm{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$.

11. Let G be a group and H a finite subset of G closed under the product from G. Show that H is a subgoup.

12. Consider the following sequence of group (homomorphisms)

$$\mathbb{Z} \xrightarrow{\phi} \mathbb{Z} \xrightarrow{\psi} G \longrightarrow 0$$

where $\phi(n) = 2n$. What familiar group must G be isomorphic to for the sequence to be exact?

13. Let $G = \langle X \rangle$ and let $f : G \longrightarrow H$. Show that $\mathrm{im}(f) = \langle f(X) \rangle$ and that $\ker(f) = \langle Z \rangle$ where $Z = \{x \in X | f(x) = e_H\}$.

14. Let G be a group. For any $x \in G$ we define $\phi_x : G \longrightarrow G$ by $\phi_x(y) = x^{-1}yx$. Show that ϕ_x is an element of $\mathrm{Aut}(G)$. We define $\mathrm{Inn}(G) = \{\phi_x | x \in G\}$. Show that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$. Give examples to show that they are not equal in general.

2.4 The Classification of Cyclic Groups

Definition 2.4.1. *We say that the group G is cyclic if it can be generated by a single element (i.e. there is an $x \in G$ such that $g = x^n$ for all $g \in G$).*

The following theorem gives a complete description of the cyclic groups.

Theorem 2.4.2. *Let G be a group. The following conditions are equivalent.*

a) G is cyclic.

b) G is a homomorphic image of $\mathbb{Z}$.

c) All homomorphic images of G are cyclic.

d) All subgroups of G are cyclic.

e) G is isomorphic to $\mathbb{Z}_n$ for some $n \geq 0$.

Proof. It is clear that both c) and d) imply a). We will show a)$\Longrightarrow$ b)$\Longrightarrow$ c)$\Longrightarrow$ e) $\Longrightarrow$ d).

a)$\Longrightarrow$ b): Since G is cyclic, $G = \{x^n | n \in \mathbb{Z}\}$. We define $\phi : \mathbb{Z} \longrightarrow G$ by $\phi(n) = x^n$. It is easy to verify that this is a surjective homomorphism.

b)$\Longrightarrow$ c): We have $\mathbb{Z} \longrightarrow G \longrightarrow H$. So in particular, H is a homomorphic image of $\mathbb{Z}$. Verify that $H = \langle f(1) \rangle$.

c)$\Longrightarrow$ e): In particular, c) means that G itself is cyclic. If $G = \{x^n | n \in \mathbb{Z}\}$ is infinite then $\phi : G \longrightarrow \mathbb{Z}$ via $\phi(x^n) = n$ is an isomorphism. Additionally, if G is finite then the "same" map gives an isomorphism to $\mathbb{Z}_n$.

e)$\Longrightarrow$ d) In particular, $G = \{x^n | n \in \mathbb{Z}\}$ is cyclic. Let $H < G$ be a subgroup and the m be the smallest positive integer such that x^m is in H (if no such m exists, then H is the identity subgroup). Now let $x^N \in H$ with N positive. We use the Euclidean algorithm to write

$$N = qm + r$$

noindent with $0 \leq r < m$. If $r \neq 0$ then $x^r \in H$ which is a contradiction. Therefore, $r = 0$ and hence $H = \langle x^m \rangle$ and we are done. □

Corollary 2.4.3. *Any cyclic group is countable.*

Corollary 2.4.4. *If G is a finite cyclic group of order n and m divides n, then G has a unique subgroup of order m.*

Proof. Let $|G| = n$ and let m divide n (say $n = km$). If x is the generator of G then it is easy to see that x^k generates a subgroup of order m (say H). It remains to see that this subgroup is unique. Suppose that K is another subgroup of order m. We will say that $K = \langle x^j \rangle$. Note that $x^{jm} = 1 = x^{km}$. Therefore both jm and km are multiples of n (and no smaller multiple of j or k is a multiple of n).

$$jm = dn$$

and $\gcd(d, m) = 1$ (else the order is lowered). Therefore, d divides j (verify). We write $j = db$ and obtain

$$dbm = dn$$

and so $bm = n$ and so $b = k$ and $j = dk$. We now have that $x^j = (x^k)^d$ and so $K = \langle x^j \rangle \subseteq \langle x^k \rangle = H$ and since the ordrs are the same, we have equality. □

We note that this explains the definition of order of an element. If $x \in G$ then $|x| = |\langle x \rangle|$.

EXERCISES:

1. Let $f : G \longrightarrow H$ be a group homomorphism and let $x \in G$. Show that if f is 1-1, then $|f(x)| = |x|$. Also show that generally, if $|f(x)|$ is finite, then either $|x| = \infty$ or $|f(x)|$ divides $|x|$.

2. Show that G is finite if and only if G possesses only finitely many subgroups.

3. Show that an infinite group is cyclic if and only if it is isomorphic to all of its nonidentity subgroups.

Chapter 3

Cosets, Normality, and Quotient Structures

3.1 Cosets and counting Techniques

The order of a finite group plays a significant role in the classification of the group. Here we begin the discussion.

Definition 3.1.1. *Let $H < G$ and $a, b \in G$. We say that a is right (left) congruent to b modulo H if $ab^{-1}(a^{-1}b) \in H$.*

It should be observed that if G is abelian, then $ab{-}1 \in H \iff a^{-1}b \in H$. This is true more generally, in fact, and the equivalence of left and right congruence modulo H is quite important.

Theorem 3.1.2. *Let $H < G$*

a) Right (left) congruence modulo H is an equivalence relation on G.

b) $[a]$ under under right (left) congruence is $Ha = \{ha | h \in H\}$ ($aH = \{ah | h \in H\}$).

c) $|Ha| = |H| = |aH|$ for all $a \in G$.

We remark that Ha is called a right coset and aH is called a left coset. It is important when $Ha = aH$ for all $a \in G$).

Proof. We do the proof only for the "right" case. It is easy to verify that congruence modulo H is reflexive, symmetric, and transitive. The equivalence class of a is the set $\{g \in G | g \sim a\}$. But $g \sim a$ means that $ga^{-1} \in H$, i.e., $g \in Ha$. For part c) consider the map $\phi : Ha \longrightarrow H$ given by $\phi(ha) = h$. It is easy to verify that this is 1-1 and onto. □

Corollary 3.1.3. *Let $H < G$.*

a) 2 right (left) cosets of H in G are either disjoint or equal.

b) $G = \bigcup_{disjoint} Ha$

c) $\forall a, b \in G, Ha = Hb \iff ab^{-1} \in H$ *and* $aH = bH \iff b^{-1}a \in H$.

d) If $\mathfrak{R}$ *is the set of distinct right cosets of* H *in* G *and* $\mathfrak{L}$ *is the set of distinct left cosets of* H *in* G *then* $|\mathfrak{R}| = |\mathfrak{L}|$.

Proof. a): Suppose that x is in Ha and Hb. We write $x = ha = h_1 b$. Now let $h_2 a \in Ha$ be arbitrary. Note that $a = h^{-1}h_1 b$ and so $h_2 a = h_2 h^{-1} h_1 \in Hb$ and so $Ha \subseteq Hb$ by symmetry, we have equality.

b): Note first that if $g \in G$, then $g \in Hg$. Now the previous part makes this obvious.

c): Clear from part a) as well.

d): We define $\psi : \mathfrak{R} \longrightarrow \mathfrak{L}$ by $\psi(Ha) = a^{-1}H$. Clearly ψ is onto. To see 1-1, note that $a^{-1}H = b^{-1}H \iff ba^{-1} \in H$. Hence $Hb = Ha$ □

These warm-up results give us some powerful tools for classical counting results in group theory.

Definition 3.1.4. *Let* $H < G$ *then the index of* H *in* G *(written* $[G : H]$*) is the number of distinct right (left) cosets of* H *in* G.

Example 3.1.5. *Consider the group* S_3 *and let* H *be a subgroup of order 3 and* K *a subgroup of order 2. Compare the cosets of* H *and* K *in* G.

Theorem 3.1.6. *If* $K < H < G$ *then* $[G : K] = [G : H][H : K]$.

Note that if any of two of the three above indices are finite, then so is the third.

Proof. Let $H = \bigcup_{j \in J} Kb_j$ and $G = \bigcup_{i \in I} Ha_i$ (with $|J| = [H : K]$ and $|I| = [G : H]$). It suffices to show that $\{Kb_j a_i | j \in J, i \in I\}$ is a complete set of coset representatives of K in G. To see that

$$\bigcup_{(i,j) \in I \times J} Kb_j a_i = \bigcup_{i \in I} (\bigcup_{j \in J} Kb_j) a_i = G$$

we let $g \in G$. Note that $g = ha_i$ and $h = kb_j$, therefore $g = kb_j a_i$.

Now assume that $Kb_j a_i = Kb_{j'} a_{i'}$ therefore $b_j a_i = kb_{j'} a_{i'}$. Recalling the the b's and k are elements of H, we obtain $Hb_j a_i = Hkb_{j'} a_{i'}$ or more compactly, $Ha_i = Ha_{i'}$ and hence $i = i'$. Since therefore $a_i = a_{i'}$ we have that $b_j = kb_{j'}$ and hence $Kb_j = Kb_{j'}$ and hence $j = j'$. This concludes the proof. □

Here is a famous, useful and generally smokin' corollary.

Corollary 3.1.7. *(Lagrange) If* $H < G$ *then* $|G| = [G : H]|H|$. *In particular if* G *is finite and* $a \in G$ *then* $|a|$ *and* $|H|$ *both divide* $|G|$.

Proof. The previous result with $K = e$. □

At this juncture we make the notational convention that if H and K are subgroups of G then $HK = \{hk | h \in H, k \in K\}$. Note that in general, this is a set and has no additional structure.

Theorem 3.1.8. *Let H and K be finite subgroups of G. Then $|HK| = \frac{|H||K|}{|H \bigcap K|}$.*

Proof. $L = H \bigcap K$ is a subgroup of K of index $n = \frac{|K|}{|H \bigcap K|}$ (and we write $K := Lk_1 \bigcup Lk_2 \bigcup \cdots \bigcup Lk_n$). Also note that $HL < H$ since L is a subgroup of H. So HK is the disjoint union $Hk_1 \bigcup Hk_2 \bigcup \cdots \bigcup Hk_n$. Therefore $|HK| = |H|n = \frac{|H||K|}{|H \bigcap K|}$. This completes the proof. □

Proposition 3.1.9. *Let $H, K < G$ then $[H : H \bigcap K] \leq [G : K]$. If $[G : K] < \infty$ then $[H : H \bigcap K] = [G : K] \iff G = KH$.*

Proof. Exercise. □

Theorem 3.1.10. *Let H and K be subgroups of finite index in G. Then $[G : H \bigcap K]$ is finite and $[G : H \bigcap K] \leq [G : H][G : K]$ and equality holds if and only if $G = HK$.*

Proof. $[G : H \bigcap K] = [G : H][H : H \bigcap K] \leq [G : H][G : K]$ (by previous and therefore finite). Additionally $[G : H \bigcap K] = [G : H][H : H \bigcap K] = [G : H][G : K] \iff G = HK$ (again by previous). □

EXERCISES:

1. Prove the unproven result(s) above.
2. Let $H, K < G$ then HK is a subgroup of G if and only if $HK = KH$.
3. Let G be a finite group and H a normal subgroup of G such that $|H|$ is relatively prime to $k = [G : H]$. Show that H is the unique subgroup of G of index k (too early?).
4. Classify all groups of order p, 4 and 6.
5. Show that if H and K are subgroups of G with finite index such that $\gcd([G : H] : [G : K]) = 1$ then $G = HK$.

3.2 Normal Subgroups

Theorem 3.2.1. *Let $N < G$ the following are equivalent:*

a) Right and left equivalence modulo N coincide (every equivalence class $[a]$ is the same under left and right equivalence).

b) Every left coset of N in G is also a right coset.

c) $aN = Na$ *for all* $a \in G$.

d) $\forall a \in G, a^{-1}Na \subseteq N$.

e) $\forall a \in G, a^{-1}Na = N$.

We say that any subgroup satisfying one and hence all of the above conditions is **normal** in G.

Proof. We will show $e) \implies d) \implies c) \implies b) \implies a) \implies e)$ and first note that $e) \implies d)$ and $c) \implies b)$ and $a) \iff c)$ are clear.

$d) \implies c)$: $a^{-1}Na \subseteq N$ for all $a \in G$ and hence $Na \subseteq aN$ for all $a \in G$. Also note that $aNa^{-1} \subseteq N$ and so $aN \subseteq Na$. This gives $aN = Na$.

$b) \implies a)$: Given that $aN = Nb$, we have that $a \in Nb$. Therefore $Na = Nb$ and $Na = aN$ for all $a \in G$. Hence right and left equivalence coincide.

$a) \implies e)$: $aN = Na$ and so $N = a^{-1}Na$. □

Example 3.2.2. *1. Every subgroup of an abelian group in normal.*

2. $Z(G)$ *is a normal subgroup of* G

3. The trivial subgroups are normal.

4. $G' := \langle \{xyx{-}1y^{-1} | x, y \in G\}$ *is a normal subgroup (called the commutator subgroup of* G.

5. Let $f : G \longrightarrow H$ *is a group homomorphism, then* $ker(f)$ *is a normal subgroup of* G.

6. Let $H < G$ *be a subgroup of* G *such that* $\sigma(H) \subseteq H, \forall \sigma \in Aut(G)$*, then* H *is a normal subgroup of* G *(called a characteristic subgroup).*

7. A_n *is normal in* S_n *and* $\mathbb{Z}_m$ *is normal in* D_m.

Definition 3.2.3. *We say that the group* G *is* **simple** *if the only normal subgroups of* G *are* G *and* $\{e\}$.

Theorem 3.2.4. *Let* K *and* N *be subgroups of* G *with* N *normal in* G.

a) $N \bigcap K$ *is normal in* K.

b) N *is normal in* $N \vee K$.

c) $NK = N \vee K = KN$.

d) If K *is normal in* G *and* $K \bigcap N = \{e_G\}$ *then* $nk = kn, \forall k \in K, n \in N$.

Proof. a) Easy. b) All you need here is for $k^{-1}nk \in N$ for all $k \in K$ and this holds. c) Clearly $NK \subseteq N \vee K$ to show equality, it suffices to show that NK is a group. Clearly NK contains the identity. Suppoer that $nk, n_1k_1 \in NK$. Note that $nkn_1k_1 = n(kn_1k^{-1})kk_1 \in NK$. Also note that $(nk)^{-1} = k^{-1}n^{-1} = k^{-1}n^{-1}kk^{-1} \in NK$. So $NK = N \vee K$. To see that $NK = KN$ note that

$nk = kk^{-1}nk \in KN$. By symmetry, we have equality. d) Assume additionally that K is normal in G and $N \bigcap N = \{e_G\}$. With this in hand we note that $nkn^{-1}k^{-1}$ is necessarily an element of N since N is normal and is an element of K since K is also normal. Hence this commutator is in $N \bigcap H$ and hence is the identity. So we have that $nk = kn$. □

Theorem 3.2.5. *Let N be a normal subgroup of G and G/N the set of left cosets of N in G. Then G/N is a group of order $[G : N]$ under the operation $(aN)(bN) = abN$.*

Proof. It suffices to show that if $a \equiv x \mathrm{mod}(N)$ and $b \equiv y \mathrm{mod}(N)$ then $ab \equiv xy \mathrm{mod}(N)$. Do so. □

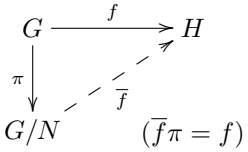
Proposition 3.2.6. *Let $N \lhd G$. Then the natural map $\pi_N : G \longrightarrow G/N$ is an epimorphism of groups.*

Proof. Easy. □

Example 3.2.7. *S_n/A_n and $\mathbb{Z}$ modulo $m\mathbb{Z}$.*

Here is an important universal mapping property that illustrates one of the important facets of normal subgroups.

Theorem 3.2.8. *Let $f : G \longrightarrow H$ be a homomorphism of groups, $N \lhd G$ and $N \subseteq ker(f)$. Then there exists a unique homomorphism $\overline{f} : G/N \longrightarrow H$ such that $\overline{f}(aN) = f(a), \forall a \in G$. What is more, $im(f) = im(\overline{f})$ and $ker(\overline{f}) = ker(f)/N$.*



Remark 3.2.9. *It is worth noting at this point that $\overline{f}$ is an isomorphism if and only if f is onto and $ker(f) = N$.*

Proof. The map that we need is

$$\overline{f} : G/N \longrightarrow H; \overline{f}(aN) = f(a).$$

We first must show that this map is well-defined. Suppose that $aN = bN$, hence $a = bn$ for some $n \in N$. This gives that $f(a) = f(bn) = f(b)f(n) = (b)$ since $b \in N \subseteq \ker(f)$. Homomorphism and the equalities of image and kernal are easy to verify. □

Corollary 3.2.10. *(First Isomorphism Theorem) If $f : G \longrightarrow H$ is a homomorphism, then f induces an isomorphism $\overline{f} : G/ker(f) \longrightarrow im(f)$.*

Here is a more general corollary.

Corollary 3.2.11. *If $f : G \longrightarrow H$ is a homomorphism, $N \lhd G, M \lhd H$ and $f(N) \subseteq M$. Then f induces a homomorphism*

$$\overline{f} : G/N \longrightarrow H/M, (aN \longmapsto f(a)M)$$

and $\overline{f}$ is an isomorphism $\iff im(f) \vee M = H$ and $f^{-1}(M) \subseteq N$. In particular, if f is onto such that $f(N) = M$ and $ker(f) \subseteq N$, then $\overline{f}$ is an isomorphism.

Remark 3.2.12. *Note that in the previous if $N = ker(f)$ and $M = \{e_H\}$, then we recover the first isomorphism theorem.*

Proof. Consider the given map. First assume that $aN = bN$. Of course this means that $an = b$ for some $n \in N$. So $f(b)M = f(an)M = f(a)f(n)M = f(a)M$ since $f(N) \subseteq M$. So the map is well-defined and it is easy to verify that it is a homomorphism.

Now if $\overline{f}$ is an isomorphism, this means that every element of H/M is of the form $f(a)M$ where $a \in G$, hence $\text{im}(f)$ and M together must generate H. And since $\overline{f}$ is 1-1, the preimage of M must be contained in N. It is also clear that these two conditions guarantee that $\overline{f}$ is an isomorphism. □

Corollary 3.2.13. *(Second Isomorphism Theorem) If K and N are subgroups of G with N normal in G, then $K/(N \bigcap K) \cong NK/N$.*

Proof. We remark first that (as left to exercises) that $N \bigcap K \lhd K$. Also NK is a group since N is normal in G and $N \lhd NK$.

We first define $f : K \longrightarrow NK/N$ by $f(k) = kN$. Note that $\ker(f) = \{k \in K | kN \subseteq N\} = K \bigcap N$. We now claim that f is onto. To see this, let $nkN \in NK/N$. Note that $nkN = k(k^{-1}nk)N = kN = f(k)$ so f is surjective. Since f is onto and the kernal is $N \bigcap K$, the first isomorphism theorem gives $K/(N \bigcap K) \cong NK/N$. □

Corollary 3.2.14. *(Third Isomorphism Theorem) Let H and K be normal subgroups of G and $K \subseteq H$. Then $H/K \lhd G/K$ and $(G/K)/(H/K) \cong G/H$.*

Once again, here is a more sweeping result.

Theorem 3.2.15. *Let $f : G \longrightarrow H$ be an epimorphism. Then the assignment $K \longmapsto f(K)$ is a 1-1 correspondence between the set of all subgroups of G containing the kernal of f and all subgroups of H. What is more, K is normal in G if and only if $f(K)$ is normal in H.*

Corollary 3.2.16. *Let $N \lhd G$, then every subgroup of G/N is of the form K/N where $N \subseteq K \subseteq G$. Additionally, $K/N \lhd G/N \iff K \lhd G$.*

EXERCISES:

1. Prove the unproven result(s) above.
2. Let $N \subseteq G$ such that $[G : N] = 2$. Show that $N \lhd G$.

3. Verify the example(s) from this section.
4. Classify all groups of order p (try for p^2).
5. Show that if G is a group such that $G/Z(G)$ is cyclic, then G is abelian.
6. Find all normal subgroups of D_n. Also compute $Z(D_n)$.
7. Let $G' = \langle \{x^{-1}y^{-1}xy | x, y \in G\} \rangle$ be the commutator subgroup of G.
   a) Show $G' \lhd G$.
   b) Show that G' is a characteristic subgroup of G.
   c) Show that if $f : G \longrightarrow A$ is a homomorphism with A abelian, then $G' \subseteq \ker(f)$.

3.3 The Symmetric and Alternating Groups

We take S_n and D_n as defined as before.

Definition 3.3.1. *A cycle is an element of S_n of the form $(a_1, \cdots, a_k)$ with the a_i's distinct elements of $\{1, 2, \cdots, n\}$. A cycle is called a transposition (or involution) if $k = 2$.*

Example 3.3.2. *Write some elements as cycle decompositions. Find inverses and orders of cycles.*

Definition 3.3.3. *We say that $\sigma_1, \sigma_2, \cdots, \sigma_r \in S_n$ are disjoint if for all $1 \leq i \leq r$ and $k \in \{1, 2, \cdots, n\}$, $\sigma_i(k) \neq k \Longrightarrow \sigma_j(k) = k, \forall j \neq i$.*

Theorem 3.3.4. *Every element of S_n is uniquely a product of disjoint cycles.*

Proof. Exercise. □

Corollary 3.3.5. *Let $\sigma \in S_n$ be a product of disjoint cycles $c_1 c_2 \cdots c_k$ of respective orders $m_1, m_2, \cdots, m_k$. Then $|\sigma| = lcm(m_1, m_2, \cdots, _k)$.*

Proof. It is clear that if $L = \text{lcm}(m_1, \cdots, m_k)$ then σ^L is the identity. Hence L is a multiple of the order of σ. We will show that $L \leq |\sigma|$ by induction on the number of disjoint cycles (k). If $k = 1$ the result clearly holds. Assume that the result holds for $k = r$. Now assume that σ is a product of $r + 1$ disjoint cycles, $c_1, c_2, \cdots, c_{r+1}$ of respective lengths $m_1, m_2, \cdots, m_{r+1}$. By the above and induction, the order of $(c_1) \cdots (c_r)$ is precisely $\text{lcm}(m_1, m_2, \cdots, m_r)$. Since (c_{r+1}) is disjoint from $(c_1) \cdots (c_r)$, the order of σ must be a common multiple of the respective orders. This concludes the inductive step. □

Corollary 3.3.6. *Every element of S_n is a product of transpositions.*

Proof. It is easy to see that $(1n)(1n-1) \cdots (13)(12) = (123 \cdots n)$. Since every cycle is a product of transpositions and every element of S_n is a product of cycles, this shows the result. □

Theorem 3.3.7. *Let $\sigma \in S_n$. If $\sigma = \tau_1\tau_2\cdots\tau_k = \xi_1\xi_2\cdots\xi_m$ where each τ_i and ξ_j is a transposition, then $k \equiv m \ mod(2)$.*

Proof. It suffices to show that the identity element cannot be written as an odd product of transpositions and we will induct on n. If $n = 2$, that is $S_n = S_2$ then it is clear that the identity cannot be written as an odd product of (1 2). We suppose that the result holds for S_n and we will show it for S_{n+1}.

We first make the following observations about rearranging transpositions:

$$(1b)(1c) = (1cb) = (1c)(cb), (c \neq b)$$

and

$$(ab)(1c) = (1c)(ab),$$

and

$$(ab)(1a) = (1ba) = (1b)(ab).(b \neq 1).$$

Suppose that $\tau_1\tau_2\cdots\tau_{2n+1} = e$. If none of the transpositions τ_i involves a "1" (if it does then we will call it a 1-transposition) then we are done by induction (as the above product could be thought of as taking place in S_n). The last two displayed realtions above show that we can rearrange successive transpositions as to get all the transpositions involving a "1" to the left (and notice that if during the algorithm we ever encounter (1 x)(1 x) then cancellation occurs in pairs preserving the parity of the original $2n + 1$.

Additionally notice that the first relation allow us to take all of our transpositions at the left (involving the "1"'s) can be rearranged (reducing the number of 1-transpositions by 1 and preserving the length). We can keep applying the first relation and since the product of the transpositions is the identity, and cancellation must occur in pairs, then we get

$$\overline{\tau}_1\overline{\tau}_2\cdots\overline{\tau}_{2m+1} = e$$

which contradicts the inductive hypothesis. This completes the proof.

□

With the previous result in hand, the following definition is a natural one.

Definition 3.3.8. *We say that $\sigma \in S_n$ is even (resp. odd) if it is the product of an even (resp. odd) number of transpositions.*

Proposition 3.3.9. *For all $n \geq 2$ we let $A_n = \{\sigma \in S_n | \sigma \text{ is odd}\}$. Then $A_n \lhd S_n$ and $|A_n| = \frac{n!}{2}$. Also A_n is the unique subgroup of S_n of index 2.*

Proof. Most of this can be captured via noting that $A_n = \ker(f)$ where $f : S_n \longrightarrow \{\pm 1\}$. □

We will now strive to prove a rather big result.

Theorem 3.3.10. *A_n is simple $\iff n \neq 4$.*

The proof of this will require a number of lemmata a number of which are of independent interest.

Lemma 3.3.11. *Let r, s be distinct in $\{1, 2, \cdots, n\}$. Then A_n ($n \geq 3$) is generated by all 3-cycles $\{(rsk) | 1 \leq k \leq n, k \neq r, s\}$.*

Proof. Note that any 3-cycle is an element of A_n so it suffices to show the other containment. Of course any element of A_n is a product of elements of the form $(ab)(ac)$ or $(ab)(cd)$ with a, b, c, d all distinct. The equations

$$(ab)(ac) = (acb)$$

and

$$(ab)(cd) = (cba)(dac)$$

show the necessary containment. □

Lemma 3.3.12. *If $N \lhd A_n$ ($n \geq 3$), and N contains a 3-cycle, then $N = A_n$.*

Proof. Let $(rsc) \in N$ and let $k \neq r, s$. Note that $(rsk) = (rs)(ck)[(rsc)(rsc)](ck)(rs) \in N$. □

We now prove the result that A_n is simple for $n \neq 4$.

Proof. Let case for 2 and 3 are trivial. Also note that the Klein four group $H = \{e, (12)(34), (13)(24), (14)(23)\} \lhd A_4$.

With this noted, we will assume that $n \geq 5$ and $N \lhd A_n$. We also note that if N is properly contained in A_n then N contains no 3-cycle.

Case 1: If N contains an element σ such that σ has a cycle of length at least 4 in its cycle decomposition. We write $\sigma = (a_1 a_2 \cdots a_r)\tau$ where $r \geq 4$ and τ is disjoint from the cycle. Let $\xi = (a_1 a_2 a_3) \in A_n$ and note that $\sigma^{-1}\xi\sigma\xi^{-1} \in N$. Therefore

$$\tau^{-1}(a_r \cdots a_1)(a_1 a_2 a_3)(a_1 a_2 \cdots a_r)\tau(a_3 a_2 a_1) = (a_1 a_3 a_r) \in N$$

which is a contradiction.

Case 2: Assume now that N contains an element σ that is a product of disjoint cycles, at least 2 of which have length 3. In the spirit of the previous, we will write $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6)\tau$. As before we will let $\xi = (a_1 a_2 a_4) \in A_n$. Again, N must contain the element $\sigma^{-1}\xi\sigma\xi^{-1} = (a_1 a_4 a_2 a_6 a_3)$ which reverts us tothe previous case.

Case 3: N contains an element σ that is the product of one 3-cycle and the rest (disjoint) 2-cycles. We write $\sigma = (a_1 a_2 a_3)\tau$ with τ a product of disjoint 2-cycles. Hence $\sigma^2 = (a_3 a_2 a_1) \in N$ and we have a contradiction.

Case 4: every element of N is a product of disjoint transpositions (an even number in fact since $N \lhd A_n$). We write $\sigma = (a_1 a_2)(a_3 a_4)\tau$ (where τ is a product of disjoint transpositions). Note that if $\delta = (a_1 a_2 a_3)$ then $\sigma^{-1}\delta\sigma\delta^{-1} = (a_1 a_3)(a_2 a_4) \in N$. Since $n \geq 5$ we pick an element a_5 distinct from the others. Let $x = (a_1 a_3 a_5)$ and $y = (a_1 a_3)(a_2 a_4)$, and note that $yxyx^{-1} = (a_1 a_3 a_5) \in N$.

This concludes the proof. □

EXERCISES:

1. Prove the unproven results from this section.
2. Prove that S_n is generated by $\{(1\ 2), (1\ 3), \cdots, (1\ n)\}$.
3. Prove that S_n is generated by $\{(1\ 2), (2\ 3), \cdots, (n-1\ n)\}$.
4. Prove that S_n is generated by $\{(1\ 2)$ and $(1\ 2\ \cdots n)$.
5. Prove that S_n is generated by $\{(1\ 2)$ and $(2\ 3\ 4\ \cdots n)$.
6. Compute $Z(D_n)$.
7. Find all normal subgroups of D_n.
8. Show that A_4 has no subgroup of order 6.
9. Let $N = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Show that $N \lhd A_4$ and $N \lhd A_4$. Additionally show that $S_4/N \cong S_3$ and that $A_4/N \cong \mathbb{Z}_3$.
10. For all divisors, d, of 120 find a subgroup of S_5 of order d or prove that one does not exist.

3.4 Direct Products and Direct Sums

Definition 3.4.1. *Let $\{G_i\}_{i\in I}$ be a family of groups. We define the direct product of the family $\{G_i\}_{i\in I}$ to be the group with underlying set $\prod_{i\in I} G_i$ and operation defined by $\{a_i\}\{b_i\} = \{a_i b_i\}$.*

Definition 3.4.2. *Let $\{G_i\}_{i\in I}$ be a family of groups. We define the weak direct product of the family $\{G_i\}_{i\in I}$ to be the subgroup of $\prod_{i\in I} G_i$ given by $\coprod_{i\in I} G_i = \prod_{i\in I}^{w} G_i = \{\{a_i\} | a_i = e_{G_i}$ almost everywhere$\}$.*

We remark here that if eash G_i is abelian then we often use the terminology "direct sum" for weak direct product. The notation $\oplus_{i\in I} G_i$ will be used.

Theorem 3.4.3. *If $\{G_i\}_{i\in I}$ is any family of groups, then*

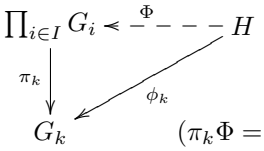
a) $\prod_{i\in I} G_i$ is a group.

b) $\forall k \in I, \pi_k : \prod_{i\in I} G_i \longrightarrow G_k$ *given by* $\pi_k(\{a_i\}) = a_k$ *is an epimorphism of groups.*

Proof. Easy. □

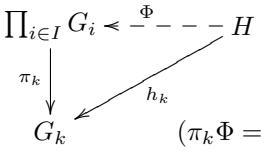
The next result is the universal mapping property (UMP) of the direct products.

Theorem 3.4.4. *Let* $\{G_i\}_{i\in I}$ *be a family of groups and* $\{\phi_i : H \longrightarrow G_i | i \in I\}$ *group homomorphisms. Then there exists a unique* $\Phi : H \longrightarrow \prod_{i\in I} G_i$ *such that* $\pi_i\Phi = \phi_i, \forall i \in I$. *The direct product is uniquely determined (up to isomorphism) with respect to this property.*

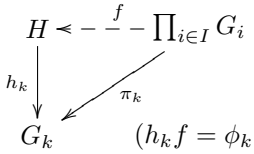


Proof. We define $\Phi : H \longrightarrow \prod_{i\in I} G_i$ by $\Phi(h) = \{\phi_i(h)\}_{i\in I}$. It is easy to see that Φ is a homomorphism making the diagram commute. To see uniqueness of Φ let ξ be another such map. Note that $\xi(h) = \{x_i\}_{i\in I}$. Now observe that $\pi_i\xi = x_i = \phi_i(h)$.

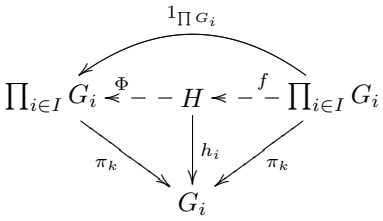
To see that the direct product is the unique solution to this UMP, suppose that H (equipped with maps $h_i : H \longrightarrow G_i$. So given we have the following:



since $\prod_{i\in I} G_i$ is a solution to the universal mapping problem. But H is a solution so we get a similar diagram:



Gluing together the diagrams in the obvious fashion, we obtain



Note the the identity map is a solution to the UMP, and by uniqueness, this must be the solution. We obtain therefore that

$$\Phi \circ f = 1_{\prod_{i\in I} G_i}$$

using the symmetric picture we get that

$$f \circ \Phi = 1_H$$

so we get that $H \cong \prod_{i\in I} G_i$.

□

Theorem 3.4.5. *If $\{G_i\}_{i\in I}$ is a family of groups, then*

a) $\coprod_{i\in I} G_i \lhd \prod_{i\in I} G_i$,

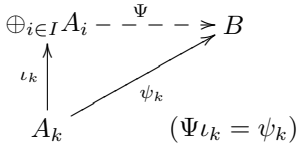
b) $\forall k \in I$, *the map* $\iota_k : G_k \longrightarrow \coprod_{i\in I} G_i$ *given by* $\iota(x) = \{x_i\}$ *where* $x_i = e_{G_i}$ *if* $i \neq k$ *and* $x_k = x$ *is a monomorphism of groups,*

c) $\forall k \in I$, $\iota_k(G_k) \lhd \prod_{i\in I} G_i$.

Proof. Exercise. □

We specialize to the abelian case for weak direct product to obtain a dual universal mapping property.

Theorem 3.4.6. *Let A_i be a family of abelian groups. If B is an abelian groups and $\{\psi_i : A_i \longrightarrow B\}$ is a family of homomorphisms then there exists a unique $\Psi : \oplus_{i\in I} A_i \longrightarrow B$ such that $\Psi\iota_k = \psi_k$ for all $k \in I$. The property determines the direct sum uniquely up to isomorphism.*



Proof. Recall that if $\{x_i\} \in \oplus_{i\in I} A_i$, then only finitely many of the x_i are nonzero. We define $\Psi : \oplus_{i\in I} A_i \longrightarrow B$ via $\Psi(\{x_i\}) = \sum_{x_i \text{ nonzero}} \psi_i(x_i)$.

It is easy to see that $\Psi\iota_k = \psi_k$ for all $k \in I$ and that Ψ is a homomorphism. It is also pretty easy to see that Ψ (and the direct sum) are both unique and the proof is dual.

□

Theorem 3.4.7. *Let $N_i \lhd G$ be such that*

a) $G = \langle \bigcup_{i\in I} N_i \rangle$ *and*

b) $\forall k \in I, N_k \bigcap \langle \bigcup_{i\neq k} N_i \rangle = \{e_G\}$.

Then $G \cong \coprod_{i\in I} N_i$.

Proof. We first remark that is $a \in N_i$ and $b \in N_j$ with $i \neq j$ then $ab = ba$ because of the intersection property (the commutator of a and b is an element of $N_i \bigcap N_j = \{e\}$.

Let the sequence $\{a_i\}$ be an element of $\coprod_{i\in I} N_i$ and recall that a_i is the identity almost everywhere. Let $I_0 \subseteq I$ be the subset of I such that $a_i \neq e_i$ for all $i \in I_0$.

Now consider $\phi : \coprod_{i\in I} N_i \longrightarrow G$ via

$$\phi(\{a_i\}) = \prod_{i\in I_0} a_i$$

(you should verify that this is a homomorphism).

Any element is a finite product of elements from the N_i's. Write $g \in G$ as $\prod a_i$ (recall that the elements of different N_i's commute). It is now obvious that g has preimage $\{y_i\}$ where $y_i = a_i$ if $i \in I_0$ and is the identity otherwise.

Now for one to one, let's look at $\ker(\phi)$. $\phi(\{a_i\}) = \prod_{i\in I_0} a_i = e$. For convenience we will write this relation as

$$a_1 a_2 \cdots a_n = e.$$

Note that $a^{-1} \in N_1 \bigcap \langle N_2 \bigcup N_3 \bigcup \cdots \bigcup N_n \rangle = e$ By induction each $a_i = e$ and the map is 1-1. □

Here are some quick last results.

Corollary 3.4.8. *Let $N_i \lhd G$. G is the (internal) weak direct product of the family $\{N_i\} \iff$ every nonidentity $a \in G$ can be written uniquely as $a_{i_1} a_{i_2} \cdots a_{i_n}$ where i_j are distinct elements of I ($a_{i_j} \neq e$).*

Theorem 3.4.9. *Let $f_i : G_i \longrightarrow H_i$ be homomorphisms and $f = \prod f_i$ be the map from $\prod G_i$ to $\prod H_i$ given by $f(\{a_i\}) \mapsto \{f_i(a_i)\}$. Then f is a homomorphism such that $f(\coprod G_i) \subseteq \coprod H_i$. $ker(f) = \prod ker(f_i)$, $im(f) = \prod im(f_i)$. So f is 1-1 and onto $\iff$ each f_i is.*

Corollary 3.4.10. *Let N_i, G_i be families of groups such that $N_i \lhd G_i$ $\forall i$.*

a) $\prod N_i \lhd \prod G_i$ *and* $\prod G_i / \prod N_i \cong \prod (G_i/N_i)$.

b) $\coprod N_i \lhd \coprod G_i$ *and* $\coprod G_i / \coprod N_i \cong \coprod (G_i/N_i)$.

Proof. For both of these just use the first isomorphism theorem. □

EXERCISES:

1. Show that to achieve the universal mapping property for direct sums, abelian is really needed.

2. Show that neither S_n nor Q_8 can be decomposed as a direct product of its proper subgroups.

3. Let G be cyclic. Show that $G \cong H \oplus K \iff |G| = n < \infty$ and n is not a prime number.

4. Let G be abelian with subgroups H and K. Show $G \cong H \oplus K$ if and only if there exist homomorphisms

$$H \underset{\iota_1}{\overset{\pi_1}{\leftrightarrows}} G \underset{\iota_2}{\overset{\pi_2}{\leftrightarrows}} K$$

such that

   (a) $\pi_1\iota_1 = 1_H$.
   (b) $\pi_2\iota_2 = 1_K$.
   (c) $\pi_1\iota_2 = 0$.
   (d) $\pi_2\iota_1 = 0$.
   (e) $\iota_1\pi_1 + \iota_2\pi_2 = 1_G$.

5. Every finitely generated abelian group of exponent p is isomorphic to $\oplus_{i=1}^{n}\mathbb{Z}_p$.

6. Let H, K, N be nontrivial normal subgroups of G and assume that $G = H \times K$. Show that $N \subseteq Z(G)$ or N intersects either H or K nontrivially.

7. Let G, H, K be abelian groups such that $G \cong H \oplus K$ and there exists $\phi : G \longrightarrow H$ a monomorphism of groups, then there exists a monomorphism $\psi : \oplus_{i=1}^{\infty}K \longrightarrow G$ (that is, G contains $\oplus_{i=1}^{\infty}K$ as a subgroup). Give an example to show that $G \ncong \oplus_{i=1}^{\infty}K$ in general.

3.5 Free Groups

Free groups are, in a certain sense, are the grandaddy of all groups. We have mentioned in class that every group is contained in a permutation group. There is a sort of dual notion here. We will see that every group is the homomorphic image of a free group.

Definition 3.5.1. *Let $x = \{x_i\}_{i\in I}$ be a set. A letter is an element $x_i \in X$. A word is a formal (finite) product of the form*

$$x_{i_1}^{\epsilon_1}x_{i_2}^{\epsilon_2}\cdots x_{i_k}^{\epsilon_k}$$

where each x_{i_j} is a letter and $\epsilon_j \pm 1$. We often write the word as a reduced word:

$$x_{i_1}^{a_1}x_{i_2}^{a_2}\cdots x_{i_k}^{a_k}$$

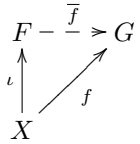
where $a_i \in \mathbb{Z}$ (obtained by grouping consecutive elements with the same index). The word is reduced if no two consecutive i_j and i_{j+1} are the same.

Theorem 3.5.2. *If X is a set then $F = F(X) = \langle X \rangle$ is a group under multiplication described above (forming words). F is called the free group on the set X.*

Proof. Exercise. □

Example 3.5.3. $\langle \emptyset \rangle = \{e\}$. $\langle a \rangle \cong \mathbb{Z}$. *If $|X| \geq 2$ then $F(X)$ is nonabelian. If $|X| \geq 1$ then every element of $F(X)$ is of infinite order.*

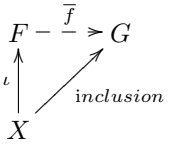
Theorem 3.5.4. *Let F be free on X and $\iota : X \longrightarrow F$ the inclusion map. If G is a group and $f : X \longrightarrow G$ is a map of sets then there exists a unique homomorphism of groups $\overline{f} : F \longrightarrow G$ such that $\overline{f}\iota = f$.*



Proof. Define $\overline{f} : F \longrightarrow G$ by $\overline{f}(e_F) = e_G$ and $\overline{f}(x_1^{a_1} \cdots x_n^{a_n}) := (f(x_1))^{a_1} \cdots (f(x_n))^{a_n}$. It is easy to see that $\overline{f}$ is a homomorphism satisfying $\overline{f}\iota = f$. Also if $g : F \longrightarrow G$ is another such homomorphism then $g(x_1^{a_1} \cdots x_n^{a_n}) = g(x_1)^{a_1} \cdots g(x_n)^{a_n} = g(\iota(x_1))^{a_1} \cdots g(\iota(x_n))^{a_n} = f(x_1)^{a_1} \cdots f(x_n)^{a_n} = \overline{f}(x_1^{a_1} \cdots x_n^{a_n})$. Hence $\overline{f}$ is unique. □

Corollary 3.5.5. *Every group G is the homomorphic image of a free group.*

Proof. Let G be generated by the set X and let F be the free group on the set X. Consider the diagram



As $\mathrm{im}(\overline{f})$ contains all generators of G, $\mathrm{im}(\overline{f}) = G$. □

We note that $G \cong F/N$ where $G = \langle X \rangle$, F is free on X and $N = \ker(\overline{f})$ where $\overline{f} : F \longrightarrow G$. So in effect we can understand G if we merely know X and N. In N we have "relations" $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} = e$ (that is, $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ is a generator of N. N is the smallest normal subgroup of F containing all the relations.

Definition 3.5.6. *Let X be a set and Y a set of reduced words on X. G is said to be the group defined by the generators $x \in X$ and the relations $w = e$, $(w \in Y)$ provided $G \cong F/N$ where F is free on X and $N \lhd F$ is generated by Y. One says that $(X|Y)$ is a presentation of G.*

Theorem 3.5.7. *Let X be a set, Y a set of reduced words, and G the group defined by the generators $x \in X$ and $w = e$, $(w \in Y)$. If H is any group such that $H = \langle X \rangle$ and H satifies all the relations $w = e$, $(w \in Y)$ then there is a ring epimorphism $\phi : G \longrightarrow H$.*

Proof. Let $F = F(X)$ and $X \xrightarrow{\text{inclusion}} H$. By the previous this induces an epimorphism $\phi : F \longrightarrow H$. Therefore as H satisfies all relations in Y, $Y \subseteq \ker(\phi)$, so there is $\overline{\phi} : F/N \longrightarrow H/\{0\} \cong H$. Therefore $G \longrightarrow F/N$ is onto. □

Example 3.5.8. *a)* $D_n = \langle a, b | a^n = 1 = b^2, bab = a^{-1} \rangle$.

b) $C_n = \langle a | a^n = e \rangle$.

c) $Q_8 = \langle a, b | a^4 = e = a^2 b^{-2} = abab^{-1} \rangle$.

We will briefly introduce the notion of free products. The idea is that words are allowed to be reduced via theor groups. (So the relations of the separate groups in the free product are employed.) For example $\mathbb{Z}_2 * \mathbb{Z}_3 = \{a_1 b_1 \cdots a_n b_n | a_i \in \mathbb{Z}_2, b_i \in \mathbb{Z}_3\}$.

Theorem 3.5.9. *Let G_i be a family of groups and $\prod_{i \in I}^* G_i$ their free product. If $\psi_i : G_i \longrightarrow H$ are homomorphisms, then there is a unique homomorphism $\Phi : \prod_{i \in I}^* G_i \longrightarrow H$ such that $\Phi \iota_k = \psi_k$ for all $k \in I$. This property uniquely determines the free product up to isomorphism.*

Proof. Exercise. □

EXERCISES:

1. Use properties of free groups to classify all cyclc groups.

2. Let F be a free group and $n \in \mathbb{Z}$. $N = \langle \{x^n | x \in F\} \rangle$. Show that $N \lhd F$.

3. Let F be free hunter on X and let $Y \subseteq X$. If H is the smallest normal subgroup of F containing Y, show that F/H is free.

4. The group generated by a and b subject to the relations $a^8 = b^2 b^4 = ab^{-1}ab = e$ has order no more than 16.

5. The cyclic group of order 6 is generated by a and b and the relations $a^2 = b^3 = a^{-1}b^{-1}ab = e$.

6. Change the previous problem to the group generated by a and b and the relations $a^2 = b^3 = e$ then the group that we get is $\mathbb{Z}_2 * \mathbb{Z}_3$.

3.6 Free Abelian Groups

In this section we will always assume that our groups are abelian. "Free abelian" is sort of like free except that there are enough relations to ensure that all elements commute...no more and no less. Basically an element of a free abelian group looks like a word (as it did in the free case) but now we have the added condition that we can commute the elements of the group.

In this section, since our groups are abelian, we will write the notation additively and we will see that there is a convenient way to think about "free abelian" in terms of "bases".

If A is our abelian group and X is a subset of A then we write

$$\langle X\rangle = \{\sum_{i=1}^{k} n_i x_i | n+i \in \mathbb{Z}, x_i \in X\}$$

Note that if $|X| = 1$ then $\langle X\rangle$ is cyclic.

Definition 3.6.1. *We say that the set X is linearly independent if for every finite subset $\{x_1, \cdots, x_n\} \subseteq X$, the relation*

$$m_1x_1 + m_2x_2 + \cdots + m_nx_n = 0$$

implies that $m_i = 0, \forall 1 \leq i \leq n$.

Definition 3.6.2. *A basis for F (if it exists) is a linearly independent subset $X \subseteq F$ such that $\langle X\rangle = F$.*

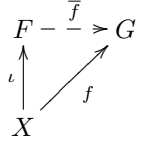
Theorem 3.6.3. *Let F be an abelian group. TFAE*

a) F has a nonempty basis.

b) F is the internal direct sum of a family of infinite cyclic groups.

c) $F \cong \sum \oplus_{i\in I}\mathbb{Z}$.

d) There is a nonempty set X and a function $\iota : X \longrightarrow F$ such that given any abelian group A and function $f : X \longrightarrow A$, there is a unique homomorphism $\overline{f} : F \longrightarrow A$ such that $\overline{f}\iota = f$.



Proof. For a) implies b), we assume that F possesses a basis and it suffices to show that there is a family of infinite cyclic groups $\langle x\rangle_{x\in X}$ such that $F = \langle\bigcup_{x\in X}\langle a\rangle\rangle$ and $\langle y\rangle \bigcap \langle\bigcup_{x\neq y}\langle x\rangle\rangle = 0$.

Let X be our basis. Note that $nx = 0$ implies that $n = 0$ as X is linearly independent. Assume that there is a $y \in X$ such that

$$ny = m_1x_1 + \cdots + m_kx_k$$

of course this means that

$$0 = -ny + m_1x_1 + \cdots + m_kx_k$$

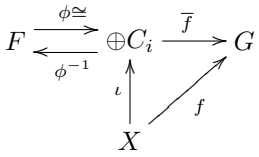
which means that $m_i = 0 = n$ and hence $\langle y\rangle \bigcap \rangle \bigcup_{x\neq y}\langle x\rangle\rangle = 0$ and hence $F \cong \oplus_{x\in X}\langle x\rangle$.

The implication 2) implies 3) is easy.

For 3) implies 4) we write F as $\oplus_{i\in I}C_i$ with $C_i \cong \mathbb{Z}$ with generator x_i. Let $X = \{x_i\}_{i\in I}$ and let $\iota : X \longrightarrow F$ be inclusion ($x_i \mapsto \{y_i\}$ where $y_j = x_i$ if $i = j$ and the identity otherwise). Let $f : X \longrightarrow G$; we define $\overline{f}$ by $\overline{f}(\{n_ix_i\}_{i\in I}) = \sum_{i\in I} n_if(x_i)$ (which makes sense as $n_i = 0$ a.e.).

Clearly $\overline{f}\iota = f$ and $\overline{f}$ is a homomorphism.

To see uniqueness assume that $g : \oplus C_i \longrightarrow G$ is such that $g\iota = f$. Note that $g(\{n_ix_i\}) = \sum n_ig(x_i) = \sum n_ig\iota(x_i) = \sum n_if(x_i)$ and hence $g = \overline{f}$. A technical note (since we did this for $\oplus\mathbb{Z}$).



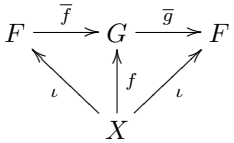
For F, ι becomes $\phi^{-1}\iota$ and $\overline{f}$ becomes $\overline{f}\phi$.

Finally for 4) implies 1), a reasonable candidate for a basis of F is $\iota(X)$. Define G to be the group $\oplus_{x\in X}\mathbb{Z}$ and $f : X \longrightarrow G$ the obvious inclusion map of sets. Note that $f(X)$ is a linearly independent subset of G. Assume that $\iota(X)$ is linearly dependent in F. Then

$$\sum n_i\iota(x_i) = 0$$

with not all $n_i = 0$. So $\sum n_i\overline{f}\iota(x_i) = 0 = \sum n_if(x_i)$. We therefore conclude that $n_0 \equiv 0$ which is a contradiction. This shows that $\iota(X)$ is linearly independent. It now suffices to show that $\iota(X)$ spans F.

As $G = \oplus_{x\in X}\mathbb{Z}$, G has the mapping property by 3) implies 4). We have the diagram



Uniqueness implies that $\overline{g}\overline{f} = 1_F$ and hence $F \cong G$. Finally observe that $\overline{g}(f(X)) = \mathrm{im}(\overline{g}) = F = \iota(X)$. This concludes the proof. □

We remark that an abelian group satisfying one, hence all, of the above conditions is called a free abelian group. They are completely determined up to isomorphism by their "size".

Theorem 3.6.4. *Any two bases of a free abelian group have the same cardinality. What is more, two free and abelian groups are isomorphic if and only if their respective bases have the same cardinality.*

Remark 3.6.5. *If F is a free abelian group with basis X then we call $|X|$ the rank of F.*

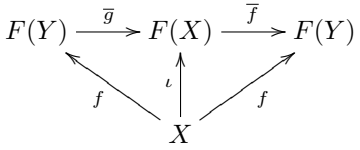
Proof. We will prove the case where the two bases of F are finite. Assume that F has two bases X and Y with $|X| = n$ and $|Y| = m$. So in particular, F is isomorphic to both n and m copies of (Z) (as a direct sum). So F has a homomorphic image (consider the subgroup that looks like $2F$)

$$\oplus_{i=1}^{n} \mathbb{Z}_2.$$

Additionally if k is an integer $k \leq m$ then $|F/2F| \geq 2^k$. It follows that $m = n$.

A similar argument shows that if F has an infinite basis then every basis of F is infinite. For the rest of proof, it suffices to show that is F has an infinite basis $|X|$ then $|F| = |X|$. This is reasonablly straightforward.

Now suppose that $F_1 \cong^{\alpha} F_2$. If X is a basis of F_1, then $\alpha(X)$ is a basis of F_2. On the other hand if X and Y are two sets of equal cardinality (say that the bijection is f), consider the diagram



Since there is a symmetric diagram it is easy to see that $F(X) \cong F(Y)$. □

Theorem 3.6.6. *Every abelian group A is the homomorphic image of a free abelian group (this free abelian group can be chosen of rank $|X|$ where $\langle X \rangle = A$...in particular if A is finitely generated then F can be chosen finitely generated).*

Proof. Similar to the more general result on free groups. □

Lemma 3.6.7. *If $\{x_1, \cdots, x_n\}$ is a basis for a free abelian group and $a \in \mathbb{Z}$ then for all $i \neq j$, $\{x_1, \cdots, x_{j-1}, x_j + ax_i, x_{j+1}. \cdots x_n\}$ is also a basis.*

Proof. It is easy to see that the two sets generate the same group. Linear independence is also a straightforward computation. □

This next result will be useful in the classification of finitely generated abelian groups.

Theorem 3.6.8. *Let F be a free abelian group of rank $n < \infty$. If A is a nonzero subgroup of F then there exists a basis $\{x_1, \cdots, x_n\}$ of F, an integer r $(1 \leq r \leq n)$ and positive integers $d_1|d_2|\cdots|d_r$ such that A is free abelian with basis $\{d_1x_1, \cdots, d_rx_r\}$.*

Remark 3.6.9. *We note that as a direct consequence of this, any subgroup of a free abelian group is also free of rank not exceeding the rank of the parent group.*

Proof. The case $n = 1$ is easy. We assume the result for all free abelian groups of rank less than n. Let S be the set of integers such that there exist a basis $\{y_1, \cdots, y_n\}$ of F and an element of A of the form

$$sy_1 + k_2y_2 + \cdots + k_ny_n.$$

Note that all of the k_i's are in S as well. Since $A \neq 0$ then $S \neq \emptyset$. So there is a smallest positive integer (say d_1) in S. And for some basis of F there is an element $v \in A$ such that

$$v = d_1y_1 + k_2y_2 + \cdots + k_ny_n.$$

Using the Euclidean algorithm we write each k_i:

$$k_i = d_1q_i + r_i$$

with each $0 \leq r_i < d_1$. We obtain that

$$v = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n$$

Letting $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$, we note that the set $W = \{x_1, y_2, \cdots, y_n\}$ is a basis for F by the previous lemma. Since $d_1 > r_i$ and d_1 is minimal, this implies that $r_i = 0$ for $2 \leq i \leq n$. And hence $v = d_1x_1$.

Now $H = \{y_2, \cdots, y_n\}$ is free abelian (it has the set as a basis) such that $F = \langle x_1 \rangle \oplus H$. We claim that $A = \langle v \rangle \oplus (A \bigcap H)$. Since $\{x_1, y_2, \cdots, y_n\}$ is a basis, it is easy to see that $\langle v \rangle \bigcap (A \bigcap H) = 0$. Now let

$$u = t_1x_1 + t_2y_2 + \cdots + t_ny_n \in A$$

with $t_1 = d_1q_1 + r_1$ with $r_1 < d_1$. So A contains

$$u - q_1v = r_1x_1 + \cdots + t_ny_n \in H \bigcap A$$

and hence by the minimality of d_1, $r_1 = 0$.

So

$$u = q_1v + \cdots + t_ny_n$$

and this establishes the claim.

Finally we note that if $A \bigcap H = 0$, then we are done (A is singly generated by d_1x_1). If $A \bigcap H \neq 0$ then by induction there is a basis $\{x_2, \cdots, x_n\}$ of H and positive integers $d_2|d_3|\cdots|d_r$ such that $A \bigcap H$ is free abelian with basis

$\{d_2x_2, \cdots, d_rx_r\}$. Since $F = \langle x_1 \rangle \oplus H$ and $A = \langle d_1x_1 \rangle \oplus (A \bigcap H)$, it is easy to see that $\{x_1, x_2, \cdots, x_n\}$ is a basis of F and that $\{d_1x_1, \cdots, d_rx_r\}$ is a basis of G. The only thing left is is to show that $d_1|d_2$. We write $d_2 = qd_1 + r$ with $0 \leq r < d_1$. Since $\{x_1 + qx_2, x_2, x_3 \cdots, x_n\}$ is a basis of F and $d_1(x_1 + qx_2) + rx_2 = d_1x_1 + d_2x_2 \in G$ the minimality of d_1 in S implies that $r = 0$. This completes the proof.

□

Corollary 3.6.10. *If G is a finitely generated abelian group generated by n elements, then any subgroup $H \subseteq G$ can be generated by m_H elements with $m_H \leq n$.*

Remark 3.6.11. *The previous corollary may be wildly untrue if G is not abelian.*

3.7 The Structure Theorem for Finitely Generated Abelian Groups

In this section we will classify completely all finitely generated abelian groups. Basically it is easy to see...they are all basically just some finite number of copies of $\mathbb{Z}$ (the "free part") and the finite part (and we will see a couple of canonical ways to write this part).

Here is the main structure theorem of this section.

Theorem 3.7.1. *Every finitely generated abelian group is isomorphic to a finite direct sum of cyclic groups in which the finite cyclic summands (if any) are of order $m_1|m_2|\cdots|m_t$.*

Remark 3.7.2. *So any finitely generated ableian group is of the form:*

$$F \oplus T$$

where

$$F \cong \oplus_{i=1}^{n} \mathbb{Z}$$

with $n \geq 0$ and

$$T \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}$$

where $t \geq 0$ and if $t > 0$ then $m_1|m_2|\cdots|m_t$.

The proof of this is fairly straightforward and depends on the results from the previous section.

Proof. Let A be finitely generated, say by n elements. Then A is the homomorphic image of F a free abelian group on n elements. Consider $\pi : F \longrightarrow A$. If π is one to one then we are done. If not then $\ker(\pi)$ can be generated by $\{d_1x_1, d_2x_2, \cdots, d_rx_r\}$ where $\{x_1, x_2, \cdots, x_n\}$ is a basis for F and $d_1|d_2|\cdots|d_r$.

It is now easy to see that

$$A \cong F/K \cong \oplus\langle x_i\rangle / \oplus \langle d_i x_i\rangle \cong (\oplus\mathbb{Z}_{d_i}) \oplus (\oplus\mathbb{Z})$$

with $s = n - r$.

□

Lemma 3.7.3. *Let C_n be a cyclic group of order n. If $n = ab$ with $gcd(a, b) = 1$ then $C_n \cong C_a \oplus C_b$.*

Proof. Since cyclic groups are isomorphic to $\mathbb{Z}_n$ we can couch the proof in these terms. Show that the map

$$\phi : \mathbb{Z}_{ab} \longrightarrow \mathbb{Z}_a \oplus \mathbb{Z}_b$$

(with a and b relatively prime) obtained by reducing each element modulo a and b respectively is an isomorphism. □

Definition 3.7.4. *A group is called torsion if every element is of finite order*

Basically we can break down a finitely generated abelian group into a torsion part and a free part.

Theorem 3.7.5. *If G is a finitely generated abelian group then there is a unique nonnegative integer s such that the number of infinite cyclic summands in the decomposition in G is precisely s. What is more if G is not free abelian, there is a unique list of integers $m_1|\cdots|m_t$ such that the torsion part of G is isomorphic to*

$$\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}.$$

(Invariant factors)
Likewise

$$\mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}}.$$

(Elementary divisors).

EXERCISES:

1. If G is a finite abelian group and $H \subseteq G$ is a subgroup, show that G has a subgroup isomorphic to G/H.
2. Show that any finitely generated subgroup of $\mathbb{Q}$ (resp. $\mathbb{Q}/\mathbb{Z}$) is cyclic.
3. Find all abelian group of order 13,500.
4. Show that if G is a finite abelian group that is not cyclic, then G contains (an isomorphic copy of) $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Chapter 4

The Structure of Groups

4.1 The Action of a Group on a Set

This is the section where we can get a good feel for what groups are really "for". The action of a group on a set is one of the main questions of applications (e.g. the action of the group of symmetries on the Rubik's cube, or on a molecular lattice). It should also be noted that many of our earlier examples are motivated by actions (e.g. D_n and S_n).

Definition 4.1.1. *Let G be a group and A a set. An action of G on A is a function $G \times A \longrightarrow A$ such that $\forall a \in A$,*

$$(g_1 g_2)a = g_1(g_2 a)$$

and

$$e_G a = a$$

for all $a \in A$.

Example 4.1.2. *Of course there is always the trivial action. Also one can allow $A := G$ and let G act on itself. As a last example, S_n acts on $\{1, 2, \cdots, n\}$.*

Here are some more large classes of important examples. These are important enough to have their own names.
Translation: Let H be a subgroup of G. Of course H acts on G via the group multiplication. But also G acts on the set of left cosets of H in G ($x(gH) = (xg)H$).
Conjugation If H is normal in G via $(g, h) = g^{-1}hg$. If H is any subgroup of G then H acts on G via $(h, g) = h^{-1}gh$. Also H acts on the set of subgroups of G via $(h, K) = h^{-1}Kh$.

Theorem 4.1.3. *Let G act on A.*

a) *The relation $x \sim x'$ (on A) if and only if $gx = x'$ for some $g \in G$ is an equivalence relation.*

b) *For all $x \in A$, $G_x = \{g \in G | gx = x\}$ is a subgroup of G called the stabilizer of x.*

Proof. Exercise. □

Definition 4.1.4. *Let G act on A and $x \in A$. The orbit of x ($orb(x)$) is the set $\{gx | g \in G\}$.*

We now define some of the "action terminology".

Definition 4.1.5. *Let G act on the set S. We define:*

a) *The kernal of the action to be $\{g \in G | gx = x, \ \forall x \in S\}$.*

b) *The action is faithful if the kernal of the action is the identity.*

Example 4.1.6. *Let G act on itself by conjugation then the orbit of $x \in G$ is precisely $\{g^{-1}xg | g \in G\}$. If H is a subgroup which acts on G by conjugation, then $_x = \{h \in H | h^{-1}xh = x\}$ is the centralizer of $x \in H, C_H(x)$. If $H = G$ this is just the earlier defined centralizer.*

Finally if H acts on the set of subgroups of G by conjugation, then the subgroup of H fixing some K is $\{h \in H | h^{-1}Kh = K\}$ is the normalizer of K in H, denoted $N_H(K)$ (if $H = G$ this is just the earlier defined normalizerof K). Note that $K \lhd N_G(K)$ ad $K \lhd G \iff N_G(K) = G$.

Definition 4.1.7. *Let G act on the set A. We say that G acts transitively on A if for all $x, y \in A$, there exists $g \in G$ such that $gx = y$.*

Equivalently, we can say that G acts transitively on A is there is a unique orbit in A.

One might ask how many ways are there for a group G to act on a set A. This will be answered presently (our notation will be that if A is a set, then S_A is the set of all permutations of A).

Theorem 4.1.8. *Let G be a group and A a nonempty set. Then there is a bijective correspondence between the set of actions of G on A and the set of homomorphisms from G to S_A. This correspondence is given by the rule that if $\phi : G \longrightarrow S_A$ then ϕ corresponds to the action $gx = (\phi(g))x$.*

Proof. Clearly a homomorphism ϕ gives rise to an action on A via the above rule. We will show that this correspondence is 1-1 and onto. Suppose first that ϕ and ψ give rise to the same action. So if $g \in G$, then $\phi(g)x = \psi(g)x$ for all $x \in A$. Therefore $\phi(g)$ and $\psi(g)$ must be the same element of S_A by definition. Hence $\phi(g) = \psi(g)$, but since g is arbitrary, we have the $\phi = \psi$.

Now let G act on A (we must show that this action "comes from" a homomorphism $\phi : G \longrightarrow S_A$). Given this action we define $phi : G \longrightarrow S_A$ via

$$\phi(g) = \sigma_g \in S_A$$

where $\sigma_g(x) = gx$.

First we note that σ_g is a permutation; indeed, if $\sigma_g(x) = \sigma_g(y)$ then $x = y$. Also note that if $x \in A$, then $g^{-1}x = y \in A$ and hence $x = gy = \sigma_g(y)$. It is also easy to see that $\sigma_{g_1 g_2} = \sigma_{g_1}\sigma_{g_2}$ and so ϕ is a homomorphism. □

Example 4.1.9. *Show that the "permutation representation of* $\mathbb{Z}_6$ *is* $\{e, (0\,1\,2\,3\,4\,5), (0\,2\,4)(1\,3\,5), (0\,3)(1\,4)(2\,5),$ *Do the same for* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

This next result is an important one. The length of the orbit of some $x \in A$ is the index of the stabilizer.

Theorem 4.1.10. *If G acts on A then the length of the orbit of $x \in A$ is $[G : G_x]$.*

Proof. We first do a computation to make an observation. Suppose that $gx = hx$ with $g, h \in G$ and $x \in A$. This is equivalent to the statement that $h^{-1}gx = x$, which is equivalent to saying that $h^{-1}g \in G_x$. This holds if and only if $gG_x = hG_x$.

We now consider the map from left cosets of G_x in G given by

$$gG_x \mapsto gx.$$

This map is clearly onto. By the above computation, it is also 1-1. This establishes this theorem. □

The next theorem highlights an important application of group actions which will prove quite useful in studying the structure of groups.

Theorem 4.1.11. *Let G be a group and H a subgroup of G. Let G act by translation (left multiplication) on the set of left cosets of H in G (we will call this set A). Let π_H be the associated permutation representation of this action.*

a) G acts transitively on A.

b) The stabilizer of $1H \in A$ is H.

c) The kernal of this action is $\bigcap_{x \in G} xHx^{-1}$ and the kernal of π_H is the largest normal subgroup of G contained in H.

Proof. For a) let $xH, yH \in A$. If $g = yx^{-1}$ then $g(xH) = yH$.

For b) we note first that clearly H is contained in the stabilizer of $1H$. So suppose that $g(1H) = H$. This implies that $gh = h'$ for some $h, h' \in H$. Hence $g = h'h^{-1} \in H$.

For c) note that $\ker(\pi_H) = \{g \in G | g(xH) = xH,\ \forall x \in G\} = \{g \in G | x^{-1}gxH = H,\ \forall x \in G\} = \{g \in G | x^{-1}gx \in H,\ \forall x \in G\} = \{g \in G | g \in xHx^{-1},\ \forall x \in G\}$. Hence $\ker(\pi_H) = \bigcap_{x \in G} xHx^{-1}$.

Now note that $\ker(\pi_H)$ is normal in G (and H). Now suppose that $N \lhd G$ and N is contained in H. Hence N is contained in $xNx^{-1} \subseteq xHx^{-1}$. So $N \subseteq \bigcap xHx^{-1}$ □

Here is a cool example.

Example 4.1.12. *The question here is "is there a subgroup of A_5 of order 20? (There is a subgroup of S_5 of order 20). Assume that there is a subgroup H of A_5 of order 20. The length of the orbit of H (under conjugation action) is either 1 or 3. If the length is 1 this implies that H is normal in A_5 which cannot be. Hence the length of the orbit is 3. So there are 3 conjugates of H in G. This induces a homomorphism from A_5 to S_3. Since S_3 is much smaller, the kernal must be nontrivial, which means that the kernal is all of A_5. But this implies (again) that H is normal in A_5.*

Proposition 4.1.13. *Let G be a finite group and $x \in G$.*

a) The number of elements in the conjugacy class of x is $[G : C_G(x)]$ which divides $|G|$.

b) If $\overline{x_1}, \overline{x_2}, \cdots, \overline{x_n}$ are the conjugacy classes in G, then

$$|G| = \sum_{i=1}^{n} [G : C_G(x)].$$

c) If K is a subgroup of G then the number of subgroups of G conjugate to K is $[G : N_G(K)]$ which $|G|$.

We remark that the equation in part b) is called the *class equation*.

Proof. For a) the orbit of x under the conjugation action is the set of elements of the form $g^{-1}xg$ with $g \in G$. Since the stabilizer is clearly $C_G(x)$, the result follows from the previous theorem. For the last statement, notice that $|G| = [G : C_G(x)]|C_G(x)|$.

For b) note that each $[G : C_G(x_i)]$ counts the conjugates of x_i. Since $\overline{x_1}, \overline{x_2}, \cdots, \overline{x_n}$ is an exhaustive list of the conjugacy classes, each element of G is contained in one of them (and hence $|G| \leq \sum_{i=1}^{n} [G : C_G(x)]$. To show the other inequality it suffices to show the the conjugacy classes are disjoint (but this is clear as conjugacy is an equivalence relation).

For c) first note (for the last statement) that $|G| = [G : N_G(K)]|N_G(K)|$. The number of subgroups of G conjugate to K is precisely the length of the orbit of K and is hence $[G : N_G(K)]$. □

We now note an important corollary (Cayley's theorem) to the corrspondence theorem between group actions G on A and homomorphisms from G to S_A. This theorem shows that any group can be thought of as a subgroup of some permutation group.

Theorem 4.1.14. *If G is a group then there is a group monomorphism from G to A_S. Hence every group is isomorphic to a group of permutations. What is more, if $|G| = n$ then G is isomorphic to a subgroup of S_n.*

Proof. Let G act on itself by left translation. This induces a homomorphism $\pi : G \to S_G$ (where S_G means the permutations on the underlying set of G). Suppose that $g \in \ker(\pi)$. We have that $\pi(g)$ is the identity permutation, hence

$$\pi(g)(x) = x = gx, \ \forall x \in G.$$

And hence $g = e_G$ and π is 1-1. □

Corollary 4.1.15. *Let G be a group*

a) For all $g \in G$ conjugation by g induces an automorphism $G \longrightarrow G$.

b) There exists a homomorphism $\phi : G \longrightarrow Aut(G)$ whose kernal is $Z(G)$.

Proof. Exercise. □

Here is a more familiar form for the class equation.

Class Equation:

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(\overline{x_i})].$$

where $\overline{x_1}, \cdots, \overline{x_m}$, $(x_i \in G \setminus Z(G))$ are the distict conjugacy classes and $[G : C_G(\overline{x_i})] >$.

Here are some interesting consequences of some of this stuff.

Corollary 4.1.16. *If G is a finite group of order p^n where p is a prime, then the center of G is nontrivial.*

Proof. Apply the class equation. □

Corollary 4.1.17. *If $[G : H] = n$ and no nontrivial subgroup of G is contained in H, then G is isomorphic is a subgroup of S_n.*

Proof. Let G act on the left cosets of H in G by translation (we will call this set of cosets A). By the Theorem 4.1.11, the kernal of the homomorphism $G \longrightarrow S_A$ is contained in H. Since there are no nontrivial normal subgroups of H, this means that the homomorphism is trivial. Hence G is a subgroup of $S_A = S_n$. □

Corollary 4.1.18. *If G is a finite group and H is a subgroup of G of index p, where p is the smallest prime dividing the order of G then H is normal in G.*

Proof. Note that there are precisely p left cosets of H in G. We therefore have a homomorphism from G to S_p. Let K be the kernal of this homomorphism. Note that G/K is isomorphic to a subgroup of S_p. Note that

$$|G/K| \mid p!$$

and

$$|G/K||K| = |G|.$$

So every divisor of $|G/K|$ divides $|G|$. Since no prime smaller than p divides $|G|$, it follows that $|G/K|$ is either 1 or p. Since $|G/K| = |G/H||H/K|$ it follows in either case that $|H/K| = 1$. Hence $H = K \lhd G$. □

Corollary 4.1.19. *Any subgroup of index 2 is normal in G.*

Proof. 2 is the smallest prime period. □

It should be noted that the previous corollary is true even when G is infinite, but the above proof is for the finite case. In general, note that any left coset is a right coset.

EXERCISES:

1. Let G be a group and A an abelian normal subgroup. Show that G/A acts on A by conjugation and show that there is a homomorphism $G/A \longrightarrow \mathrm{Aut}(A)$.
2. Suppose that G is a group and $a \in G$ is an element that has precisely 2 conjugates in G. Show that G is not simple.
3. Let S be a set of at least 2 elements and suppose that G acts transitively on S. Show that
   a) If $x \in S$ then the orbit of x is all of S.
   b) $\forall x, y \in S$, G_x and G_y are conjugate.
   c) If G has the property that $\{g \in G | gx = x \ \forall x \in S\} = \{e_G\}$ and if $N \lhd G$ and $N \subseteq G$ for some $x \in S$ then $N = \{e\}$.
   d) $\forall x \in S$, $|S| = [G : G_x]$. In particular, if $|S|$ and $|G|$ are both finite then $|S| \mid |G|$.
4. Find all automorphisms of $\mathbb{Z}_6$. Note that none of these are inner automorphisms.
5. If $G/Z(G)$ is cyclic, then G is abelian.
6. Show that every automorphism of S_4 is an inner automorphism.
7. Let G be a group with an element of order greater than 2. Show that $\mathrm{Aut}(G)$ is nontrivial.
8. Let G be any group of order greater than 2. Show that $\mathrm{Aut}(G)$ is nontrivial.
9. Suppose that $|G| = pn$ with p a prime $p > n$. If $H \subseteq G$ is of order p, then $H \lhd G$.
10. If $N \lhd G$ and $|N| = p$ and $|G| = p^n$ then $N \subseteq Z(G)$.
11. Show that $\mathrm{Inn}(G) \cong G/Z(G)$.

4.2 The Sylow Theorems

These may be the most important (finite) group structural results. In this section p will always mean a (positive) prime integer.

Lemma 4.2.1. *Suppose that $|G| = p^n$ and that G acts on A, a finite set. If $S_0 = \{x \in S | gx = x \ \forall g \in G\}$ then $|S| \equiv |S_0| mod p$.*

Proof. An orbit $\overline{x}$ contains one element $\iff x \in S_0$. We write S as the disjoint union

$$S = S_0 \bigcup \overline{x_1} \bigcup \cdots \bigcup \overline{x_k}.$$

Each $|\overline{x_i}| = [G : G_{x_i}]$ so p divides $|\overline{x_i}|$. Hence $|S| = |S_0| + pm$. □

This next result is the celebrated Cauchy's Theorem (which depends heavily on p being prime).

Theorem 4.2.2. *If p is a prime dividing $|H|$ then G has an element of order p.*

Proof. Let S be the set of $p-$tuplesof elements of G, $(a_1, a_2, \cdots, a_p)$ such that $a_1 a_2 \cdots a_p = e_G$. Note that the first $p-1$ choices determine the last for "entries" determine the last. Hence $|S| = n^{p-1}$ where $n = |G|$. Since $p|n$ we have that $|S| \equiv 0 \mathrm{mod}(p)$.

We now let $\mathbb{Z}_p$ act on this set via the action

$$\overline{k}(a_1, a_2, \cdots, a_k, a_{k+1}, \cdots, a_p) = (a_k, a_{k+1}, \cdots, a_p, a_1, \cdots, a_{k-1}).$$

It is easy to verify that this is a group action.

Note $(a_1, a_2, \cdots, a_p) \in S_0$ if and only if $a_1 = a_2 = \cdots = a_p$ (and certainly $e = e = \cdots = e$ is in S_0 so S_0 is nonempty). So $vert S_0| \neq 0$, but $|S_0| \equiv |S| \mathrm{mod}(p)$ therefore there are at least p elements in S_0. So $(a, a, \cdots, a) \in S_0$ and hence $a^p = e$. □

Definition 4.2.3. *We say that G is a $p-$group if every element of G has order p^n for some integer $n \geq 0$.*

We remark that a finite group is a $p-$group $\iff |G| = p^n$.

Definition 4.2.4. *Let G be a finite group of order $p^n m$ where $gcd(p, m) = 1$. We say that a maximal $p-$subgroup of G (of order p^n) is called a Sylow $p-$subgroup of G.*

We also say that a subgroup H of G is a $p-$subgroup of G if H is a $p-$group. We now introduce the very important Sylow Theorems (possibly the most important structure theorems for finite groups).

Theorem 4.2.5. *Let $|G| = p^n m$ with $n \geq 1$ and $gcd(p, m) = 1$.*

I.) G contains a subgroup of order p^j for all $1 \leq j \leq n$ and every subgroup of order p^j is normal in some subgroup of order p^{j+1} for all $j < n$.

II.) If H is a $p-$subgroup of G and P is any Sylow $p-$subgroup of, then there an an $x \in G$ such that $H \subseteq x^{-1}Px$ (in particular, all Sylow $p-$subgroups are conjugate.

III.) If k is the number of Sylow $p-$subgroups of G, then k divides $|G|$ and $k \equiv 1 mod(p)$.

Let's look at some quick applications.

Example 4.2.6. *Look at the structure of groups of order pq. Also note that there is no simple group of order 56, 80, 36.*

Our proof the Sylow theorems requires the use of the following lemma.

Lemma 4.2.7. *If G is a finite group and H is a $p-$subgroup of G then $[N_G(H) : H] \equiv [G : H] mod(p)$.*

Proof. Let S be the set of left cosets of H in G and let H act on S by translation. Note that $|S| = [G : H]$. Now $xH \in S_0 \iff hxH = xH \ \forall h \in H \iff x^{-1}hx \in H \ \forall h \in H \iff x \in N_G(H)$.

So $|S_0|$ is equal to the number of cosets xH with $x \in N_G(H)$. Therefore $|S_0| = [N_G(H) : H] \equiv [G : H] \text{mod}(p)$. □

Corollary 4.2.8. *If H is a $p-$subgroup of the finite group G such that $p|\ [G : H]$ then $N_G(H) \neq H$.*

Proof. $[G : H] \equiv [N_G(H) : H] \text{mod}(p)$. Since $[G : H] \equiv 0 \text{mod}(p)$ we have that $[N_G(H) : H]$ must be at least p. □

Now we get to the proofs of the Sylow theorems.

Proof. I.) Since $p|\ |G|$, G must contain an element of order p. We proceed by induction (the previous statement taking care of the base case). Assume that H is a subgroup of G of order p^j with $1 \leq j < n$. Since $p|\ [G : H]$ and $H \lhd N_G(H)$, $H \neq N_G(H)$ by the previous lemma. Also note that $1 < |N_G(H)/H] = [N_G(H) : H] \equiv [G : H] \equiv 0 \text{mod}(p)$. We conclude that $p|\ |N_G(H)/H|$ and $N_G(H)/H$ contains a subgroup of order p. This subgroup is of the form H_1/H with H_1 a subgroup of G. Note that $H \lhd H_1$ and $|H_1| = |H|\ |H_1/H| = p^{j+1}$.

II.) Let S be the set of left cosets of P in G (P some Sylow $p-$subgroup of G) and let H act on S by translation. $|S_0| \equiv |S| \equiv [G : H] \text{mod}(p)$. But p does not divide $[G : P]$ and hence $|S_0| \neq 0$. So there is an $xP \in S_0$. Note that $xP \in S_0 \iff hxP = xP \ \forall h \in H \iff x^{-1}hxP = P \ \forall h \in H$. Hence $x^{-1}Hx \subseteq P$ and so $H \subseteq xPx^{-1}$. For the last statement, note that if H is a Sylow $p-$subgroup then $|H| = |P|$ and $H = xPx^{-1}$.

III.) By the previous, the number of Sylow $p-$subgroups is precisely the number of conjugates of any one of them (say P). This number is $[G : N_G(P)]$ which, of course, must divide $|G|$. Let S be the set of all Sylow $p-$subgroups and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q$ for all $x \in P$. This holds if and only if $P \subseteq N_G(Q)$. Both P and Q are Sylow $p-$subgroups of G (and hence of $N_G(Q)$) and hence P and Q are conjugate in $N_G(Q)$. But since $Q \lhd N_G(Q)$, $Q = P$. We conclude that $S_0 = P$. Since $|S| \equiv |S_0| \mathrm{mod}(p)$ and $|S_0| = 1$, we have that $|S| \equiv 1 \mathrm{mod}(p)$. So the number of Sylow $p-$subgroups of G is of the form $1 + kp$.

□

Example 4.2.9. *Some more demonstrations of the power of the Sylow theorems.*

4.3 Semidirect Products

Semidirect products provide a useful way for constructing non-abelian groups. What is more they are "easy" to identify.

Let G and H be groups and $\theta : H \longrightarrow \mathrm{Aut}(G)$ be a homomorphism. These are the tools used in the construction of the semidirect product.

Theorem 4.3.1. *Let G and H be groups and $\theta : H \longrightarrow Aut(G)$ be a homomorphism. The set $G \times H$ endowed with the multiplication*

$$(g, h)(g_1, h_1) = (g\theta(h)(g_1), hh_1)$$

forms a group called the semidirect product of G and H ($G \times_{theta} H$).

Proof. It is easy to verify that the multiplication is associative. The identity of the semidirect product is (e_G, e_H). Also the inverse of (g, h) is $(\theta(h^{-1})(g^{-1}), h^{-1})$.

□

Example 4.3.2. *Let G and H be arbitrary groups and let $\theta : H \longrightarrow Aut(G)$ be the trivial map (the identity automorphism is assigned to any element of H). Then the semidirect product is just the ordinary direct product.*

Theorem 4.3.3. *Let G be a group. The following conditions are equivalent*

a) There are subgroups $N, H \subseteq G$ with N normal in G such that $NK = G$ and $N \bigcap K = e_G$.

b) $G \cong N \times_\theta K$.

Proof. b) implies a) is straightforwad. The more interesting direction is a) implies b). To see this assume that we have $N \lhd G$ and $K \subseteq G$ such that $NK = G$ and $N \bigcap K = e_G$. We define $\theta : K \longrightarrow \mathrm{Aut}(G)$ by

$$\theta(k) = \phi_k \in \mathrm{Aut}(G)$$

where

$$\phi_k(g) = kgk^{-1}.$$

To show that $G \cong N \times_\theta K$ we consider the map $\psi : G \longrightarrow N \times_\theta K$ given by

$$\psi(g) = (n, k)$$

where $g = nk$ (we are guaranteed that g can be written in this form by the assumption that $G = NK$). We first note that this representation is unique. Indeed if $nk = n_1k_1$, this implies that $n_1^{-1}n = k_1k^{-1}$ and hence this element is the identity since $N \bigcap K = e_G$. So we obtain $n = n_1$ and $k = k_1$.

It is also clear that ψ is onto.

Note that $\ker(\psi)$ is the identity. Finally note that if $g = nk$ and $g_1 = n_1k_1$ that $\psi(gg_1) = \psi(nkn_1k_1) = \psi(nkn_1k^{-1}kk_1) = (nkn_1k^{-1}, kk_1)$. Now note that $(nkn_1k^{-1}, kk_1) = (n\phi_k(n_1), kk_1) = (n\theta(k)(n_1), kk_1) = (n, k)(n_1, k_1) = \psi(g)\psi(g_1)$. □

Here is a nice application.

Example 4.3.4. *Find all groups of order 20. Since* $20 = 2^2 5$*, we can see that there is a unique Sylow 5-group (N) and hence is normal. It is also easy to see that if K is (one of the) Sylow 4 groups, then* $K \bigcap N = e_G$ *and* $NK = G$*. Since* $Aut(N) \cong \mathbb{Z}_4$ *and K is either isomorphic to* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ *or* $\mathbb{Z}_4$ *there are only a few possibilites. There are 5 total (2 abelian and 3 not).*

Example 4.3.5. *Suppose that* $p \equiv 1 mod(q)$*. Show that there are precisely 2 groups of order pq.*

EXERCISES:

1. Classify all groups of order p^3, p^2q and p^2q^2.
2. Show that A_5 is the only nonabelian simple group of order 90.
3. Let G be a group with center $Z(G)$.
   a) Show that if $G/Z(G)$ is cyclic, then G is abelian.
   b) Use this result to show that if $|G| = p^2$ with p a positive prime integer, then G is abelian.
   c) Show that if $|G| = p^3$ then
   $$Z(G) \cong \begin{cases} G & \text{if } G \text{ is abelian} \\ \mathbb{Z}_p & \text{if } G \text{ is not abelian} \end{cases}$$
   d) Show that if $|G| = p^3$ and G is not abelian, then $G/Z(G) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$.

4. Let p, q, r be distinct positive prime integers. Show that there is no simple group of order pqr.

5. Let p and q be distinct positive prime integers.

   a) Show that there is no simple group of order p^n, $n \geq 1$.

   b) Show that there is no simple group of order p^2q.

6. Prove the following statements for groups of specific order.

   a) Show that any group of order 35 is cyclic.

   b) Show that any group of order 99 is abelian and classify them all.

   c) Show that no group of order 24 is simple.

   d) Show that no group of order 72 is simple.

7. Let p and q be distinct positive primes. Show that any group of order pq or p^2q is a semidirect product of its Sylow subgroups (this problem is true in much more generality).

8. Give an example of a group which cannot be decomposed into a semidirect product of two of its proper subgroups.

9. This problem is devoted to showing that A_5 is the only simple group of order less than or equal to 100. We start by assuming that $|G| = 60$ and that G is simple.

   a) Find the possibilities for the number of Sylow 2-subgroups (n) of G and show that we only need concern ourselves with $n = 5$ or $n = 15$.

   b) Show that if $n = 5$ then G is isomorphic to a subgroup of S_5 and conclude that $G \cong A_5$.

   c) Show that if $n = 15$ then there are two Sylow 2-subgroups (say P and Q) that must intersect in a subgroup of G of order 2.

   d) If $H = N_G(P \bigcap Q)$ show that $4|\ |H|$ and conclude that $|H| = 12$. (Hint: any group of order 4 is abelian so $N_G(P \bigcap Q) \supseteq P$.)

   e) Show that since the index of H in G less than or equal to 5, $G \cong A_5$.

   f) Now assume that $|G| \leq 100$ and is simple. Make a list of the possible orders of G (eliminating most of them via earlier results). Eliminate all possibilities except for $|G| = 60$ or 90.

   g) Finally assume that $|G| = 90$ and is simple. Show that G must have 6 Sylow 5−subgroups.

   h) Show that G is necessarily isomorphic to a subgroup of A_6. (Hint: G can be considered a simple subgroup of S_6; consider $G \bigcap A_6$).

   i) Derive a contradiction by showing that A_6 has no subgroup of order 90. (Hint: if A_6 has a subgroup of order 90, look at the orbit of this group under conjugation action...what is the order of its normalizer?)

4.4 Nilpotent and Solvable Groups

Let G be a group. Then $Z(G) := Z_1(G) \lhd G$. Let $Z_2(G)$ be the inverse image of $Z_1(G/Z_1(G))$ via the canonical $G \longrightarrow G/Z_1(G)$. Note that $Z_2(G) \lhd G$ and contains $Z_1(G)$. In general $Z_j(G)$ is the inverse image of $Z(G/Z_{j-1}(G))$ via the canonical projection from G. This gives an ascending central series

$$\{e\} \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots \subseteq Z_n(G) \subseteq \cdots$$

Definition 4.4.1. *We say that G is nilpotent if $Z_n(G) = G$ for some n.*

Of course any abelian group is nilpotent.

Theorem 4.4.2. *Every finite p group is nilpotent.*

Proof. Of course every subgroup and quotient group of a p group is again a p group. Suppose that $Z_n(G) \neq G$. Since p groups have nontrivial centers, it follows that $Z_{n+1}(G)$ strictly contains $Z_n(G)$. As G is finite, this process must terminate. □

Theorem 4.4.3. *The direct product of a finite number of nilpotent groups is nilpotent.*

Proof. It suffices to show this for the case $H \times K$ where H and K are nilpotent. Assume inductively that

$$Z_n(G) = Z_n(H) \times Z_n(K).$$

The canonical epimorphism $\phi : G \longrightarrow G/Z_n(G)$ is the composition

$$G = H \times K \xrightarrow{\quad\pi\quad} H/Z_n(H) \times K/Z_n(K) \xrightarrow{\psi} H \times K/(Z_n(H) \times Z_n(K)) =$$

$$= H \times K/Z_n(H \times K) = G/Z_n(G)$$

where $\pi = \pi_H \times \pi_K$ and we will say that ϕ is the total composition.

$Z_{n+1}(G) = \phi^{-1}(Z(G/Z_n(G))) = \pi^{-1}\psi^{-1}(Z(G/Z_n(G))) = \pi^{-1}(Z(H/Z_n(H) \times K/Z_n(K))) = \pi^{-1}(Z(H/Z_n(H) \times Z(K/Z_n(K))) = \pi_H^{-1}(Z(H/Z_n(H))) \times \pi_K^{-1}(Z(K/Z_n(K))) = Z_{n+1}(H) \times Z_{n+1}(K)$.

This establishes our fact, the rest follows.

□

Lemma 4.4.4. *If $H \subsetneq G$ where G is nilpotent, then $H \subsetneq N_G(H)$.*

Proof. Let $Z_0(G) = e$ and n the largest integer such that $Z_n(G) \subseteq H$. Let $a \in Z_{n+1}(G) \setminus H$. For all $h \in H, Z_n ah = Z_n ha$ in $G/Z_n(G)$ since $Z_n(G)$ is in the center of $Z_{n+1}(G)$ by definition. Therefore, $ah = h'ha$ where $h' \in Z_n(G) \subseteq H$. Hence $aha^{-1} = h'h \in H$ and $a \in N_G(H)$, but $a \notin H$ and we have a contradiction. □

The follwoing theorem characterizes finite nilpotent groups.

Theorem 4.4.5. *A finite group is nilpotent if and only if it is the direct product of its Sylow subgroups.*

Proof. $\Longleftarrow$ is implied by the previous. So we will prove the other direction. Assume that G is nilpotent and that P is a Sylow $p-$subgroup of G. If $P \neq G$ then $P \neq N_G(P)$ It turns out that $N_G(P)$ is its own normalizer (easy exercise). Hence by the previous, $N_G(P) = G$ and P is the unique Sylow $p-$subgroup. Now it is easy to see that

$$G \cong \prod_{i=1}^{k} P_i$$

with each P_i being the Sylow p_i-subgroup (since the intersection of the distinct Sylow $p-$subgroups is trivial and the fact that $G = P_1 P_2 \cdots P_k$ is generated by all of them). □

Corollary 4.4.6. *If G is a finite nilpotent group and m divides the order of G then G has a subgroup of order m.*

Proof. This is a direct consequence of the previous and the Sylow theorems. □

We will now look at a special sequence of groups called the derived series. But first we recall that if $N \lhd G$ then G/N is abelian if and only if $G' \subseteq N$ (with G' the commutator subgroup of G).

We consider the series of derived subgroups of G:

$$G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq G^{(3)} \supseteq \cdots$$

where $G^{(1)} = G'$ and $G^{(n)} = (G^{(n-1)})'$.

Definition 4.4.7. *We say that G is solvable if $G^{(n)} = e$ for some n.*

Theorem 4.4.8. *Every nilpotent group is solvable.*

Proof. Note that $Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$ is abelian, so $Z_n(G)' \subseteq Z_{n-1}(G)$ for all $n \geq 1$ and $Z_1(G)' = Z(G)' = e$. For some n, $Z_n(G) = G$, therefore $Z(G/Z_{n-1}(G)) = Z_n(G)/Z_{n-1}(G) = G/Z_{n-1}(G)$ is abelian. So $G^{(1)} = G' \subseteq Z_{n-1}(G)$, $G^{(2)} = (G^{(1)})' \subseteq Z_{n-1}(G)' \subseteq Z_{n-2}(G)$, $G^{(3)} \subseteq Z_{n-3}(G), \cdots, G^{(n-1)} \subseteq Z_1(G)$ and $G^{(n)} \subseteq e$. Hence G is solvable. □

Theorem 4.4.9. *a) Every subgroup and homomorphic image of a solvable group is solvable.*

b) If $N \lhd G$ is such that both N and G/N are solvable, then G is solvable.

Proof. 1) Suppose that $f : G \longrightarrow H$ is an onto homomorphism. Note that $f(G^{(i)}) = H^{(i)}$ for all i. If G is solvable then $f(G^{(n)}) = f(e) = e = H^{(n)}$ and hence H is solvable.

If $H \subseteq G$ then $H^{(i)} \subseteq G^{(i)}$ therefore if $G^{(n)} = e$ then $H^{(n)} = e$.

2) Now consider $f : G \longrightarrow G/N$ (the natural projection map). As G/N is solvable then $f(G^{(n)}) = (G/N)^{(n)} = e$. Therefore $G^{(n)} \subseteq ker(f) = N$. As $G^{(n)}$ is a subgroup of N (and N is solvable) then $G^{(n)}$ (and hence G) is solvable. □

It should be noted that (for example) no non-abelian simple group is solvable. It is also of historical note the the famed Feit-Thompson Theorem (which says that all groups of odd order are solvable) occupies an entire issue of the Pacific Journal of Mathematics ("Solvability of groups of odd order" Pacific J. Math. 13, 1963, pp.775–1029).

EXERCISES:

1. Show that A_5 is the only group of order less than or equal to 100 that is not solvable.

2. Let D_n be the dihedral group on the $n-$gon.

   a) Show that $x^2 \in D_n'$ for all $x \in D_n$.

   b) If n is odd, show that $D_n' = \mathbb{Z}_n$.

   c) If $n = 2m$ is even show that $D_n' = \mathbb{Z}_m$.

   d) D_n is nilpotent if and only if $n = 2^k$.

3. Show that S_3 and S_4 are solvable, but not nilpotent.

4. Construct all semidirect products of $\mathbb{Z}_5$ and $\mathbb{Z}_4$ (realize one as a subgroup of S_5 and another as a subgroup of S_9...there are more than 2, though).

5. Using the notation $[a, b] = aba^{-1}b^{-1}$, show that

$$[ab, c] = a[b, c]a^{-1}[a, c].$$

4.5 Normal Series

Definition 4.5.1. *A chain of distinct subgroups*

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n$$

such that $G_{i+1} \lhd G_i$ is called a subnormal series. The groups G_i/G_{i+1} are called the factors and n is called the length. The series is called normal if $G_i \lhd G$ for all i

Example 4.5.2.

$$G \supsetneq G^{(1)} \supsetneq G^{(2)} \supsetneq \cdots \supsetneq G^{(n)}$$

is a normal series and so is

$$Z_1(G) \subsetneq Z_2(G) \subsetneq \cdots \subsetneq Z_n(G) = G$$

if G is nilpotent.

Definition 4.5.3. *A one term refinement of*

$$G_0 \supsetneq G_1 \supsetneq \cdots \subsetneq G_n$$

is a series of the form

$$G_0 \supsetneq G_1 \supsetneq \cdots \subsetneq G_i \supsetneq N \supsetneq G_{i+1} \supsetneq \cdots \supsetneq G_n$$

with $N \lhd G_i$ and $G_{i+1} \lhd N$. A refinement of a series is a sequence of one term refinements.

Definition 4.5.4. *A subnormal series*

$$G_0 \supsetneq G_1 \supsetneq \cdots \subsetneq G_n = e$$

is called a composition series if each factor G_i/G_{i+1} is simple. It is called solvable if each factor is abelian.

Theorem 4.5.5. *Let G be a group.*

a) Every finite group has a composition series.

b) Every refinement of a solvable series is a solvable series.

c) A subnormal series is a composition series if and only if it has no proper refinements.

Proof. Exercise. □

Now we see why "solvable" series have this name.

Theorem 4.5.6. *G is a solvable group if and only if it possesses a solvable series.*

Proof. ($\Longrightarrow$) It is easy to see that the derived series is a solvable series.
($\Longleftarrow$) Suppose that G has a solvable series:

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = e.$$

Note that $G_1 \supseteq G^{(1)}$ since G/G_1 is abelian. This gives that $G_2 \supseteq G_1^{(1)} = G^{(2)}$. Continuing this process we obtain $e = G_n \supseteq G^{(n)}$ and this establishes the theorem. □

We leave the last theorem of the section as an exercise. This theorem is the celebrated Jordan-Holder theorem and is one of the major motivations for the classification of finite simple groups.

Theorem 4.5.7. *Any two composition series of G are equivalent. Hence if G possesses a composition series, then it determines a unique list of simple groups.*

Example 4.5.8. *We look first at an easy abelian example. Consider the two composition series for* $\mathbb{Z}_6$*:*

$$\mathbb{Z}_6 \supseteq \mathbb{Z}_3 \supseteq e$$

and

$$\mathbb{Z}_6 \supseteq \mathbb{Z}_2 \supseteq e.$$

Although these composition series may look different, they possess the same length that the same list of simple groups ($\mathbb{Z}_2$ *and* $\mathbb{Z}_3$ *in different orders).*

Chapter 5

Rings

5.1 Preliminaries

Definition 5.1.1. *A ring is a nonempty set, R, together with two binary operations $(+, \cdot)$ such that*

a) $(R, +)$ *is an abelian group.*

b) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c \in R$.

c) $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$ *for all* $a, b, c \in R$.

We remark here that if $ab = ba$ for all $a, b \in R$ then we say that R is commutative. Additionally, if there is an element (denoted $1 = 1_R$) such that $1(a) = a(1) = a$ for all $a \in R$ then R is said to have (multiplicative) identity.

Theorem 5.1.2. *Let R be a ring.*

a) $0(a) = a(0) = 0$ *for all* $a \in R$.

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

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

d) $(na)b = a(nb) = (ab)n$ *for all* $a, b \in R$ *and* $n \in \mathbb{Z}$.

e) $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$.

Proof. Exercise. □

Definition 5.1.3. *An element $a \in R$ is said to be a left (right) zero divisor if there is a nonzero $b \in R$ such that $ab = 0$ ($ba = 0$). An element which is both a left and right zero divisor is called a zero divisor. Additionally, if $a^n = 0$ for some $n \geq 1$ we say that a is nilpotent.*

We remark that the element 0 (in a nonzero ring) is always a zero divisor (we will sometimes refer to 0 as the trivial zero divisor).

Definition 5.1.4. *Let R be a ring with identity. An element $a \in R$ is said to be left (right) invertible if there is an element $b \in R$ such that $ba = 1$ ($ab = 1$). The element b, if it exists, is called a left (right) inverse of a. If a is both left and right invertible, it is called invertible or a unit.*

Proposition 5.1.5. *If a is a unit in R (a ring with identity) and b is a left inverse of a and c is right inverse of a, then $b = c$.*

Proof.

$$c = (1)c = (ba)c = b(ac) = b(1) = b.$$

□

The previous result shows that the units of R form a group under multiplication (often denoted by $U(R)$).

Definition 5.1.6. *A (nonzero) commutative ring with identity is called an (integral) domain if it possesses no notrivial zero divisors. A ring D with identity is called a division ring if $U(D) = D \setminus \{0\}$. A commutative division ring is called a field.*

Proposition 5.1.7. *If R is a division ring, then R has no nontrivial zero divisors. In particular, any field is an integral domain.*

Proof. Suppose that R is a division ring and that $ab = 0$ with $a \neq 0$. Since a is nonzero, there is an element $x \in R$ such that $xa = 1$. This implies that $x(ab) = 0 = (xa)b = (1)b = b$; so $b = 0$ and we are done. □

Example 5.1.8. *Here is a fundamental construction that is "full of" zero divisors. Let R_i, $i \in \Gamma$ be a family of rings, we construct the direct sum $\oplus_{i\in\Gamma} R_i$ and direct product $\prod_{i\in\Gamma} R_i$ of the families (considering each R_i as a group at first). Multiplication is then defined "coordinate-wise" on the sequences. Check that if $|\Gamma| > 1$ (and each R_i is nonzero) then you are guaranteed to have nontrivial zero divisors. Also check that $\prod_{i\in\Gamma} R_i$ has an identity if and only if each R_i has an identity and that $\oplus_{i\in\Gamma} R_i$ has an identity if and only if each R_i has an identity and $|\Gamma| < \infty$.*

Theorem 5.1.9. *Any finite integral domain is a field.*

We remark that, in fact, more is true here. One can remove the hypothesis "with identity" (i.e. any finite commutative ring with no nontrivial zero divisors is a field). It is also true that any finite division ring is a field and in this sense the result can be generalized further.

Proof. Since R is finite, consider all powers of a nonzero element $a \in R$. There must be positive integers $n > m$ such that $a^n = a^m$. from this we deduce that $a^{n-m} = 1$ (as R has no nontrivial zero divisors). Hence the inverse of a is a^{n-m-1}. □

One of the consequences of this observation is that (in contrast to group theory) most of the "interesting" rings are infinite.

Theorem 5.1.10. *Let R be a ring with identity, n a positive integer, and $a, b, a_i \in R$.*

a) If $ab = ba$ then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

b) If $a_i a_j = a_j a_i$ for all i, j then

$$(a_1 + a_2 + \cdots + a_s)^n = \sum_{k_1+k_2+\cdots+k_s=n} \frac{n!}{k_1!k_2!\cdots k_s!} a_1^{k_1} a_2^{k_2} \cdots a_s^{k_s}.$$

Proof. Exercise (follows easily by induction). □

Definition 5.1.11. *Let R and S be rings. A function $f : R \longrightarrow S$ is said to be a ring homomorphism if*

a) $f(a+b) = f(a) + f(b)$ for all $a, b \in R$.

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

We remark that the usual descriptives apply to ring homomorphisms (e.g. isomorphism, epimorphism, etc.).

Example 5.1.12. *The function "reduction modulo n" is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_\kappa$. Also consider homomorphisms from R to $R \oplus R$ and from $R[x]$ to R via $f(x) \mapsto f(a)$ for some fixed $a \in R$.*

Definition 5.1.13. *Let R be a ring. If there is a smallest integer $n > 0$ such that $na = 0$ for all $a \in R$, we say that R is of characteristic n. If no such n exists, then R is of characteristic 0.*

Example 5.1.14. *The characteristic of $\mathbb{Z}$ is 0. Note that the characteristic of $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \cdots \oplus \mathbb{Z}_{2^n}$ is 2^n, but the characteristic of $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \cdots \oplus \mathbb{Z}_{2^n} \cdots$ is 0.*

Theorem 5.1.15. *Let R be a ring with identity of characteristic $n > 0$.*

a) If $\phi : \mathbb{Z} \longrightarrow R$ is the map given by $\phi(k) = (k)1_R$, then ϕ is a homomorphism with kernal $n\mathbb{Z}$.

b) n is the smallest integer such that $(n)1_R = 0$.

c) If R has no nontrivial zero divisors, then n is prime.

Proof. Number 1 is easy to verify. For 2, it is clear that $n1_R = 0$. Assume that $m1_R = 0$ with $m < n$ and let $a \in R$ be arbitrary. Note that $ma = m1_R a = 0$ and this means that the characteristic of R is less than n which is a contradiction.

Finally we note that if n is not prime then n can be factored nontrivially into two integers ($n = mk$) with both m and k greater than 1. Note that $m1_R \neq 0$ and $k1_R \neq 0$, but $(m1_R)(k1_R) = (n1_R) = 0$ and this is a contradiction. □

Is the converse to part c) true? How much is true if "with identity" is removed? Generally speaking rings without identity can be quite badly behaved. But here is a saving grace. Any ring can be thought of as a subring of a ring with identity.

Theorem 5.1.16. *Every ring R can be embedded in a ring S with identity. What is more, the characteristic of S can be chosen to coincide with the characteristic of R or it can be chosen to be of characteristic* 0.

Proof. Consider the construction

$$S = R \oplus \mathbb{Z}$$

as a group with multiplication given by

$$(r, n)(t, m) = (rt + rm + tn, nm).$$

This gives the appropriate of S of characteristic 0. For one of coinciding characteristic, replace $\mathbb{Z}$ with $\mathbb{Z}_n$ where n is the characteristic of R. □

EXERCISES:

1. Establish the claims made for the direct product and direct sum of a family of rings.

2. We say that R is a Boolean ring if $x^2 = x$ for all $x \in R$. Show that any Boolean ring is of characteristic 2 and commutative. Must it have an identity?

3. Let R be a nonzero ring such that for all nonzero $a \in R$, there is a unique $b \in R$ such that $aba = a$. Establish the following results.

   a) R has no nontrivial zero divisors.

   b) $bab = b$ (with the notation as above).

   c) R has an identity.

   d) R is a division ring.

4. Suppose that R is commutative with identity and the characteristic of R is a nonzero prime number p. Show that for all $a, b \in R$, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ and use this to show that for all n, the function $\phi_n : R \longrightarrow R$ given by $\phi_n(x) = x^{p^n}$ is a ring homomorphism.

5. We recall that $a \in R$ is nilpotent if $a^n = 0$ for some $n \geq 1$. Show that if R is commutative, the the set of nilpotent elements forms an ideal of R. Give a counterexample for the noncommutative case.

6. Give an example of an injective ring homomorphism $f : R \longrightarrow S$ such that $f(1_R)$ is not a unit of S.

5.2 Ideals

Definition 5.2.1. *Let R be a ring. A subset $T \subseteq R$ that is itself a ring is called a subring of R. A subring $I \subseteq R$ is called a left (right) ideal if for all $x \in I$ and $r \in R$, $rx \in I$ ($xr \in I$). I is called an ideal if it is both a left and right ideal.*

Note that sometimes if R has an identity, then the terminology "subring" also demands that 1_R is an element of T. We will make clear which we are using, but the default will be the more general definition above.

Example 5.2.2. *(0) and R are both subrings and ideals. $Z(R) = \{z \in R | zr = rz \ \forall \ r \in R\}$ is a subring of R, but not necessarily an ideal.*

Example 5.2.3. *If $f : R \longrightarrow S$ is a ring homomorphism, then $ker(f)$ is an ideal of R and $im(f)$ is a subring of S.*

Example 5.2.4. *An exhaustive list of the ideals in $\mathbb{Z}$ is the set of ideals $n\mathbb{Z}$, $n \in \mathbb{Z}$.*

Example 5.2.5. *If R is a ring with identity and $I \subseteq R$ is an (left) ideal then $I = R$ if and only if $1_R \in I$.*

Theorem 5.2.6. *A nonempty subset $I \subseteq R$ is a left ideal if and only if for all $a, b \in I$ and $r \in R$,*

a) $a - b \in I$; and

b) $ra \in I$.

Corollary 5.2.7. *Let $\{I_j\}$, $j \in \Gamma$ be a collection of left ideals of R. Then $\bigcap_{j \in \Gamma} I_j$ is a left ideal of R.*

Definition 5.2.8. *Let X be a subset of R and $\{I_j\}$, $j \in \Gamma$ the family of all left ideals of R containing the set X, then the left ideal generated by X is $\langle X \rangle = \bigcap_{j \in \Gamma} I_j := I$.*

Notes: *If X is a finite set then we say that I is finitely generated. If $|X| = 1$, then we say that I is principal. A principal ideal ring (PIR) is a ring in which every ideal is principal. A principal ideal domain (PID) is a PIR that is an integral domain (e.g. $\mathbb{Z}$).*

Theorem 5.2.9. *Let R be a ring and X a subset of R.*

a) The principal ideal (a) consists of elements of R of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i$ ($r_i, s_i, r, s \in R$ and $n \in \mathbb{Z}$).

b) If R has an identity the above can be shortened to $\sum_{i=1}^{m} r_i a s_i$.

c) If $a \in Z(R)$ then (a) consists of elements of the form $ra + na$ with $r \in R$ and $n \in \mathbb{Z}$.

d) $Ra = \{ra + na | r \in R, n \in \mathbb{Z}|$ *is a left ideal of* R *(which might not contain* a*). If* $1_R \in R$ *then* $a \in Ra$*.*

e) If $1_R \in R$ *and* $a \in Z(R)$ *then* $Ra = aR = (a)$*.*

f) If $1_R \in R$ *and* $X \subseteq Z(R)$ *then* $\langle X \rangle$ *consists of all finite sums of the form*

$$r_1x_1 + r_2x_2 + \cdots + r_nx_n$$

with $r_i \in R$ *and* $x_i \in X$*.*

Definition 5.2.10. *Let* I *and* J *be left ideals of* R*. We define*

$$I + J = \{x + y | x \in I, y \in J\}$$

and

$$IJ = \{\sum_{i=1}^{m} x_i y_i | x_i \in I, y_i \in J\}.$$

Theorem 5.2.11. *Let* $A_1, A_2, \cdots, A_n, A, B, C$ *be left ideals of* R*.*

a) $A_1 + A_2 + \cdots + A_n$ *and* $A_1A_2 \cdots A_n$ *are left ideals of* R*.*

b) $A + (B + C) = (A + B) + C$*.*

c) $(AB)C = A(BC)$*.*

d) $B \sum A_i = \sum BA_i$ *and* $(\sum A_i)C = \sum A_iC$*.*

Proof. Exercise. □

Theorem 5.2.12. *Let* R *be a ring and* $I \subseteq R$ *an ideal. Then the quotient group* R/I *is a ring with multiplication given by*

$$(a + I)(b + I) = ab + I$$

for all $a, b \in R$*. What is more, if* R *is commutative, so is* R/I *and if* R *has an identity, then so does* R/I*.*

Proof. We leave most details to the reader, but we will show that multiplication is well-defined. Suppose that $a + I = x + I$ and $b + I = y + I$. This means that $a - x, b - y \in I$. We write $a = x + i$ and $b = y + j$ with $i, j \in I$. Note that $ab = xy + xj + iy + ij$ and since $xj + iy + ij \in I$, $ab + I = xy + I$ and the multiplication is well-defined. □

Theorem 5.2.13. *If* $f : R \longrightarrow S$ *is a homomorphism, then* $ker(f)$ *is an ideal of* R*. If* I *is an ideal in* R*, then* $\pi_I : R \longrightarrow R/I$ *is an epimorphism of rings with kernal* I*.*

Proof. We have already established the first statement. For the second we know that π_I is a ring epimorphism (since it is a ring homomorphism and is onto). The kernal being I can be obtained by observing that it is the kernal of the group homomorphism. □

Theorem 5.2.14. *If $f : R \longrightarrow S$ is a homomorphism of rings and $I \subseteq R$ is an ideal in the kernal of f then there is a unique ring homomorphism $\overline{f} : R/I \longrightarrow S$ such that $\overline{f}(a+I) = f(a)$ for all $a \in R$. $im(\overline{f}) = im(f)$ and $ker(\overline{f}) = ker(f)/I$. If particular $\overline{f}$ is an isomorphism if and only if f is onto and $I = ker(f)$.*

Proof. The proof of this is almost exactly the same as the analogous theorem in group theory. □

We now record the first isomorphism theorem.

Corollary 5.2.15. *If $f : R \longrightarrow S$ is a homomorphism, then f induces an isomorphism $R/ker(f) \cong im(f)$.*

Corollary 5.2.16. *If $f : R \longrightarrow S$ is a homomorphism and $I \subseteq R$ and $J \subseteq S$ are ideals such that $f(I) \subseteq J$, then f induces a homomorphism*

$$\overline{f} : R/I \longrightarrow S/J$$

with $\overline{f}(a+I) = f(a) + J$. Additionally $\overline{f}$ is an isomorphism if and only if $im(f) + J = S$ and $f^{-1}(J) \subseteq I$. In particular, if f is an epimorphism such that $f(I) = J$ and $ker(f) \subseteq I$ then $\overline{f}$ is an isomorphism.

Here are the second and third isomorphism theorems.

Theorem 5.2.17. *Let I, J be ideals in R.*

a) There is an isomorphism of rings $I/(I \bigcap J) \cong (I+J)/J$.

b) If $I \subseteq J$ then J/I is an ideal of R/I and there is an isomorphism of rings $(R/I)/(J/I) \cong R/J$.

Proof. Again the proof is very similar to the group-theoretic results. □

Theorem 5.2.18. *If $I \subseteq R$ is an ideal then there is a 1-1 correspondence between ideals of R containing I and ideals of R/I given by $J \mapsto J/I$. Hence every ideal of R/I is of the form J/I with J an ideal of R containing I.*

5.3 Types of Ideals

There are different flavors of ideals out there and here we will list some of the more important ones.

Definition 5.3.1. *We say that $\mathfrak{M} \subsetneq R$ is a maximal ideal if there is no other ideal properly between $\mathfrak{M}$ and R.*

Definition 5.3.2. *We say that $\mathfrak{P}$ is prime if $\mathfrak{P} \supseteq AB$ implies $\mathfrak{P} \supseteq A$ or $\mathfrak{P} \supseteq B$.*

Remark 5.3.3. *The collection of all prime ideals of R is called the spectrum of R (Spec(R)). The collection of maximal ideals is called the maximal spectrum of R (MaxSpec(R)).*

beginthm If $\mathfrak{P}$ is an ideal with the property that $ab \in \mathfrak{P}$ implies that $a \in \mathfrak{P}$ or $b \in \mathfrak{P}$, then $\mathfrak{P}$ is prime. Additionally, if R is commutative, then the converse holds.

Proof. Suppose that $AB \subseteq \mathfrak{P}$ and that $A \subsetneq \mathfrak{P}$. Select an element $a \in A \setminus \mathfrak{P}$. Note that for all $b \in B$, $ab \in AB \subseteq \mathfrak{P}$. Since $\mathfrak{P}$ has the property listed and $a \notin \mathfrak{P}$, we have that $b \in \mathfrak{P}$ for all $b \in B$. Hence $B \subseteq \mathfrak{P}$ and $\mathfrak{P}$ is prime.

For the other statement, we will assume that R is commutative and that $\mathfrak{P}$ is prime. Assume that $ab \in \mathfrak{P}$. Therefore, we have that $(ab) \subseteq \mathfrak{P}$ and hence

$$(ab) = (a)(b) \subseteq \mathfrak{P}.$$

Since $\mathfrak{P}$ is prime, $\mathfrak{P} \supseteq (a)$ (without loss of generality). Hence $a \in \mathfrak{P}$. (Where did we use the assumption "commutative"...I assure you that we did). □

Example 5.3.4. *Look at primes in $\mathbb{Q}[x, y]$ and $\mathbb{Z}$. All primes are maximal in a finite ring.*

Here are some more types of ideals that are mostly used in the commutative situation.

Lemma 5.3.5. *Let R be commutative and $I \subsetneq R$ an ideal. The set $rad(I) = \sqrt{I} = \{x \in R | x^n \in I \text{ for some } n \in \mathbb{N}\}$ is an ideal of R (called the radical of I).*

Definition 5.3.6. *Let R be commutative and $I \subsetneq R$ an ideal. We say that I is radical if $I = \sqrt{I}$. We say that R is primary if $ab \in I$ with $a \notin I$ implies that $b^n \in I$ for some $n \in \mathbb{N}$.*

The following result (via its corollaries) shows the value of looking at quotient structures.

Theorem 5.3.7. *Let R be a commutative ring with identity and let $I \subsetneq R$ be an ideal.*

a) I is maximal if and only if R/I is a field.

b) I is prime if and only if R/I is an integral domain.

c) I is radical if and only if R/I is a reduced (that is, R/I has no nonzero nilpotent elements).

d) I is primary if and only if all zero divisors of R/I are nilpotent.

Proof. For a), first assume that I is maximal and consider a nonzero coset $x + I \in R/I$. Since $x + I$ is a nonzero coset, this means that $x \notin I$ and hence $(x, I) = R$. So there is an element $r \in R$ and an element $z \in I$ such that $rx + z = 1$ and hence $(x + I)(r + I) = 1 + I$ and R/I is a field.

On the other hand, assume that R/I is a field. Let J be an ideal properly containing I and select an element $x \in J \setminus I$. Since R/I is a field, we have that there is an inverse (say $(y+I)$) to the nonzero coset $x+I$, i.e. $(x+I)(y+I) = 1+I$. This means that there is an element $z \in I$ such that $xy + z = 1$. This means that the ideal $(x, I) = R$ and since $J \supseteq (x, I)$, we have that $J = R$ and hence I is maximal.

For d) first assume that I is primary and that $x + I$ is a zero divisor of R/I. So there is a nonzero coset $y + I \in R/I$ such that $(x + I)(y + I) = 0 + I$, i.e., $xy \in I$ with $y \notin I$. Since I is primary, we must have that $x^n \in I$ and hence the coset $(x + I)$ is nilpotent.

Now assume that every zero divisor of R/I is nilpotent and let $xy \in I$ with $x \notin I$. This means that $y+I$ is a zero divisor of R/I and hence $y+I$ is nilpotent. Therefore $y^n \in I$ and I is primary.

b) and c) are simliar and left as exercises.

□

We now produce a corollary or two to show the usefulness of quotient rings as well as to highlight the interplay between these types of ideals.

Corollary 5.3.8. *Let R be commutative with identity and $I \subseteq R$ a proper ideal. Then we have the following implications: I is maximal $\implies$ I is prime and I is prime $\iff$ I is both primary and radical.*

Proof. For the first statement, if I is maximal this implies that R/I is a field and hence an integral domain. So I is prime.

For the second statement note that if I is prime then R/I is a domain. Since any domain is reduced, I must be radical. Additionally since the only zero divisor of a domain is 0 (which is nilpotent) I must be primary.

For the other implication, assume that I is radical and primary. In this case, R/I must be reduced (no nonzero nilpotents) and every zero divisor of R/I must be milpotent (0). So R/I is a domain and I is prime. □

Corollary 5.3.9. *The radical of a primary ideal is prime.*

Proof. We will show this directly. Assume that $J = \sqrt{I}$ where I is primary. Suppose that $ab \in J$. Since J is the radical of I, there is an n such that $a^n b^n \in I$. Now note that if $a^n \in I$, this implies that $a \in \sqrt{I} = J$ and we are done. If $a^n \notin I$, then since I is primary, there is a $k \in \mathbb{N}$ such that $b^{nk} \in I$ and hence $b \in \sqrt{I} = J$. In either case, $a \in J$ or $b \in J$ and J is prime. □

We are now going to prove one of the fundamental results in ring theory (the existence of maximal ideals in rings with identity). But first, we must make (an axiom of) choice to believe. We produce a result called Zorn's Lemma (which is intimately tied to the axiom of choice).

ZORN'S LEMMA: Let S be a partially ordered set with the property that every chain (linearly ordered subset) in S has an upper bound in the set. Then S has a (at least one) maximal element.

As I said, do not try to prove this.

Theorem 5.3.10. *Let R be a ring with identity. Then R has a maximal (left) ideal. What is more, any ideal I is contained in a maximal ideal $\mathfrak{M}$.*

Proof. Let $I \subsetneq R$ be our (left) ideal (if you merely want existence of a maximal ideal you can take $I = (0)$). Let $\Gamma = \{J | J \text{ is a proper (left) ideal of } R \text{ containing } I\}$ with the partial ordering being set-theoretic containment. Note that *Gamma* is nonempty as $I \in \Gamma$.

To apply Zorn's Lemma, we need to verify that every chain in Γ has an upper bound in Γ. Let $C = \{I_j\}$ be a chain (that is, a linearly ordered subset of Γ). We claim that $U := \bigcup I_j$ is an upper bound for C (more precisely, the fact that it is an upper bound is clear...we merely have to show that $U \in \Gamma$).

To this end, we first claim that U is an (left) ideal of R. Indeed, if $x, y \in U$ then $x \in I_\alpha$ and $y \in I_\beta$. Since I_α and I_β are elements of C, then we will assume that $I_\alpha \subseteq I_\beta$ without loss of generality. Hence $x - y \in I_\beta \subseteq U$. Showing that $rx \in U$ is similar.

To see that U is proper, note that if it is not, then $1 \in U$ and hence $1 \in I_\alpha$ for some α. Hence I_α is not proper which is a contradiction.

Since U is an upper bound in Γ, Zorn's Lemma applies and hence Γ has a maximal element $\mathfrak{M}$. This element $\mathfrak{M}$ is a maximal ideal of R containing I and we are done. □

Example 5.3.11. *Can you list the maximal ideals of the ring $\prod_{i=1}^{\infty} \mathbb{Z}_2$?*

Here are some generalizations of earlier results (without proof).

Theorem 5.3.12. *Let R be a commutative ring such that $R^2 = R$ (in particular, this holds if R has identity), then any maximal ideal of R is prime.*

Theorem 5.3.13. *Let $\mathfrak{M}$ be a proper ideal in a ring R with identity.*

a) If $\mathfrak{M}$ is maximal and R is commutative, then $R/\mathfrak{M}$ is a field.

b) If $R/\mathfrak{M}$ is a division ring, then $\mathfrak{M}$ is maximal.

It should be noted in tandem with the above theorem that, in particular, if R is commutative with identity then $\mathfrak{M}$ is maximal if and only if $R/\mathfrak{M}$ is a field and R is a field if and only if R has no proper ideals if and only if (0) is maximal if and only if any nonzero homomorphism $f : R \longrightarrow S$ is injective.

Theorem 5.3.14. *Let $\{R_i | i \in \Lambda\}$ be a nonempty family of rings and $\prod_{i\in\Lambda} R_i$ the direct product of the underlying groups.*

a) $\prod_{i\in\Lambda} R_i$ is a ring with pointwise product.

b) If R_i has identity or is commutative for all i, then so is $\prod_{i\in\Lambda} R_i$.

c) For all k, the projection $\pi_k : \prod_{i\in\Lambda} R_i \longrightarrow$ *is a ring epimorphism.*

d) For all k the inclusion $\iota_k : R_k \longrightarrow \prod_{i\in\Lambda} R_i$ *is a monomorphism of rings.*

Theorem 5.3.15. *Let* $\{R_i\}$ *be a family of rings, S a ring, and* $\{\phi_i : S \longrightarrow R_i\}$ *a family of homomorphisms. Then there is a unique* $\phi : S \longrightarrow \prod R_i$ *such that* $\pi_i\phi = \phi_i$ *for all i. The direct product is determined up to isomorphism by this property.*

Proof. The proof is very similar to the analogous result for groups. The needed map is $\phi(s) = \{\phi_i(s)\}$. Verify that this works. □

Theorem 5.3.16. *Let* $A_1, A_2, \cdots, A_n$ *be ideals in R such that*

a) $A_1 + A_2 + \cdots + A_n = R$ *and*

b) $A_k \bigcap (A_1 + A_2 + \cdots + A_{k-1} + A_{k+1} + \cdots + A_n) = 0.$

Then $R \cong A_1 \times A_2 \times \cdots \times A_n$.

Proof. Consider the map $\phi : A_1 \times A_2 \times \cdots \times A_n \longrightarrow R$ given by $\phi(a_1, a_2, \cdots, a_n) = a_1 + a_2 + \cdots + a_n$. It is clear that ϕ is an additive group homomorphism. Additionally by the first assumption, ϕ is onto and to see that ϕ is one to one, note that if $\phi(a_1, \cdots, a_n) = a_1 + \cdots + a_n = 0$ then we have that $a_i = -(a_1 + a_2 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_n) \in A_i \bigcap (A_1 + A_2 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_n) = 0$. So an arbitrary $a_i = 0$ and ϕ is one to one.

The only remaining part to show is that ϕ is a homomorphism with respect to the multiplicative structure. But note that $\phi((a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)) = \phi((a_1b_1, \cdots, a_nb_n)) = a_1b_1 + \cdots + a_nb_n$. Also note that $(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) = \sum_{i=1}^n \sum_{j=1}^n a_ib_j$. But if $i \neq j$ then $a_ib_j \in A_i \bigcap A_j = 0$ and hence this sum is precisely $a_1b_1 + \cdots + a_nb_n$ and this shows that ϕ is a homomorphism. □

The next result is the famous Chinese Remainder Theorem. We state this in slightly more generality than is usually seen in practice (our assumption will be that if A is an ideal of R then $R^2 + A = R$ which always holds if R has an identity or, more generally is an idempotent ring).

Theorem 5.3.17. *Let* $A_1, A_2, \cdots, A_n$ *be ideals in a ring R such that* $R^2 + A_i = R$ *for all i and* $A_i + A_j = R$ *if* $i \neq j$. *If* $b_1, b_2, \cdots, b_n \in R$ *then there is a* $b \in R$ *such that*

$$b \equiv b_i mod(A_i)$$

for all i. What is more, b is uniquely determined up to congruence modulo $A_1 \bigcap A_2 \bigcap \cdots \bigcap A_n$.

Example 5.3.18. *Find a solution to your favorite set of congruence equations.*

Corollary 5.3.19. *If* $A_1, A_2, \cdots, A_n$ *are ideals in R then there is a monomorphism of rings*

$$\theta : R/(A_1 \bigcap A_2 \bigcap \cdots \bigcap A_n) \longrightarrow R/A_1 \times R/A_2 \times \cdots \times R/A_n$$

and if $R^2 + A_i = R$ *for all i and* $A_i + A_j = R$ *if* $i \neq j$ *then* θ *is an isomorphism.*

5.4 Factorization in Commutative Rings

Since a large part of the understanding of the multiplicative structure of a commutative ring, R, concerns factorization, factorization is, in a sense, what separates (commutative) ring theory from the theory of abelian groups. In this section we will give a brief overview of basic factorization. In this section all rings are commutative.

Definition 5.4.1. *A nonzero element $a \in R$ is said to divide b ($a|b$) if there exists an $x \in R$ such that $ax = b$. If $a|b$ and $b|a$ then a and b are associates.*

Theorem 5.4.2. *Let R be commutative with identity and $a, b, u \in R$.*

a) $a|b$ if and only if $(b) \subseteq (a)$.

b) a and b are associates if and only if $(a) = (b)$.

c) $u \in U(R)$ if and only if $u|r$ for all $r \in R$ if and only if $(u) = R$.

d) The relation "$a \sim b$ if and only a and b are associates" is an equivalence realtion on R.

e) If $a = bu$ with $u \in U(R)$ then a and b are associates. If R is an integral domain, then the converse holds.

Proof. We will prove part e), leaving the others as exercises. Suppose that $a = bu$ with u a unit, then, of course, $b|a$. Since $u \in U(R)$, $u^{-1} \in R$ and hence we have that $au^{-1} = b$ and hence $a|b$ so a and b are associates. For the converse statement (assuming that R is a domain), we assume that a and b are associates. Hence there are element $x, y \in R$ such that $a = bx$ and $ay = b$. Combining these two equations, we obtain that $a = yxa$ or $a(1 - yx) = 0$. One of these factors must be 0 since R is a domain. If $a = 0$ then $b = 0$ and we are degenerate. Therefore $1 - yx = 0$ and $1 = yx$. So x (and y) is a unit and we are done. □

We now distinguish between the notions of "irreducibility" and "prime."

Definition 5.4.3. *Let R be commutative with identity. An nonzero, nonunit element $c \in R$ is said to be irreducible if $c = ab$ implies that a or b is a unit of R. The nonzero nonunit element $p \in R$ is said to be prime if $p|(ab)$ implies that $p|a$ or $p|b$.*

Example 5.4.4. *In the integers p being prime and irreducible coincide (and coincides with the familiar notion of "prime integer"). In $\mathbb{Z}$, we also say 0 is prime (the definition above does not cover this, we will see later why this choice is made.*

Example 5.4.5. *Verify that if F is a field, then in the domain $F[x^2, x^3]$ the elements x^2 and x^3 are irreducible elements that are not prime.*

Example 5.4.6. *Verify that in $\mathbb{Z}_6$, the element $\overline{3} = \overline{33}$ is not irreducible, but is prime.*

Theorem 5.4.7. *Let p and c be nonzero elements of an integral domain.*

a) p is prime if and only if (p) is a prime ideal.

b) c is ireducible if and only if (c) is maximal in the set of principal ideals.

c) Any prime element is irreducible.

d) If R is a PID then the notions of prime and irreducible are equivalent.

e) Every associate of an irreducible (resp. prime) element is irreducible (resp. prime).

f) The only divisors of an irreducible, c, are units and associates of c.

Proof. a) Suppose that (p) is prime and $p|ab$. Hence $ab \in (p)$ and hence a or b is an element of (p). This means that p divides a or p divides b. For the converse, suppose that p is a nonzero prime element and that $ab \in (p)$. Therefore $ab = rp$ for some $r \in R$ and hence $p|ab$. Since p is a prime element, $p|a$ without loss of generality and hence $a \in (p)$.

c) Let p be prime and suppose that $p = ab$. Hence $p|ab$ and since p is prime we will say that $p|a$ without loss of generality. So $p = ap'$. Rewriting the equation, we get that $p = pa'b$ and since R is an integral domain, we have that $a'b = 1$. Therefor b is a unit and p is irreducible.

d) We have to show that any irreducible is prime in a PID. Let c be an irreducible element of R and suppose that $c|ab$. Hence $ab = cr$ for some $r \in R$. Suppose that c does not divide a (equivalently the ideal (c) does not contain (a)). Consider the ideal (a, c). This ideal must be principal, say $(a, c) = (x)$. Hence $x|c$ and so $c = yx$. Since c is irreducible, this means that either x ir y is a unit. If y is a unit, this implies that $c|a$ (since $x|a$ and x and c are associates) and this is a contradiction. On the other hand, if x is a unit, then $(a, c) = R$ and there are elements $u, v \in R$ such that

$$ua + vc = 1,$$

multiplying both sides by b, we get

$$uab + vbc = b = (ur + vb)c$$

and $c|b$ and we are done. The others are left for exercises. □

It is not true in general that any element of a domain can be factored into irreducible elements.

Example 5.4.8. *Show that the domain $\mathbb{Z} + x\mathbb{Q}[x]$ is not atomic and neither is $\overline{\mathbb{Z}}$.*

Definition 5.4.9. *We say that a domain, R, is atomic if every nonzero nonunit of R can be factored into a (finite) product of irreducible elements (or atoms).*

Example 5.4.10. *$\mathbb{Z}, \mathbb{Z}[x_1, x_2, \cdots, x_n]$ are examples of atomic domains. More generally any Noetherian domain (that is, all ideals are finitely generated) is atomic.*

Lemma 5.4.11. *Let R be a domain and let x be an element of R that can be factored into prime elements: $x = p_1 p_2 \cdots p_n$. Then this factorization is unique up to reordering and units (that is, if $q_1 q_2 \cdots q_m$ is any other irreducible factorization then $n = m$ and for all $1 \leq i \leq n$, $p_i = u_i q_j$ for some $u_i \in U(R)$).*

Proof. The proof of this lemma is an easy induction. The first step will show how it is done. Assume that we have the prime factorization $x = p_1 p_2 \cdots p_n$ and that

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

with each q_i irreducible. Note that p_1 divides the right side of the above equation, and since p_1 is prime, p_1 must divide one of the q_i's. Without loss of generality we say that p_1 divides q_1 and we have

$$c p_1 = q_1.$$

Since q_1 is irreducible, c must be a unit and hence q_1 is an associate of p_1 (and hence prime). Divide out both sides by p_1 and proceed by induction (this continuation also gives that $n = m$). □

Here is the daddy mack of factorization domains.

Theorem 5.4.12. *Let R be an atomic integral domain. The following conditions are equivalent.*

a) If $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m$ are two irreducible factorizations then $n = m$ and there is a $\sigma \in S_n$ such that $a_i = u_i b_{\sigma(i)}$ with $u_i \in U(R)$ for all $1 \leq i \leq n$.

b) If $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_n$ are two irreducible factorizations then $n = m$ there is a $\sigma \in S_n$ such that $a_i = u_i b_{\sigma(i)}$ with $u_i \in U(R)$ for all $1 \leq i \leq n$.

c) Every nonzero nonunit in R can be factored into prime elements.

Any domain satifying one (hence all) of the above conditions is called a unique factorization domain (UFD).

Proof. The equivalence of a) and c) follow from the above. The fact that a) and b) is equivalent is more difficult and will not be shown here. □

Definition 5.4.13. *We say that a subset (not containing 0) is multiplicatively closed is $s, t \in S$ implies that $st \in S$.*

Lemma 5.4.14. *Let S be a multiplicatively closed subset of R and I an ideal of R such that $I \bigcap S = \emptyset$. Then I can be expanded to a prime ideal $\mathfrak{P}$ containing I such that $\mathfrak{P}$ is maximal with respect to the property that $\mathfrak{P} \bigcap S = \emptyset$.*

Proof. The fact that such an ideal exists is a Zorn's Lemma argument (Zornify the collection of ideals containing I which exclude S). It is an exercise to see that such an ideal (maximal with respect to excluding S) is prime. □

Here is a nice ideal-theoretic characterization of UFD.

Theorem 5.4.15. *Let R be an integral domain. R is a UFD if and only if every nonzero prime ideal contains a nonzero prime element.*

Proof. First assume that R is a UFD and that $\mathfrak{P}$ is a nonzero prime ideal of R. Let $x \in \mathfrak{P}$ be a nonzero element. Since R is a UFD, we factor x into prime elements:

$$x = p_1 p_2 \cdots p_n \in \mathfrak{P}$$

and since $\mathfrak{P}$ is a prime ideal, then (at least) one of the p_i's is in $\mathfrak{P}$. In particular, $\mathfrak{P}$ contains a nonzero prime element.

On the other hand, suppose that R is a domain with the property that every nonzero prime ideal conatins a nonzero prime element. If R is not a UFD, then there is an element $a \in R$ such that a cannot be factored into prime elements. Let S be the multiplicative subset of R generated by primes (every element of S is a product of primes). Note that $(a) \bigcap S = \emptyset$. Indeed, if not, then there is a nonzero $r \in R$ such that ra is a product of primes:

$$ra = p_1 p_2 \cdots p_n.$$

Since each prime divides either r or a, we have that $r = r' p_{i_1} \cdots p_{i_k}$ and $a = a' p_{j_1} \cdots p_{j_m}$. Note that $r', a^p rime$ are necessarily units and hence a is a product of primes which is a contradiction.

Since $(a) \bigcap S = \emptyset$, we can expand (a) to a prime ideal $\mathfrak{P}$ such that $\mathfrak{P} \bigcap S = \emptyset$. But since $\mathfrak{P}$ excludes S, it can contain no prime element, which is a contradiction. □

Corollary 5.4.16. *Any PID is a UFD.*

Proof. Let R be a PID and let $\mathfrak{P}$ be a nonzero prime ideal. $\mathfrak{P} = (x)$ and hence conatins a prime element, so R is a UFD. □

Definition 5.4.17. *Let R be an integral domain. We say that R is a Euclidean domain if there exists a function $\phi : R \setminus \{0\} \longrightarrow \mathbb{N} \bigcup \{0\}$ such that $\phi(a) \leq \phi(ab)$ and if $a, b \in R$ with $b \neq 0$ then there exists $q, r \in R$ such that*

$$a = qb + r$$

with $r = 0$ or $\phi(r) < \phi(b)$.

Example 5.4.18. *$F[x]$ and $F[[x]]$ are Euclidean as well as $\mathbb{Z}$ and $\mathbb{Z}[i]$.*

Theorem 5.4.19. *Any Euclidean domain is a PID and hence a UFD.*

Proof. If I is an (nonzero) ideal in R, consider the element $x \in I$ such that $\phi(x)$ is minimal. It is easy to see that x generates I. □

Definition 5.4.20. *At atomic integral domain is a half-factorial domain (HFD) if given two irreducible factorizations*

$$\pi_1\pi_2\cdots\pi_n = \xi_1\xi_2\cdots\xi_m$$

then $n = m$.

Example 5.4.21. *Let $F \subsetneq K$ be a nontrivial extension of fields, then $F + xK[[x]]$ is an HFD. Another example of an HFD is $\mathbb{Z}[\sqrt{-5}]$ (and of course any UFD is an HFD). An example of a non-HFD is $F[x^2, x^3]$.*

Definition 5.4.22. *Let S be a subset of a commutative ring R. An element d is said to be a greatest common divisor for the set S if*

a) $d|s$ for all $s \in S$ and

b) if $c|s$ for all $s \in S$ then $c|d$.

Theorem 5.4.23. *Let R be a commutative ring with identity.*

a) If R is a PIR then gcd$(a_1, a_2, \cdots, a_n)$ exists and what is more, this greatest common divisor is an $R-$linear combination of the elements $a_1, a_2, \cdots, a_n$.

b) If R is a UFD then gcd$(a_1, a_2, \cdots, a_n)$ exists.

We remark that an integral domain such that any two elements (and hence any finite set of elements) has a greatest common divisor is called a GCD-domain. If a GCD-domain has the additional property that for all a, b, $\gcd(a, b)$ is a linear combination of a and b, then R is called a Bezout domain.

Example 5.4.24. *$F[x, y]$ is a GCD-domain that is not a Bezout domain. Bezeout domains are precisely the domains where every finitely-generated ideal is principal. See if you can find an example of a Bezout domain that is not a PID.*

5.5 Localization

In this section we look at one of the most fundamental constructions in commutative algebra. We will assume that our rings in this section are commutative.

We first recall from the previous section the notion of multiplicative set (that is, a subset of R closed under multiplication. These sets form the basis for the concept of localization (which may be thought of as a generalization of "forming fractions"). Note that the rules that we are used to in multiplying and adding fractions in $\mathbb{Q}$:

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

and

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

seem to naturally demand that the set of "denominators" be closed under multiplication. Basically, if $S \subseteq R$ is a multiplicatively closed set, then we can think of S as a collection of "possible denominators" in some ring that is related to the original ring R. Before we make this precise, we give an example of a fundamental type of multiplicatively closed set.

Example 5.5.1. *Let R be commutative and let $\{\mathfrak{P}_i\}_{i\in I}$ be a collection of prime ideals of R. Then the set*

$$S := R \setminus \bigcup_{i\in I} \mathfrak{P}_i$$

is a multiplicatively closed subset of R. Indeed, if $a, b \in S$ then for all $i \in I$, neither a not b is in $\mathfrak{P}_i$. Since each $\mathfrak{P}_i$ is prime, ab is is no $\mathfrak{P}_i$ either.

Definition 5.5.2. *We say that the multiplicatively closed $S \subseteq R$ is saturated if $st \in S$ implies that $s, t \in S$.*

Theorem 5.5.3. *A set, S, ($0 \notin S$) is multiplicatively closed and saturated if and only if it is the complement of a set theoretic union of prime ideals.*

Proof. It is easy to see that the complement of a set-theoretic union of primes is a saturated multiplicatively closed set...the converse is the more interesting statement.

Suppose that S is a saturated, multiplicatively closed subset of R and suppose $x \in S^{\mathrm{c}}$. Note that since S is saturated, $(x)\bigcap S = \emptyset$. By the previous results, we can expand (x) to a prime ideal $\mathfrak{P}$ such that $\mathfrak{P}\bigcap S = \emptyset$. Hence every element in the complement of S is in a prime ideal that misses S and we are done. □

Proposition 5.5.4. *Let $S \subseteq R$ be a multiplicatively closed subset. The relation on $R \times S$ given by*

$$(r, s) \sim (r', s') \iff \exists t \in S \text{ such that } t(rs' - r's) = 0$$

is an equivalence relation.

Proof. Clearly $(r, s) \sim (r, s)$ and $(r, s) \sim (r', s')$ implies that $(r', s') \sim (r, s)$. Transitivity is what is needed to be shown.

Suppose that $x, y, z \in R$ and $a, b, c \in S$ and that $(x, a) \sim (y, b)$ and $(y, b) \sim (z, c)$. So there are $s, t \in S$ such that $s(xb - ya) = 0$ and $t(yc - zb) = 0$. Multiply the first equation by $ct \in S$ and the second by $as \in S$ to obtain $sctxb - syact = 0$ and $tycas - tzbas = 0$. Now add these two equations to obtain $sctxb - tzbas = 0 = stb(xc - za)$. Since $stb \in S$ we have that $(x, a) \sim (z, c)$. □

Theorem 5.5.5. *Let R be commutative and S a multiplicatively closed subset. The set $S^{-1}R = R_S$ of equivalence classes of $R \times S$ (we denote the equivalence class of (r, s) by $\frac{r}{s}$) forms a commutative ring with identity under the operations*

$$\frac{x}{s} + \frac{y}{t} = \frac{xt + sy}{st}$$

and

$$(\frac{x}{s})(\frac{y}{t}) = \frac{xy}{st}.$$

Additionally, if $R \neq 0$ has no nonzero zero-divisors and $0 \notin S$ then R is an integral domain. What is more, if $R \neq 0$ has no nonzero zero-divisors and $S = R \setminus \{0\}$, then R_S is a field.

Proof. Exercise. □

Proposition 5.5.6. *Let S be a multiplicatively closed subset of R.*

a) For a fixed $s \in S$ the map $\phi_s : R \longrightarrow R_S$ given by $\phi_s(r) = \frac{rs}{s}$ is a well-defined homomorphism of rings such that $\phi_s(t)$ is a unit in R_S for all $t \in S$.

b) If $0 \notin S$ and S contains no zero-divisors, then ϕ_s is one to one. In particular, any integral domain may be embedded in its quotient field.

c) If R has identity and S is a subset of $U(R)$, then ϕ_s is an isomorphism.

Proof. Exercise. □

Theorem 5.5.7. *Let S be a multiplicatively closed subset of R and T a commutative ring with identity. If $f : R \longrightarrow T$ is a homomorphism of rings with $f(s) \in U(T)$ for all $s \in S$ then there exists a unique homomorphism of rings $\overline{f} : R_S \longrightarrow T$ such that $\overline{f}\phi_s = f$. The ring R_S is completely determined up to isomorphism by this property.*

Proof. The map $\overline{f}(\frac{r}{s}) = f(r)(f(s))^{-1}$ is what is needed. Fill in the details. □

We now turn our attention to the (ideal) structural interplay between R and R_S.

Theorem 5.5.8. *Let S be a multiplicatively closed subset of a commutative ring R.*

a) If $I \subseteq R$ is an ideal then $S^{-1}I = \{\frac{x}{s} | x \in I,\ s \in S\}$ is an ideal of R_S.

b) If I, J are ideals in R then

$$S^{-1}(I + J) = S^{-1}I + S^{-1}J$$
$$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$$
$$S^{-1}(I \bigcap J) = S^{-1}I \bigcap S^{-1}J$$

Lemma 5.5.9. *Let S be a multiplicatively closed subset of R (commutative with identity) then $S^{-1}I = S^{-1}R$ if and only if $S \bigcap I \neq \emptyset$.*

Proof. Suppose that $S^{-1}I = S^{-1}R$, in particular, $1 \in S^{-1}I$. So there is an element $t \in S$ (and $\frac{x}{s} \in S^{-1}I$) such that $t(s-x) = 0$. Hence $xt = st \in S$ and $S \bigcap I \neq \emptyset$.

On the other hand, suppose that $x \in S \bigcap I \neq \emptyset$. Note that $x(\frac{1}{x}) = 1 \in S^{-1}I$ and hence $S^{-1}I = S^{-1}R$. □

Proposition 5.5.10. *Let R be commutative with identity, $I \subseteq R$ an ideal and S a multiplicatively closed subset.*

a) $I \subseteq \phi_s^{-1}(S^{-1}I)$.

b) If $I = \phi_s^{-1}(J)$ for some ideal $J \subseteq R_S$, then $S^{-1}I = J$.

c) If $\mathfrak{P}$ is a prime ideal of R and $S \bigcap \mathfrak{P} = \emptyset$, then $S^{-1}\mathfrak{P}$ is a prime ideal of R_S and $\phi_s(S^{-1}\mathfrak{P}) = \mathfrak{P}$.

We remark here that part b) says that every ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal $I \subseteq R$.

Theorem 5.5.11. *Let R be commutative with identity and S a multiplicatively closed subset of R. Then there is a one to one correspondence between primes of R missing S and primes of R_S.*

Proof. Check that the assignment $\mathfrak{P} \mapsto S^{-1}\mathfrak{P}$ works. □

Here we record the standard notation that if $\mathfrak{P}$ is a prime ideal of R then $R_{\mathfrak{P}} = R_S$ where $S = R \setminus \mathfrak{P}$.

Corollary 5.5.12. *Let R be commutative with identity and $\mathfrak{P}$ a prime ideal.*

a) There is a one to one correspondence between primes of $R_{\mathfrak{P}}$ and primes of R contained in $\mathfrak{P}$.

b) $\mathfrak{P}_{\mathfrak{P}}$ is the unique maximal ideal of $R_{\mathfrak{P}}$.

Definition 5.5.13. *Let R be a commutative ring with identity. We say that R is quasi-local (resp. semi-quasi-local) if R has a unique (resp. only finitely many) maximal ideals.*

We note that the terminology "local ring" (resp. "semi-local ring") is reserved for quasi-local rings (resp. semi-quasi-local rings) that are Noetherian.

Theorem 5.5.14. *Let R be commutative with identity. The following conditions are equivalent.*

a) R is quasi-local.

b) All nonunits of R are contained in some fixed maximal ideal $\mathfrak{M} \subsetneq R$.

c) All nonunits of R form an ideal.

5.6 Polynomial and Power Series Rings

We have seen these types of rings (in differents contexts) since at least the days of calculus. Polynomial are fundamental structures in ring theory and power series provide a topological flavor to the mix (the power series ring is a completion of a polynomial ring). We will go teh other way, by defining power series first.

Theorem 5.6.1. *Let $R[[x]] = \{\sum_{n=0}^{\infty} r_n x^n | r_n \in R\}$ be the set of "formal sums" with addition defined by*

$$\sum_{n=0}^{\infty} r_n x^n + \sum_{n=0}^{\infty} s_n x^n = \sum_{n=0}^{\infty} (r_n + s_n) x^n$$

and multiplication by

$$(\sum_{n=0}^{\infty} r_n x^n)(\sum_{n=0}^{\infty} s_n x^n) = \sum_{n=0}^{\infty} c_n x^n$$

where $c_n = \sum_{i=0}^{n} r_i s_{n-i}$. Then $R[[x]]$ is a ring with $R[x] = \{f \in R[[x]] | r_n = 0$ almost everywhere $\}$.

The ring $R[[x]]$ is called the ring of formal power series with coefficients in R and $R[x]$ is the ring of polynomials with coefficients in R.

Proof. Exercise. □

We note that the polynomial rings (or power series rings) can be extended inductively to the $n-$variable case. Polynomial can also be defined for any (infinite) number of variables as well. For power series this is less clear and there are at least three distinct definitions of "what it means" to be a power series ring in infinitely many variables.

Definition 5.6.2. *For a polynomial $f(x) = \sum_{i=0}^{n} r_i x^i$ with $r_n \neq 0$ we define the degree of $f(x)$ ($deg(f)$) to be n. We say that zero polynomial has degree $-\infty$.*

For a power series of the form $x^n \sum_{i=0}^{\infty} r_i x^i$ (with $r_0 \neq 0$) we define the order of $f(x)$ ($ord(f)$) to be n. We say that the order of the zero power series is ∞.

Proposition 5.6.3. *Let f, g be polynomials in $R[x]$ and α, β be power series in $R[[x]]$.*

a) $deg(fg) \leq deg(f) + deg(g)$ and equality holds if the leading coefficient of either f or g is not a zero-divisor.

b) $deg(fg) \leq max(deg(f), deg(g))$.

c) $ord(\alpha\beta) \geq ord(\alpha) + ord(\beta)$ and equality holds if either the smallest coefficient of α or of β is not a zero-divisor.

d) ord$(\alpha+\beta) \geq max($*ord*$(\alpha),$ *ord*$(\beta))$.

Proof. We will prove part a)...the rest are similar. Write $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ where a_n and b_m are both nonzero. Note that

$$f(x)g(x) = (\sum_{i=0}^{n} a_i x^i)(\sum_{j=0}^{m} b_j x^j) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j}$$

and clearly $\deg(fg) \leq n+m$. Also note that if either a_n or b_m is nonzero then $a_n b_m \neq 0$ and we see that in this case equality holds. □

Proposition 5.6.4. *R is commutative (respectively has identity or is a domain) if and only if $R[x]$ is. The same holds if "$R[x]$" is replaced with "$R[[x]]$".*

Proof. We will attempt to prove only that which is not blatently obvious (e.g. the "with identity" statement is an easy check). If R is a domain, the degree (resp order) statements from the above show that $R[x]$ (resp $R[[x]]$) is a domain. On the other hand it is easy to see that if R is not a domain, then neither $R[x]$ nor $R[[x]]$ can be. □

Proposition 5.6.5. *Let R be a commutative ring with identity.*

a) $f(x) \in R[x]$ is a unit if and only if $f(0) \in U(R)$ and all other coefficients are nilpotent (in particular, if R is a domain then the units of $R[x]$ coincide with the units of R).

b) $g(x) \in R[[x]]$ is a unit if and only if $g(0) \in U(R)$.

c) $g(x) \in R[[x]]$ is irreducible if $g(0)$ is irreducible in R.

We remark that "commutativity" is not needed for part b).

Proof. For a) we will show the case where R is an integral domain (the more general case being slightly more complicated, but doable as an exercise). The implication ($\Longleftarrow$) is clear in any case. If R is a domain and f is a unit then there is a polynomial g such that $fg = 1$. By the previous, we have that $\deg(fg) = \deg(f) + \deg(g) = 0$. This forces the degrees of f and g to be 0 (that is, both f and g are in R).

For part b) the implication ($\Longrightarrow$) is clear. So we assume that $g(x) = a_0 + a_1x + a_2x^2 + \cdots \in R[[x]]$ is such that $g(0) = a_0$ is a unit in R. We will inductively build a power series $f(x) = b_0 + b_1x + b_2x^2 + \cdots$ such that $g(x)f(x) = 1$. Clearly we choose $b_0 = a_0^{-1}$. Assume that we have chosen $b_1, b_2, \cdots b_n$ so that

$$\sum_{i=0}^{k} a_{k-i} b_i = 0$$

for all $1 \leq k \leq n$. We merely need to show that we can select b_{n+1} in a similar fashion.

Consider $\sum_{i=0}^{k+1} a_{k+1-i} b_i = \sum_{i=0}^{k} a_{k+1-i} b_i + a_0 b_{k+1}$. So to guarantee that this sum is zero, we merely need to select

$$b_{k+1} = -a_0^{-1}(\sum_{i=0}^{k} a_{k+1-i}b_i).$$

and this completes the proof.

□

Proposition 5.6.6. *Let $I \subseteq R$ be an ideal of the commutative ring wit identity R, $I[x] = \{\sum_{k=0}^{n} \alpha_k x^k | \alpha_k \in I\}$, and $I[[x]] = \{\sum_{k=0}^{\infty} \alpha_k x^k | \alpha_k \in I\}$.*

a) $I[x]$ is an ideal of $R[x]$ and $R[x]/I[x] \cong (R/I)[x]$.

b) $I[[x]]$ is an ideal of $R[[x]]$ and $R[[x]]/I[[x]] \cong (R/I)[[x]]$.

c) I is prime in R if and only if $I[x]$ is prime (resp. maximal) in $R[x]$.

d) I is prime in R if and only if $I[[x]]$ is prime (resp. maximal) in $R[[x]]$.

e) I is prime (resp. maximal) in R if and only if (I, x) is prime (resp. maximal) in $R[x]$.

f) I is prime (resp. maximal) in R if and only if (I, x) is prime (resp. maximal) in $R[[x]]$.

Proof. For a) consider the map $\phi : R[x] \longrightarrow R/I[x]$ given by $\phi(\sum \alpha_k x^k) = \sum \overline{\alpha_k} x^k$ where $\overline{\alpha_k}$ denotes the coset $\alpha_k + I$. It is easy to see that ϕ is onto with kernal $I[x]$. The power series case case in b) is similar. For parts c) and d) we see that if I is prime, then R/I is a domain and hence so is $(R/I)[x]$ and $(R/I)[[x]]$ (and hence $I[x]$ and $I[[x]]$ are prime). Conversely, if $I[x]$ or $I[[x]]$ is prime, then $(R/I)[x]$ or $(R/I)[[x]]$ is a domain which in either case means that R/I is a domain. Hence I is prime.

Finally for parts e) and f), we merely note that $R[x]/(I, x) \cong R/I$ and $R[[x]]/(I, x) \cong R/I$ (the proof is similar to a) and b)). From this observation, the results follow. □

Corollary 5.6.7. *Let R be commutative with identity. Any maximal ideal of $R[[x]]$ is of the form $(\mathfrak{M}, x)$ where $\mathfrak{M} \subseteq R$ is a maximal ideal. In particular, R is a (semi-) quasi-local ring is an only if $R[[x]]$ is a (semi-) quasi-local ring.*

Proof. By the above, any ideal of the form $(\mathfrak{M}, x)$ is maximal. It remains to show that any maximal ideal in $R[[x]]$ is of this form. Let $\Gamma \subseteq R[[x]]$ be a maximal ideal. We first claim that $x \in \Gamma$. If this is not the case, then $x \notin \Gamma$ and by the maximality of Γ, $(\Gamma, x) = R[[x]]$. Hence there are power series $\gamma \in \Gamma$ and $f \in R[[x]]$ such that

$$\gamma + xf = 1.$$

It is immediate that the constant term of γ must be 1, but then $\gamma \in U(R[[x]])$ by the above results. This is a contradiction.

Since $x \in \Gamma$, we will claim that Γ is of the form (I, x) where $I = \Gamma \bigcap R$. It is clear that $(I, x) \subseteq \Gamma$ so we will show the other inclusion. Let $\gamma \in \Gamma$. We write $\gamma = a_0 + xg(x)$ and note that since $x \in \Gamma$, we have

$$\gamma - xg(x) = a_0 \in \Gamma \bigcap R,$$

and hence $gamma \in (I, x)$. Since there is a one to one correspondence between maximal ideals of R and maximal ideals of $R[[x]]$, the statement about (semi-) quasi-local rings follows. □

We note here that the previous results are wildly untrue for polynomials (for example in $\mathbb{Q}[x]$ the ideal $(1 + x)$ is maximal, but does not contain x). This is a fairly rare instance where power series behave nicer than polynomials.

We now look at some rather familiar family of homomorphism obtained by "plugging in."

Proposition 5.6.8. *Let T be a polynomial or power series ring in n variables over R. Let $\overline{v}$ be an element of $R \times R \times \cdots \times R$.*

a) The map $\phi_{\overline{0}} : T \longrightarrow R$ given by $\phi_{\overline{0}}(f) = f(\overline{0})$ is an epimorphism of rings (in the polynomial case $\overline{0}$ can be replaced by $\overline{v}$.

b) The inclusion $\iota : R \longrightarrow T$ is a monomorphism of rings such that $\phi_{\overline{0}}\iota = 1_R$.

Proof. Verification is routine computation. □

Theorem 5.6.9. *Let R and S be commutative with identity and $\phi : R \longrightarrow S$ a homomorphism such that $\phi(1) = 1$. If $s_1, s_2, \cdots, s_n \in S$ then there is a unique $\overline{\phi} : R[x_1, x_2, \cdots, x_n] \longrightarrow S$ such that $\overline{\phi}|_R = \phi$ and $\overline{\phi}(x_i) = s_i$ for all i. The property determines $R[x_1, x_2, \cdots, x_n]$ up to isomorphism.*

Here is a result that illustrates the interplay of localization and polynomials and power series.

Proposition 5.6.10. *Let R be a domain and $S \subseteq R$ a multiplicatively closed set.*

a) $R[x]_S \cong R_S[x]$.

b) $R[[x]]_S \subseteq R_S[[x]]$.

Proof. Part a) is an exercise in collecting denominators. Part b) is similar. □

Example 5.6.11. *Consider the ring $\mathbb{Z}$ and $S = \mathbb{Z} \setminus \{0\}$. It is easy to see that $\mathbb{Z}[[x]]_S \subsetneq \mathbb{Z}_S[[x]]$. In fact equality for part b) of the above rarely happens (one of the equivalent conditions for equality is that for every countable collection of elements $s_i \in S$ it must be the case that $\bigcap R_{s_i} \neq (0)$).*

We will now focus on some factorization and finiteness theorems for $R[x]$ and $R[[x]]$.

We begin with an earlier mentioned result.

Proposition 5.6.12. *Let F be a field, then $F[x]$ and $F[[x]]$ are Euclidean domains.*

Proof. Exercise. The functions to utilize are the degree function (for the polynomial case) and the order function (for the power series case). □

Theorem 5.6.13. *Let R be a UFD, then $R[x]$ is a UFD.*

We remark that the converse is also true (and easier to show).

Proof. We use the earlier characterization of UFD. That is, to show that $R[x]$ is a UFD, it suffices to show that every nonzero prime ideal of $R[x]$ contains a nonzero prime element.

Let Γ be a prime ideal of $R[x]$. First suppose that $\Gamma \bigcap R \neq (0)$. In this case, $\Gamma \bigcap R$ is necessarily a nonzero prime ideal of R (is $ab \in \Gamma \bigcap R$ with $a, b \in R$ then one of a or b is in Γ and R). So, since R is a UFD, it must contain a nonzero prime element (of R). We will call this element p. We will show that p is also prime in $R[x]$.

Suppose that p divides $f(x)g(x)$ but divides neither $f(x)$ nor $g(x)$. If we write $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$ then there is a smallest i such that p does not divide a_i and a smallest j such that p does not divide b_j. Consider the coefficient of x^{i+j} in $f(x)g(x)$:

$$a_0b_{i+j} + \cdots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0.$$

Clearly p divides all of the terms to the left and to the right of a_ib_j. Since p divides the coefficient itself, p divides a_ib_j and as p is prime, p must divide either a_i or b_j and this is a contradiction. So p is prime in $R[x]$. We conclude that any prime ideal Γ such that $\Gamma \bigcap R \neq (0)$ contains a prime element, so we will assume that $\Gamma \bigcap R = (0)$.

Consider the ideal $\Gamma K[x]$ where K is the quotient field of R. Since $\Gamma \bigcap R = (0)$, Γ contains no units of $K[x]$ and is proper. Also since $K[x]$ is a PID, $\Gamma K[x] = (f(x))$ and we can assume that $f(x) \in R[x]$ (by clearing denominators). Additionally, since R is a UFD, we can assume the greatest common divisor the coefficients is 1. Certainly $f(x)$ is prime in $K[x]$ since it generates a prime ideal (and $(f(x))$ is prime because is the localization of the prime ideal Γ). We merely need to show that $f(x)$ is prime in $R[x]$. We start with the claim that if $k(x)f(x) = g(x) \in R[x]$, then $k(x) \in R[x]$. To see this note that $k(x) = \frac{p(x)}{r}$ with $p(x) \in R[x]$ and $r \in R$. Replacing $k(x)$ in the previous equation and multiplying both sides of the equation by r gets us

$$p(x)f(x) = rg(x).$$

Now factor r into primes, $r = p_1p_2 \cdots p_n$. Note that p_1 is prime in $R[x]$ as well and divides $p(x)f(x)$. Since p_1 does not divide $f(x)$ (since the gcd of its terms is 1), it must divide $p(x)$. By induction, $r|p(x)$ and hence $k(x) \in R[x]$.

With this claim established, we see that $\Gamma = (f(x))$ and hence $f(x)$ is our nonzero prime in Γ. □

Corollary 5.6.14. *If R is a UFD then $R[x_1, x_2, \cdots, x_n]$ is a UFD.*

Proof. The base case is the previous result. Inductively, $R[x_1, \cdots, x_{n-1}]$ is a UFD. Hence be the previous (again) $R[x_1, \cdots, x_{n-1}, x_n] = (R[x_1, \cdots, x_{n-1}])[x_n]$ is a UFD. □

We now introduce a couple of auxiliary results that pertain to roots of polynomials.

Definition 5.6.15. *Let $R \subseteq T$ be commutative rings. We say that $t \in T$ is a root of $f(x) \in R[x]$ if $f(t) = 0$.*

We remark that this can be extended to the multi-variable case (or the non-comutative case if the distinction "left" and "right" roots is made.

Proposition 5.6.16. *Let R be commutative with identity. Then $r \in R$ is a root of $f(x) \in R[x]$ if and only $x - r$ divides $f(x)$.*

Proof. Exercise. □

Theorem 5.6.17. *Let $R \subseteq T$ be integral domains and $f \in R[x]$ a nonzero polynomial of degree n. Then $f(x)$ has at most n distinct roots in T.*

Proof. Let $t_1, t_2, \cdots t_k$ be the distinct roots of $f(x)$ in T. By the above results, $f(x) = f_1(x)(x - t_1)$ with $f_1(x) \in T[x]$. Now plug in t_2 to get

$$f(t_2) = f_1(t_2)(t_2 - t_1)$$

and since $t2 \neq t_1$, we have that t_2 is a root of $f_1(x)$. So we write $f(x) = f_2(x)(x - t_2)(x - t_1)$. Proceeding by induction we obtain

$$f(x) = f_k(x)(x - t_k) \cdots (x - t_2)(x - t_1)$$

and since $textdeg(f) = n$, it is easy to see that $k \leq n$. □

The next result is known as the "rational root test".

Theorem 5.6.18. *Let R be a unique factorization domain with quotient field K and let*

$$f(x) = r_0 + r_1 x + \cdots + r_n x^n \in R[x].$$

with $r_0 \neq 0$. If $u = \frac{a}{b}$ is a root of $f(x)$ with a, b relatively prime elements of R then $a|r_0$ and $b|r_n$.

Proof. Since $\frac{a}{b}$ is a root we have $\sum_{i=0}^{n} r_i (\frac{a}{b})^i = 0$. Clearing the denominator, we get

$$r_0 b^n + r_1 a b^{n-1} + \cdots + r_{n-1} a^{n-1} b + r_n a^n$$

and since a and b are relatively prime, $a|r_0$ and $b|r_n$. □

The following is useful (especially in the characteristic p situation) for determining multiple roots. We say that r is a multiple root of $f(x)$ is $f(x) = (x-r)^n g(x)$ where $n > 1$ (if $n = 1$ we say that the root is simple).

Definition 5.6.19. *Let R be a domain and $f(x) = \sum_{i=0}^{n} r_i x^i \in R[x]$. The formal derivative of $f(x)$ is $f'(x) = \sum_{i=1}^{n} i r_i x^{i-1}$.*

Theorem 5.6.20. *Let R be a domain and $f, g \in R[x]$.*

a) $(rf)' = rf'$ *for all* $r \in R$.

b) $(f+g)' = f' + g'$.

c) $(fg)' = fg' + f'g$.

d) $(f^n)' = nf^{n-1}f'$.

e) r is a multiple root of f if and only if $f(r) = 0$ and $f'(r) = 0$.

f) If R is a field and f and f' are relatively prime, then f has no multiple roots.

Proof. Exercise. □

We conclude this section with the famous Eisenstein's criterion.

Theorem 5.6.21. *Let R be a UFD with quotient field K. If*

$$f(x) = r_0 + r_1 x + \cdots + r_n x^n \in R[x]$$

is of degree at least 1 and p is a prime of R such that

a) $p | r_i,\ 0 \leq i \leq n-1$, *and*

b) p does not divide r_n and p^2 does not divide r_0,

then $f(x)$ is irreducible in $K[x]$ (and if the gcd of the coefficients is 1, then f is irreducible in $R[x]$).

Proof. For this proof, we will go ahead and assume that the gcd of the coefficients of f is 1 (since dividing out by a nonzero coefficient does not affect the irreducibility in $K[x]$).

Suppose that $f(x) = k_1(x)k_2(x)$ with $k_1, k_2 \in K[x]$ of positive degree. Write $k_1 = \frac{g_1}{a_1}$ and $k_2 = \frac{g_2}{a_2}$ with $g_1, g_2 \in R[x]$ and $a_1, a_2 \in R$. We can clear the denominators to get

$$a_1 a_2 f(x) = g_1(x) g_2(x)$$

and as we have done before (since R and $R[x]$ are UFDs) we can show that each prime dividing either a_1 or a_2 must divide g_1 or g_2. This allows the reduction to the assumption that

$$f = g_1 g_2$$

with $g_1, g_2 \in R[x]$. Let p be the prime satisfying the Eisenstein criterion above. Note that since p but not p^2 divides r_0 precisely one of the constant coefficients of g_1 or g_2 contains exactly one factor of p (without loss of generality, we will say that the constant coefficient of g_1, a_0, is divisible by p). Since p does not divide f, there must be coefficients of both g_1 and g_2 that are not divisible my p. Let a_k be the smallest degree coefficient of g_1 that is not divisible by p. Write

$$g_1 = a_0 + a_1 x + \cdots + a_k x^k + \cdots a_n x^n$$

and

$$g_2 = b_0 + b_1 x + \cdots + b_m x^m$$

with $(p, b_0) = 1 = (p, a_k)$.

We now note that the k^{th} degree term of f is

$$a_0 p b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0.$$

Since a_i has a factor of p for $0 \leq i \leq k-1$ and p divides the k degree term of f (since $k < \deg(f) = n + m$), then p divides $a_k b_0$ which is a contradiction. □

5.7 A Short (for now) Blurb on Noetherian Rings

Classically, Noetherian rings were defined via the ascending chain condition on ideals. There is an easier (in my book, anyway) characterization of Noetherian rings that involves generators. That is, a ring is Noetherian if every ideal is finitely generated. Finite generation of all ideals (and the ascending chain condition) are very strict conditions on a ring and consequently, there are many nice theorems for Noetherian rings. Additionally, finiteness conditions such as these often lend themselves to computational methods and recently this (and the great improvement in computer power and accessibility) has caused quite a growth in "computational commutative algebra."

We begin by noting that "Noetherian-ness" is considered in the non-commutative case as well, but we begin here by restricting to the commutative.

Theorem 5.7.1. *Let R be a commutative ring. The following conditions are equivalent.*

a) Every ascending chain of ideals stabilizes. That is, if

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

is a ascending chain of ideals of R then there is an n such that $I_k = I_n$ for all $k \geq n$.

b) Every ideal of R is finitely generated.

c) Every prime ideal of R is finitely generated.

Definition 5.7.2. *Any ring satifying one, hence all of the above, is called Noetherian.*

Proof. Exercise. □

We note that for item c) of the above the following lemma may prove useful.

Lemma 5.7.3. *Let R be a commutative ring. If there is an ideal $I \subseteq R$ that is not finitely generated, then there is an ideal $J \subseteq R$ an ideal that is maximal with respect to not being finitely generated, and any such J is prime.*

Proof. Exercise. □

The Noetherian property is preserved under a wide variety of properties some of which we will give in the following.

Theorem 5.7.4. *Let R be a Noetherian ring. Then the following are also Noetherian.*

a) R_S where S is a multiplicatively closed subset of R.

b) R/I where $I \subseteq R$ is an ideal.

Additionally, if R has an identity, then the following are also Noetherain.

c) (The Hilbert Basis Theorem) If R is commutative with identity and R is Noetherian, then so is $R[x]$.

d) If R is commutative with identity and R is Noetherian, then so is $R[[x]]$.

Proof. Later. □

Chapter 6

Modules

6.1 Introduction and preliminaries

The theory of modules is central in the algebra and damn near everywhere where algebra and its techniques are useful. Modules can be thought of as a generalization of two familiar notions: the notion of a vector space and the notion of an abelian group.

Even in the days of calculus, we saw that the study of vector and vector spaces were essential in being able to implement the techniques of multivariable calculus and differential equations effectively. The notion of a vector space is the notion of a mathematical structure that is closed under addition (the sum of two vectors is a vector). More correctly the set of vectors form an abelian group under addition. What sets a vector space apart from an ordinary abelian group is the fact that the set of vectors is equipped with "scalar multiplication" where the scalars come from a field (in elementary courses, usually $\mathbb{R}$ or $\mathbb{C}$).

The notion of an $R-$module is the generalization of "vector space" where the scalars are taken from some ring R (instead of the more specific "field". Since a vector space and its generalization, the $R-$module is first and foremost an abelian group, we also think of $R-$modules as the generalization of abelian group (e.g. an abelian group equipped with "scalar" multiplication from R).

Since the ring R need not be commutative, we will make the definition of left $R-$module first. Throughout this course there will be many theorems for left $R-$modules. The reader should realize that any such theorem has an analog theorem for right $R-$modules.

Definition 6.1.1. *A left $R-$ module is an abelian group $(M,+)$ equipped with a function $R \times M \to M$ (we write $(r,m) \mapsto rm$) such that for all $r,s \in R$ and $a,b \in M$ we have*

a) $r(a+b)=ra+rb$

b) $(r+s)a=ra+sa$

c) r(sa)=(rs)a

We remark here that if $1 \in R$ and $1_R a = a$ for all $a \in M$ then M is called a unitary $R-$module (this will be the default assumption). If R is a division ring we call M a left vector space. As an exercise verify that $0_R(a) = 0_M = (r)0_M$ for all $r \in R$ and $a \in M$.

Example 6.1.2. *Note that any abelian group is a $\mathbb{Z}$ module. The set of continuous functions from $[0,1]$ to $\mathbb{R}$ is an $\mathbb{R}-$vector space. If R is any ring and I is a left ideal of R, then I is a left $R-$module. (It is worth noting that $\mathbb{Z}_2$ is a $\mathbb{Z}-$ module, but not an ideal of $\mathbb{Z}$.) For another example, if $R \subseteq S$ are rings, then S is an $R-$module. For a more exotic example (which we will see again later) let $\mathbb{F}$ be a field and V a vector space over $\mathbb{F}$ and $T : V \longrightarrow V$ a linear transformation. Then V is an $F[x]$ module via*

$$f(x)v = f(T)v.$$

Finally, we note that the analog of $\mathbb{R}$ is a module. More precisely, if R is a ring then

$$\oplus_{\alpha \in \Lambda} R$$

is an $R-$module with "scalar" multiplication given by

$$r\{s_\alpha\}_{\alpha \in \Lambda} = \{rs_\alpha\}_{\alpha \in \Lambda}.$$

Next we generalize the familiar notion of linear transformation (abelian group homomorphism).

Definition 6.1.3. *Let A, B be $R-$modules and $f : A \longrightarrow B$ be a function. We say that f is an (left) $R-$module homomorphism if*

a) $f(x+y) = f(x) + f(y)$ for all $x, y \in A$.

b) $f(rx) = rf(x)$ for all $r \in R$, $x \in A$.

If R is a division ring, then this is called a linear transformation.

Lemma 6.1.4. *$\phi : M \longrightarrow N$ is an $R-$module homomorphism if and only if $\phi(x + ry) = \phi(x) + r\phi(y)$ for all $x, y \in M$ and for all $r \in R$.*

Proof. Exercise. □

Example 6.1.5. *If A, B are any abelian groups then "$\mathbb{Z}-$ module homomorphism" is synonomous with "abelian group homomorphism".*

Example 6.1.6. *The function $f_n : \mathbb{Z} \longrightarrow \mathbb{Z}$ given by $f_n(x) = nx$ is a $\mathbb{Z}-$module homomorphism, but not a ring homomorphism. The same is true of the function $g : R[x] \longrightarrow R[x]$ given by $g(r(x)) = xr(x)$ (i.e., this is an $R-$module homomorphism which is not a ring homomorphism.*

As is the case with our other morphisms, we can talk about "mono" (injective), "epi" (surjective), and bijective $R-$module homomorphisms. The terminology will be analogous to earlier terminology in groups and rings.

It is important at this juncture to introduce an important class of abelian groups that are, in certain important cases, also $R-$modules.

Proposition 6.1.7. *Let M and N be $R-$modules. The set $Hom_R(M,N) = \{\phi : M \longrightarrow N | \phi$ is an $R-$module homomorphism.$\}$ is an abelian group (under pointwise addition of functions). Additionally, if R is commutative, then $Hom_R(M,N)$ is an $R-$module.*

Proof. We will leave the fact that $\mathrm{Hom}_R(M,N)$ is an abelian group as an exercise and verify the second statement. If R is commutative then we define the scalar multiplication by

$$(r\phi)(x) = r(\phi(x))$$

for all $r \in R$. Then it is easy to see that $\mathrm{Hom}_R(M,N)$ is an $R-$module. □

Definition 6.1.8. *Let M be a left $R-$module and N a subgroup of M. We say that N is a (left) submodule of M if $rN \subseteq N$ for all $r \in R$.*

Proposition 6.1.9. *Let R be a ring and M a (unitary) left R module. Then $N \subseteq M$ is a left $R-$submodule of M if and only if N is nonempty and $x+ry \in N$ for all $x, y \in N$ and $r \in R$.*

Proof. The necessity of the condition is straightforward. Assume that for all $x, y \in N$ and $r \in R$, $x + ry \in N$. Choose $r = -1$ to see that for all $x, y \in N$, $x-y \in N$. So N is an abelian group. Now choose $x = 0$ to see that $rN \subseteq N$. □

Example 6.1.10. *If M is a $\mathbb{Z}-$module then any subgroup of M is a $\mathbb{Z}-$submodule of M.*

Example 6.1.11. *If $f : A \longrightarrow B$ is an $R-$homomorphism, then $ker(f) = \{x | f(x) = 0\}$ is an $R-$submodule of A. Additionally, $Im(f) = \{f(x) | x \in A\}$ is an $R-$submodule of B. If $C \subseteq B$ is an $R-$submodule of B then $f^{-1}(C) = \{x \in A | f(x) \in C\}$ is an $R-$submodule of A.*

Example 6.1.12. *If X is a subset of some $R-$module, A, then $\langle X \rangle$ (the $R-$submodule spanned by X) is the intersection of all $R-$submodules of A containing X. That is:*

$$\langle X \rangle = \bigcap_{X \subseteq M \subseteq A} M.$$

If $X = \bigcup_{i \in I} B_i$ where each B_i is an $R-$submodule of A, then $\langle X \rangle$ is called the sum of the B_i's and if $I = \{1, 2, \cdots, n\}$ then $\langle X \rangle = B_1 + B_2 + \cdots + B_n$.

We conclude this section with a special and important class of $R-$modules.

Definition 6.1.13. *Let R be commutative with 1. An $R-$algebra is a ring A with identity equipped with a ring homomorphism $f : R \longrightarrow A$ $(f(1_R) = 1_A)$ such that $f(R)$ is contained in the center of A.*

Proposition 6.1.14. *If A is an $R-$algebra, then A is an $R-$module.*

Proof. We define $a(r) = r(a) = f(r)a$. Note that $1(a) = f(1)a = 1_A a = a$. For the second property $(r+s)a = (f(r+s))a = (f(r) + f(s))a = f(r)a + f(s)a = ra + sa$. Also $(rs)a = (f(rs))a = (f(r)f(s))a = f(r)(f(s)a) = f(r)(sa) = r(sa)$ and finally $r(a+b) = f(r)(a+b) = f(r)a + f(r)b = ra + rb$. □

Example 6.1.15. *A good canonical example of an $R-$algebra is the matrix ring $M_n(R)$. The relevant homomorphism is the map that takes the element $r \in R$ to the $n \times n$ diagonal matrix with all r's on the diagonal.*

Definition 6.1.16. *If A and B are $R-$algebras then an $R-$algebra homomorphism $\phi : A \longrightarrow B$ is a ring homomorphism such that*

a) $\phi(1_A) = 1_B$ and

b) $\phi(ra) = r\phi(a)$ for all $r \in R$ and $a \in A$.

6.2 Quotient Structures and the Homomorphism Theorems

The idea of quotient structure is the analog of what we have seen in the theory of groups and rings. We begin with the following theorem.

Theorem 6.2.1. *Let $B, C \subseteq A$ be modules.*

a) The quotient group A/B is an $R-$module with $R-$action given by $r(a + B) = ra + B$.

b) The map $\pi_B : A \longrightarrow A/B$ given by $\pi_B(a) = a + B$ is an $R-$module homomorphism with kernal B.

c) There is an $R-$module homomorphism $B/(B \bigcap C) \cong (B + C)/C$.

d) If $C \subseteq B$ then $B/C \subseteq A/C$ and $(A/C)/(B/C) \cong A/B$.

Proof. For part a) it suffices to show that the action is well-defined. Suppose that $x + B = y + B$. Hence $x - y \in B$ and so $r(x - y) \in B$. We conclude that $rx + B = ry + B$ and the action is well-defined. Showing that the multiplication satisfies the axioms is easy since A is an $R-$module. Part b) is routine. Parts c) and d) are consequences of the next theorem and we leave them for exercises. □

An application of the next result is the "best way" to prove parts c) and d) of the above theorem. There are myriad others. This is called the first isomorphism theorem.

Theorem 6.2.2. *Let $f : A \longrightarrow B$ be an $R-$module homomorphism, then f induces and $R-$module isomorphism*

$$\overline{f} : A/ker(f) \xrightarrow{\cong} Im(f).$$

Proof. Define the map

$$\overline{f} : A/\ker(f) \longrightarrow \mathrm{Im}(f)$$

via $\overline{f}(a+\ker(f)) = f(a)$. Since f is an $R-$module homomorphism, it is easy to see that $\overline{f}$ is as well. It is also clear that $\overline{f}$ is onto the image of f. It remains to show that $\overline{f}$ is one to one, and so assume that $\overline{f}(a+\ker(f)) = 0 = f(a)$. This means that $a \in \ker(f)$ and we are done. □

For our last result we will produce a corollary that shows submodule corresponce in quotient structures.

Corollary 6.2.3. *If R is a ring and $B \subseteq A$ are $R-$modules then there is a 1-1 correspondence between submodules of A/B and submodules of A containing B.*

Proof. Let C be a submodule of A containing B. We know that from a previous result that $C/B \subseteq A/B$. On the other hand, assume that M is a submodule of A/B. Consider the canonical projection

$$\pi_B : A \longrightarrow A/B.$$

Now consider the submodule of A: $\pi_B^{-1}(M)$. Verify that $M \longleftrightarrow \pi_B^{-1}(M)$ gives pur 1-1 cprrespondence. □

6.3 The Direct Product and Direct Sum

As one may expect the universal constructions of direct product and direct sum have an important analog in the theory of modules. We will see that the central theorems from abelian group theory carry over in this realm, and in particular we will see later that any $R-$module is the homomorphic image of a particular direct sum of special $R-$modules.

Theorem 6.3.1. *Let $\{A_i\}_{i\in I}$ be a family of $R-$modules and $\prod_{i\in I} A_i$ and $\oplus_{i\in I} A_i$ be respectively the direct product and direct sum of the family as abelian groups.*

a) The direct product $\prod_{i\in I} A_i$ is an $R-$module with $R-$action given by $r\{a_i\}_{i\in I} = \{ra_i\}_{i\in I}$.

b) The direct sum $\oplus_{i\in I} A_i$ is an $R-$submodule of $\prod_{i\in I} A_i$ with the inherited $R-$action.

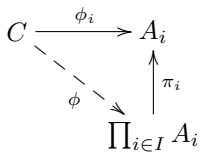
c) For all $k \in I$ the canonical projection $\pi_k : \prod_{i\in I} A_i \longrightarrow A_k$ ($\pi_k(\{a_i\}) = a_k$) is an $R-$module epimorphism.

d) For each $k \in I$ the canonical injection $\iota_k : A_k \longrightarrow \oplus_{i\in I} A_i$ ($\iota_k(a) = \{x_i\}_{i\in I}$ where $x_i = 0$ if $i \neq k$ and $x_k = a$) is an $R-$module monomorphism.

Proof. The proof of this is extremely similar to the proof of the analog theorem from group theory. □

As was the case earlier, the direct product and direct sum are (unique) solutions to certain universal mapping problems.

Theorem 6.3.2. *If R is a ring, $\{A_i | i \in I\}$ is a family of $R-$modules, C is an $R-$module and $\{\phi_i : C \longrightarrow A_i | i \in I\}$ is a family of $R-$module homomorphisms then there is a unique $R-$module homomorphism $\phi : C \longrightarrow \prod_{i\in I} A_i$ such that $\pi_i\phi = \phi_i$ for all $i \in I$. Additionally $\prod_{i\in I} A_i$ is uniquely determined (up to isomorphism) by this property.*

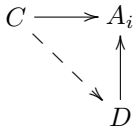


Proof. $\phi(c) = \{\phi_i(c)\}_{i\in I}$ is the map (verify that this is indeed an $R-$module homomorphism). Assume that ξ is another such $R-$module homomorphism satisfying the universal mapping problem.

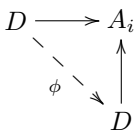
We write $\xi(c) = \{c_i\}$ and note that $\pi_i(\xi(c)) = c_i = \phi_i(c)$. Hence each $c_i = \phi_i(c)$ and $xi \equiv \phi$.

We will next demonstrate that the direct product is the unique (up to isomorphism) solution to this universal mapping problem.

Assume that D is another solution to this universal mapping problem (i.e. D is an $R-$module that has the same properties as the direct product). We have the diagram:

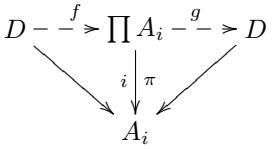


in particular, replacing C with D we obtain

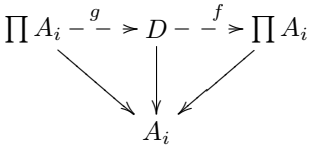


and we note that $\phi = 1_D$ is an obvious solution to this mapping problem and so ϕ must be precisely 1_D by uniqueness.

We now consider the augmented diagram



Considering the "big triangle" we see that $gf = 1_D$ must be the solution by uniqueness. Augmenting the diagram from a different perspective (swapping the roles of D and $\prod A_i$ since they are both solutions to the universal mapping problem) we get the diagram

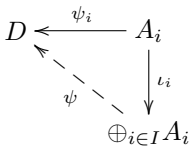


and in a similar fashion to the above, we obtain that $fg = 1_{\prod A_i}$.

In conclusion, we obtain that $gf = 1_D$ and $fg = 1_{\prod A_i}$ and hence $D \cong \prod A_i$. □

There is a dual result with respect the direct sum (more precisely, the direct sum rears its head as the solution to the dual mapping problem).

Theorem 6.3.3. *If R is a ring, $\{A_i | i \in I\}$ is a family of $R-$modules, D is an $R-$module and $\{\psi_i : A_i \longrightarrow D | i \in I\}$ is a family of $R-$module homomorphisms, then there is a unique $R-$module homomorphism $\psi : \oplus_{i\in I} A_i \longrightarrow D$ such that $\psi\iota_i = \psi_i$ for all $i \in I$. What is more, the direct sum is uniquely determined up to isomorphism by this property.*



Proof. The proof here is "dual" (e.g. essentially the same with the arrows reversed) to the previous proof. The unique map in question is $\psi(\{a_i\}) = \sum_{i\in I} \psi_i(a_i)$. Note that since $\{a_i\} \in \oplus_{i\in I} A_i$ all but finitely many of the a_i's are 0 and hence the sum $\sum_{i\in I} \psi_i(a_i)$ is finite and "makes sense". □

We conclude this brief look at these constructions with the following result, which is a nice characterization of when an $R-$ module is a direct sum of some of its submodules.

Proposition 6.3.4. *Let R be a ring and $\{A_i\}_{i\in I}$ a family of $R-$ submodules of A such that*

a) A is the sum of the family $\{A_i\}$.

b) For all $k \in I$, $A_k \bigcap \overline{A_k} = 0$ where $\overline{A_k}$ is the sum of $\{A_i\}_{i \neq k}$.

Then $A \cong \oplus_{i \in I} A_i$.

Proof. Define $\phi : \oplus_{i \in I} A_i \longrightarrow A$ by $\phi(\{a_i\}) = \sum_{i \in I} a_i$. Since $\{a_i\}$ is an element of $\oplus A_i$, this sum is finite. The verification that ϕ is an $R-$module homomorphism is routine. We will show that ϕ is one to one and onto.

To see that ϕ is one to one, suppose that $\{a_i\} \in \ker(\phi)$ and that at least one of the a_i's (say a_k) is nonzero. We therefore have that

$$-a_k = \sum_{i \neq k} a_i$$

and hence a_k is an element of both A_k and the submodule of A generated by the family $\{A_i\}_{i \neq k}$. By assumtion, this means that $a_k = 0$ which is our contradiction, and hence $\ker(\phi) = 0$.

For the onto-ness (what a word) let $a \in A$. Since the sum of the A_i's is precisely A, we know that there is a (finite) sum $a_{i_1} + \cdots + a_{i_k}$ that is equal to a. Let $\{x_j\}$ be the sequence defined by $x_{i_1} = a_{i_1}, \cdots, x_{i_k} = a_{i_k}$ and $x_j = 0$ for all other indices. Note that $\phi(\{x_j\}) = a$. □

6.4 Exact Sequences

Exact sequences are the genesis of some very very important tools in commutative algebra, homological algebra, algebraic K-theory, and algebraic topology. Exact sequences of $R-$modules can contain such (seemingly) diverse information as factorization information of a commutative ring and the basic genus structure of a topological space.

Definition 6.4.1. *A sequence of $R-$module homomorphisms*

$$\cdots \longrightarrow A_{n-1} \xrightarrow{f_n} A_n \xrightarrow{f_{n+1}} A_{n+1} \longrightarrow \cdots$$

is called exact at A_n if $Im(f_n) = ker(f_{n+1})$. We say that the sequence is exact if it is exact at A_n for all n.

Definition 6.4.2. *An exact sequence of the form*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is called a short exact sequence (SES) if f is one to one, g is onto and $ker(g) = Im(f)$.

As it turns out, short exact sequences are the building blocks of general exact sequences in the following sense. If

$$\cdots \longrightarrow A_{n-1} \xrightarrow{f} A_n \xrightarrow{g} A_{n+1} \longrightarrow \cdots$$

then this sequence can be obtained by "splicing together" certain short exact sequences (as an exercise you should try to figure out how this is done).

Example 6.4.3. *a) The sequence* $0 \longrightarrow A \xrightarrow{f} B$ *is exact if and only if* f *is 1-1, the sequence* $B \xrightarrow{g} C \longrightarrow 0$ *is exact if and only if* g *is onto, the sequence* $0 \longrightarrow A \xrightarrow{h} B \longrightarrow 0$ *is exact if and only if* h *is onto.*

b) If $n \neq 0$*, the sequence* $0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{\pi_n} \mathbb{Z}_n \longrightarrow 0$ *with* $f(k) = nk$ *and* $\pi_n(a) = \overline{a}$ *(the reduction of a modulo n) is a short exact sequence.*

c) Any sequence of the form $0 \longrightarrow A \xrightarrow{f} A \oplus C \xrightarrow{g} C \longrightarrow 0$ *with* $f(a) = (a, 0)$ *and* $g(a, c) = c$ *is short exact. (It should be noted that there are usually many ways to have the maps make the sequence be exact, for example if* $A = C$*, we could also have* $f(a) = (a, a)$ *and* $g(x, y) = x - y$*). This example is a special kind of short exact sequence called a split exact sequence. Since the middle term is the sum of the second and fourth, there are maps* $h : C \longrightarrow A \oplus C$ *such that* $gh = 1_C$ *and there is a* $k : A \oplus C \longrightarrow A$ *such that* $kf = 1_A$*. In other words we could "run" the sequence in reverse. An example of a short exact sequence that does not split is given above in b) if* $n \neq 1$*.*

We now introduce a couple of results that are fundamental if you wish to apply the concept of exactness. The proofs of most of these will be omitted as exercises, but all of them require an interesting (and fun) technique known as a "diagram chase." This technique will be demonstrated in the proof of the short five lemma (but all of the diagram chase proofs are similar.

This first result is called the five lemma.

Proposition 6.4.4. *Consider the following commutative diagram of* $R-$*module homomorphisms with exact rows*

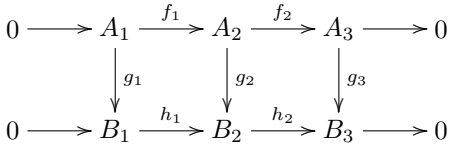
$$\begin{array}{ccccccccc} A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \xrightarrow{f_3} & A_4 & \xrightarrow{f_4} & A_5 \\ \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_2} & & \downarrow{\scriptstyle g_3} & & \downarrow{\scriptstyle g_4} & & \downarrow{\scriptstyle g_5} \\ B_1 & \xrightarrow{h_1} & B_2 & \xrightarrow{h_2} & B_3 & \xrightarrow{h_3} & B_4 & \xrightarrow{h_4} & B_5 \end{array}$$

a) If g_2 *and* g_4 *are onto and* g_5 *is one to one then* g_3 *is onto.*

b) If g_2 *and* g_4 *are one to one and* g_1 *is onto then* g_3 *is one to one.*

Now we produce a corollary which is often referred to as the short five lemma.

Corollary 6.4.5. *Consider the following commutative diagram of* $R-$*module homomorphisms with exact rows*



a) If g_1 and g_3 are onto then g_2 is onto.

b) If g_1 and g_3 are one to one then g_2 is one to one.

c) If g_1 and g_3 are isomorphisms that g_2 is an isomorphism.

Before beginning the proof, we note that this follows directly from the five lemma, but we will prove this result from scratch to demonstrate the technique of diagram chasing.

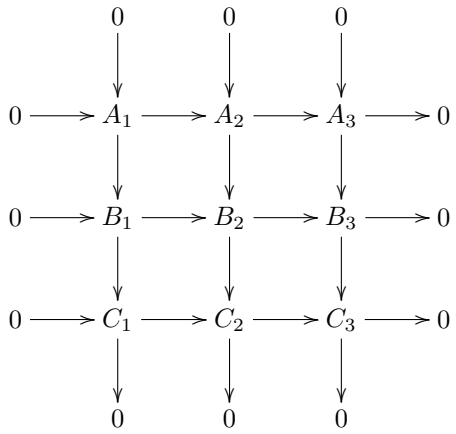
Proof. Of course c) follows directly from a) and b) so we will only show a) and b).

For a) let $b_2 \in B_2$. The only direction that we can go is to the left so let $b_3 = h_2(b_2) \in B_3$. Since g_3 is onto, there is a $a_3 \in A_3$ such that $g_3(a_3) = b_3$. Additionally, f_2 is onto, so we can find $a_2 \in A_2$ such that $f_2(a_2) = a_3$. Now we consider $x = g_2(a_2) \in B_2$ (if $x = b_2$ we are done, but there is no guarantee of this). Note that by commutativity of the diagram, we have that $h_2(x) = b_3 = h_2(b_2)$ and hence $h_2(b_2 - x) = 0$, that is, $b_2 - x \in \ker(h_2) = \text{im}(h_1)$. Consequently, there is a $b_1 \in B_1$ such that $h_1(b_1) = b_2 - x$. Now since g_1 is onto there is an $a_1 \in A_1$ such that $g_1(a_1) = b_1$, and by the commutativity of the diagram $g_2(f_1(a_1)) = b_2 - x$. Notice that $y = f_1(a_1) \in A_2$ and $g_2(y + a_2) = g_2(y) + g_2(a_2) = b_2 - x + x = b_2$ and hence g_2 is onto.

For b) assume that $a_2 \in \ker(g_2)$, and hence $g_2(a_2) = 0$ and so $h_2(g_2(a_2)) = g_3(f_2(a_2)) = 0$ by commutativity of the diagram. Since g_3 is one to one, we have that $f_2(a_2) = 0$, so $a_2 \in \ker(f_2) = \text{im}(f_1)$. So we can find (a unique, since f_1 is one to one) element a_1 such that $f(a_1) = a_2$. Note that $g_2(f_1(a_1)) = 0 = h_1(g_1(a_1))$ Since both h_1 and g_1 are one to one, a_1 must be 0, and hence $a_2 = f_1(a_1) = f_1(0) = 0$ and g_2 is one to one. This completes the proof. □

The next result is known as the 3×3 lemma.

Theorem 6.4.6. *Consider the following commutative diagram of $R-$module homomorphisms*

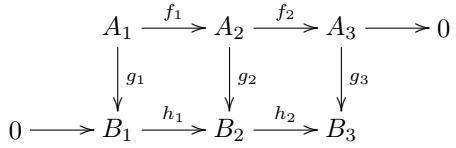


a) If the columns and the bottom two rows are exact, then the top row is exact.

b) If the columns and the top two rows are exact, then the bottom row is exact.

Our final "homological theorem" is the very famous snake lemma and it is one of the major tools of homological algebra and its applications. The important part of the result is the existence of the well-defined homomorphism ∂ called the boundary map which allows passage from n^{th} homology to $(n-1)^{\text{th}}$ homology.

Theorem 6.4.7. *Consider the following commutative diagram with exact rows*



then there is an exact sequence

$$ker(g_1) \xrightarrow{\alpha_1} ker(g_2) \xrightarrow{\alpha_2} ker(g_3) \xrightarrow{\partial} coker(g_1) \xrightarrow{\beta_1} coker(g_2) \xrightarrow{\beta_2} coker(g_3)\,.$$

Additionally, if f_1 is one to one, then so is α_1 and if h_2 is onto, then so is β_2.

We will close out this section with a result that characterizes when a short exact sequence is a split exact sequence.

Theorem 6.4.8. *Let R be a ring and*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

a short exact sequence of $R-$module homomorphisms. Then the following conditions are equivalent.

a) There is an $R-$module homomorphism $h : C \longrightarrow B$ such that $gh = 1_C$.

b) There is an $R-$module homomorphism $k : B \longrightarrow A$ such that $kf = 1_A$.

c) $B \cong A \oplus C$.

We remark that this will be our formal definition of a split exact sequence; namely a split exact sequence is a short exact sequence satisfying one, and hence all, of the above conditions.

Proof. For a)$\Longrightarrow$ b) we need to find an intelligent way to associate an element of A with a given element $b \in B$. We do this by "cleaning" b. Given a $b \in B$, we are not guaranteed an element $a \in A$ such that $f(a) = b$, so we consider $hg(b) \in B$. Note that $g(b - hg(b)) = g(b) - ghg(b) = g(b) - g(b) = 0$. We conclude that $b - hg(b) \in \ker(g) = \text{im}(f)$. With this insight, we define $k(b) = f^{-1}(b - hg(b))$. Since f is one to one, this assignment is well-defined. Suppose that $f^{-1}(b_1 - hg(b_1)) = a_1$ and that $f^{-1}(b_2 - hg(b_2)) = a_2$ and note that $f(a_1 + a_2) = b_1 + b_2 - hg(b_1 + b_2)$. Hence we have that $k(b_1 + b_2) = f^{-1}(b_1 + b_2 - hg(b_1 + b_2)) = a_1 + a_2 = k(b_1) + k(b_2)$. The proof that $k(rb) = rk(b)$ is similar. Note that $kf(a_1) = f^{-1}(f(a_1) - hgf(a_1)) = f^{-1}(f(a_1)) = a_1$ and so a) implies b).

For b)$\Longrightarrow$ c) consider the map $\phi : B \longrightarrow A \oplus C$ given by $\phi(b) = (k(b), g(b))$ (verify that this is an $R-$module homomorphism). First let $b \in \ker(\phi)$. So we have $k(b) = 0$ and $g(b) = 0$. This means that $b \in \ker(g) = \text{im}(f)$ and so there is an $a \in A$ such that $b = f(a)$. Therefore $0 = k(b) = k(f(a)) = a$. Since $a = 0$, we have that $b = 0$ and ϕ is one to one.

Now let $(a, c) \in A \oplus C$ be arbitrary. Since g is onto we can select $b \in B$ such that $g(b) = c$. Unfortunately, it may not be the case that $k(b) = a$. We can, however, vary b by any element of $\ker(g) = \text{im}(f)$. Some computations show that the appropriate element to choose is $b - fk(b) + f(a)$. Indeed note that $\phi(b - fk(b) + f(a)) = (k(b - fk(b) + f(a)), g(b - fk(b) + f(a)) = (k(b) - kfk(b) + kf(a), g(b)) = (a, c)$ and ϕ is an isomorphism.

For now we leave c)$\Longrightarrow$ a) as an exercise.

□

6.5 Free Modules

Free modules are, in a certain sense, the easiest modules to picture (they are most like the more familiar vector spaces). Free modules are also the "mothers of all modules" in the sense that every $R-$module is the homomorphic image of a free $R-$module. Free modules are precisely that modules that have a notion of a basis (a very nice generating set) and we begin with the definition of a basis.

Definition 6.5.1. *A subset X of an $R-$module M is said to be linearly independent if given any $x_1, x_2, \cdots, x_n \in X$, the relation*

$$\sum_{i=1}^{n} r_i x_i = 0$$

implies that $r_i = 0$ *for all* $1 \leq i \leq n$.

We remark (surprise, surprise) that a set that is not linearly independent is called linearly dependent. Also if M is generated by X, we say that X spans M. Finally we tie these together by saying that a linearly independent subset of M that spans M (if such a subset of M exists) is called a basis of M. Modules which actually have a basis are free modules that we have been alluding to.

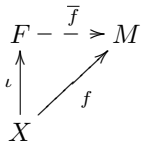
Theorem 6.5.2. *Let R be a ring with identity and F a unitary $R-$module. The following conditions are equivalent.*

a) F has a nonempty basis.

b) F is the (internal) direct sum of a family of cyclic $R-$modules each of which is isomorphic to R as an $R-$module.

c) F is $R-$module isomorphic to a direct sum of some number of copies of the $R-$module R.

d) There exists a nonempty set X and a function $\iota : X \hookrightarrow F$ such that given any unitary $R-$module M and function $f : X \longrightarrow M$, there exists a unique $R-$module homomorphism $\overline{f} : F \longrightarrow M$ such that $\overline{f}\iota = f$.



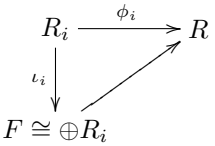
Proof. We first consider a) implies b). Let X be a basis of F. Note that if $x \in X$ then $R \cong Rx$ as a left $R-$module (since the singleton set $\{x\}$ is linearly independent). Also note that $F = \sum_{x \in X} Rx$ (but the sum may not be direct and that is what we need to show). Suppose that $m \in Rx \bigcap (\sum_{y \in X \setminus x} R_y)$ then we can write

$$rx = \sum r_i y_i$$

and hence the set X is linearly dependent.

The implication b) implies c) is easy and is left to the reader.

For c) implies d) let $F \oplus R_i$ with each R_i isomorphic is R via $R_i \xrightarrow{\phi_i} R$. So (for all i we have the commutative diagram



Define $X = \{x_i\}_{i \in I}$ where x_i is such that $\phi_i(x_i) = 1_R$. So our function *iota* : $X \longrightarrow F$ assigns to each cyclic generator its image in F. That is $\iota(x_i) = \iota_i(x_i)$ and say that $f : X \longrightarrow M$ makes the assignment $f(x_i) = m_i \in M$. The desired homomorphism is the homomorphism that obeys the rule:

$$\overline{f}(\sum r_i \iota_i(x_i)) = \sum r_i m_i$$

and uniqueness is an easy exercise.

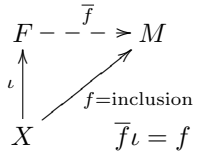
We leave the last implication to the reader.

□

Here is an important corollary that reflects the universal nature and importance of free modules.

Corollary 6.5.3. *Every unitary module M over a ring with identity is the homomorphic image of a free $R-$module. In fact, if M is finitely generated, then the free module may be chosen to be finitely generated.*

Proof. Let X be a generating set of M and consider the diagram



In the diagram above the module F is free on the set X (note that if X is finite then F is finitely generated). We have an induced homomorphism $\overline{f} : F \longrightarrow M$ and $X \subset \text{im}(\overline{f})$ therefore since X is a generating set, $\text{im}(\overline{f}) = M$ and this gets the first statement. Also as was pointed out earlier, if M is finfitely generated (that is, X my be chosed to be finite) then F is finitely generated. □

Here we do a little specialization to the case of vector spaces.

Lemma 6.5.4. *A maximal linearly independent subset of a vector spcae V over a division ring D is a basis of V.*

Proof. Let X be a maximal linearly independent subset (how do we know such an animal exists...we don't yet, but will later see that in important cases these do exist). Let W be a subspace of V spanned by X. If $W = V$ then we are done so we selesct $a \in V \setminus W$. Of course $\{a\} \bigcup X$ must be linearly dependent, so we have an equation of the form

$$ra + \sum r_i x_i = 0$$

with $x_i \in X$, $r, r_i \in R$ and $r \neq 0$ (if the last condition does not hold then the linear independence of the set X would force all of the r_i's to be 0 as well).

Manipulating this equation gives us that

$$a = \sum -r^{-1} r_i x_i \in V$$

which is a contradiction. Hence there is no $a \in V \setminus W$ and so $V = W$ and we are done. □

Here is a big module structure theorem for modules over a division ring (vector spaces). This is why "linear algebra" is much easier that modules in general...over a field modules are always free.

Theorem 6.5.5. *Every vector space V over a division ring D has a basis and is therefore free. More generally, every linearly independent subset of V is contained in a basis of V.*

Before we prove this theorem, we also remark that if every unitary module over a ring with identity, D, is free, then D is a division ring.

We also point out that this business about "every linearly independent subset of V is contained in a basis for V" does not extend to free modules over a general ring. Indeed if you consider the simple example of $\mathbb{Z}$ as a $\mathbb{Z}$ module, consider the maximal linearly independent subset $\{2\}$. This set is not contained in a basis for $\mathbb{Z}$, because any two element subset of the integers is linearly independent. The problem here is that $\{2\}$ does not span $\mathbb{Z}$ and we immediately see the contrasting situation of a ring not being a division ring (i.e., we can see that we somehow need $\frac{1}{2}$ to be an integer for the set $\{2\}$ to have a chance of spanning $\mathbb{Z}$).

Proof. We will prove the more general statement and capture it all at once.

Suppose that X is a linearly independent subset of V (note that such a set has to exist in a nonzero vector space). Consider the collection of linearly independent subsets of V that contain X (and we will call it Γ). This is a partially ordered set under inclusion. Let $\{\mathfrak{C}_i\}$ be a chain in Γ. Note that $C = \bigcup_i \mathfrak{C}_i$ is linearly independent (verify!) and hence is an upper bound for the chain in Γ. Thus Zorn's Lemma gives the existence existence of a maximal element and this establishes the theorem. □

Remark 6.5.6. *If R is a ring that has a division ring as a homomorphic image (e.g. any commutative ring with identity), then R has the invariant dimension property. That is for any free module F over R, any two bases have the same cardinality. If R has the invariant dimension property, then two free modules E and F are isomorphic if and only if they have the same rank. For an example of a ring which does not have the invariant dimension property consider K, a field, and $F = \oplus_{n=1}^{\infty} K$. If $R = Hom_K(F, F)$. For any n, $R \cong \oplus_{m=1}^{n} R$ (check this).*

In closing we look at a couple of familiar properties of vector spaces. The proofs are left as exercises.

Theorem 6.5.7. *Let W be a subspace of V.*

a) $dim_D(W) \leq dim_D(V)$.

b) If $dim_D(W) = dim_D(V)$ and $dim_D(V)$ is finite, then $W = V$.

c) $dim_D(V) = dim_D(W) + dim_D(V/W)$.

d) *If* $f : V \longrightarrow W$ *is a linear transformation then* $dim_D(V) = dim_D(ker(f)) + dim_D(im(f))$.

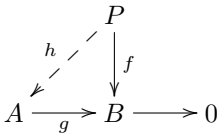
e) *If* V *and* W *are finite dimensional then* $dim_D(V) + dim_D(W) = dim_D(V \bigcap W) + dim_D(V + W)$.

Example 6.5.8. *Build a* 2×2 *matrix and examine the above theorem.*

6.6 Projective and Injective Modules

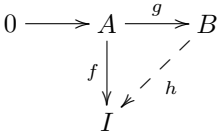
We will define and prove some of the analogous results for projectives and injectives. Please note the "dual" (arrow reversing) nature of some of the definitions and results. For many projective (respectively injective) results there is a very similar injective (resp. projective) result.

Definition 6.6.1. *Consider the following diagram of* $R-$*modules with the bottom row exact.*



We say that P *is projective if there is an* $R-$*module homomorphism* $h : P \longrightarrow A$ *such that* $gh = f$.

Definition 6.6.2. *Consider the following diagram of* $R-$*modules with the top row exact.*

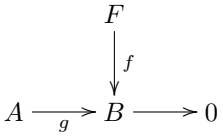


We say that I *is injective if there is an* $R-$*module homomorphism* $h : B \longrightarrow I$ *such that* $hg = f$.

We will now investigate some of the consequences of these definitions in tandem.

Theorem 6.6.3. *Every (unitary) free module over* R *is projective.*

Proof. Consider the following diagram



Let F be free on the set X (and we will denote the canonical injection from X into F by $\iota : X \hookrightarrow F$). Since g is onto, there is $a_i \in A$ such that $g(a_i) = f\iota(x_i)$ for all i. Therefore we have a function $f^* : X \longrightarrow A$ such that $f^*(x_i) = a_i$. Since F is free, this induces an $R-$module homomorphism $h : F \longrightarrow A$ such that $h\iota(x_i) = a_i$. Therefore $gh\iota(x_i) = g(a_i) = f\iota(x_i)$ and hence $gh = f$. Hence F is projective. □

Definition 6.6.4. *Let D be an abelian group. We say that D is divisible if given $d \in D$ and $0 \neq n \in \mathbb{Z}$, there exists a $d' \in D$ such that $nd' = d$.*

Basically, in a divisible group we can divide by any nonzero integer.

Lemma 6.6.5. *D is divisible if and only if D is an injective $\mathbb{Z}-$module.*

Proof. ($\Longleftarrow$) Let D be injective and $d \in D$ and n be a nonzero integer. Consider the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \langle n \rangle & \xrightarrow{\subseteq} & \mathbb{Z} \\ & & {\scriptstyle f}\downarrow & \swarrow_{h} & \\ & & D & & \end{array}$$

Let $d' = h(1)$ and therefore $nd' = nh(1) = h(n) = f(n) = d$ and hence D is divisible.

The other direction is an exercise. □

Note that in the parallel results coming up many of the proofs are dual (in some places the proofs are more different).

Theorem 6.6.6. *The following conditions on the $R-$module P are equivalent.*

a) P is projective.

b) Every short exact sequence of the form $0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$ is split exact.

c) There is an $R-$module K and a free module F such that $F \cong P \oplus K$.

Theorem 6.6.7. *The following conditions on the $R-$module I are equivalent.*

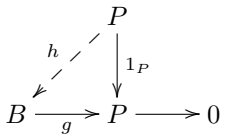
a) I is injective.

b) Every short exact sequence of the form $0 \longrightarrow I \longrightarrow B \longrightarrow C \longrightarrow 0$ is split exact.

c) I is a direct summand of any module of which it is a submodule.

Proof. We will provide a proof of the projective result. Try to do the injective one yourself.

For a) implies b) consider the short exact sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$. We now consider the diagram



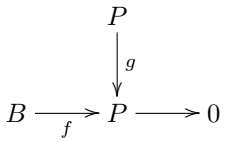
Since P is projective, there exists $h : P \longrightarrow B$ such that $gh = 1_P$, and hence the short exact sequence splits.

For b) implies c), we assume b) and assume that P is our given projective module. We know that any R module is the homomorphic image of a free module F (i.e. we have the onto map $F \xrightarrow{\phi} P \longrightarrow 0$. Hence we have the short exact sequence

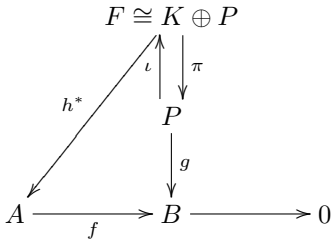
$$0 \longrightarrow \ker(\phi) \longrightarrow F \xrightarrow{\phi} P \longrightarrow 0.$$

Since the sequence must split, we have that $F \cong P \oplus \ker(\phi)$ and we have established b) implies c).

For the implication c) implies a) consider the following diagram.



Keeping in mind that there is a free module F with $F \cong K \oplus P$, we expand the diagram



where $\pi(k, p) = p$ and $\iota(p) = (0, p)$ (note $\pi\iota = 1_P$). Since any free module is projective there is an $h^* : F \longrightarrow A$ such that $fh^* = g\pi$. Now consider the map $P \longrightarrow A$ given by $h^*\iota$. Note that $f(h^*\iota) = g\pi\iota = g$ and hence P is projective. □

We note here the the proof of the dual injective theorem requires the result that will be recorded later that says that every $R-$module can be embedded in an injective $R-$module.

Corollary 6.6.8. *Let $\{P_i\}_{i\in I}$ be a family of $R-$modules. $\oplus_{i\in I} P_i$ is projective if and only if P_i is projective for all $i \in I$.*

Proof. If each P_i is projective, then for all i there is a Q_i such that $Q_i \oplus P_i$ is free. Hence we have the free module

$$\oplus_{i\in I}(P_i \oplus Q_i) \cong (\oplus_{i\in I} P_i) \oplus (\oplus_{i\in I} Q_i)$$

and hence the module $\oplus_{i\in I} P_i$ (being the summand of a free module) is projective.

On the other hand, assume that $\oplus_{i\in I} P_i \cong P_i \oplus (\oplus_{j\neq i} P_j$ is projective. So we can find an $R-$module K so that $K \oplus_{i\in I} P_i$ is free and hence $P_i \oplus (K \oplus (\oplus_{j\neq i} P_j))$ is free and hence P_i is projective. □

Corollary 6.6.9. *Let $\{I_j\}_{j\in\Gamma}$ be a family of $R-$modules. $\prod_{j\in\Gamma} I_j$ is injective if and only if I_j is injective for all $i \in \Gamma$.*

Proof. Very similar to the previous. Exercise. □

Corollary 6.6.10. *Every $R-$module is the homomorphic image of a projective $R-$module.*

Proof. Any free is projective. □

Theorem 6.6.11. *Every $R-$module M can be embedded in an injective $R-$module.*

Proof. Exercise. As a hint, first show that M (considered as an abelian group) can be embedded in a divisible abelian group D. Now embed M (as an $R-$module) in the $R-$module $\mathrm{Hom}_{\mathbb{Z}}(R, D)$. □

6.7 Hom

The notation $\mathrm{Hom}_R(A, B)$ will denote the set of $R-$module homomorphisms $f : A \longrightarrow B$. The is an abelian group under the standard addition (and note that the addition respects the standard function composition of $R-$module homomorphisms.

We consider $R-$module homomorphisms $\gamma : C \longrightarrow A$ and $\xi : B \longrightarrow D$. The map $\eta : \mathrm{Hom}_R(A, B) \longrightarrow \mathrm{Hom}_R(C, D)$ given by

$$f \mapsto \xi f \gamma$$

is an $R-$module homomorphism. We call this the homomorphism induced by ξ and γ. Note that if $B = D$ and $\xi = 1_D$, then the map is $f \mapsto f\gamma$ (denoted $\overline{\gamma}$). If $A = C$ and $\gamma = 1_A$ then the map is $f \mapsto \xi f$ (and is denoted $\overline{\xi}$). We will motly be considering these special cases.

Theorem 6.7.1. *Let R be a ring. The sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ is exact if and only if for all $R-$modules D the sequence*

$$0 \longrightarrow Hom_R(D, A) \xrightarrow{\overline{f}} Hom_R(D, B) \xrightarrow{\overline{g}} Hom_R(D, C)$$

is exact.

Additionally $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *is exact if and only if for every* $R-$*module* D *the sequence*

$$0 \longrightarrow Hom_R(C, D) \xrightarrow{\overline{g}} Hom_R(B, D) \xrightarrow{\overline{f}} Hom_R(A, D)$$

is exact.

We say that the "Hom functor" is left exact.

We will prove the first statement and leave the proof of the second as an exercise.

Proof. It would probably be helpful to see a diagram of how the induced maps on Hom actually "work". Suppose we have the exact sequence $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$. This sequence induces

$$0 \longrightarrow \mathrm{Hom}_R(C, D) \xrightarrow{\overline{g}} \mathrm{Hom}_R(B, D) \xrightarrow{\overline{f}} \mathrm{Hom}_R(A, D)$$

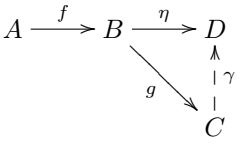
$$\gamma \longmapsto \gamma g$$

$$\eta \longmapsto \eta f$$

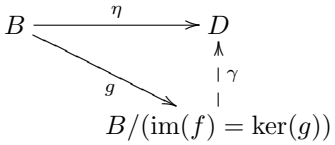
First we will show that $\overline{g}$ is one to one. Assume that γg is the $0-$map. So $\gamma g(b) = 0$ for all $b \in B$. But since g is onto, this means that for all $c \in C$ there exists a $b_c \in B$ such that $g(b_c) = c$. Hecn $\gamma(c) = 0$ for all $c \in C$ (that is γ is the $0-$map) and hence $\overline{g}$ is injective.

We now note that $\overline{f}\overline{g}(\gamma) = \overline{f}(\gamma g) = \gamma f g = 0$ as fg is the $0-$map. Hence we have that $\mathrm{im}(\overline{g}) \subseteq \ker(\overline{f})$. We now need to show the other containment.

Let $\eta \in \ker(\overline{f})$, that is, $\eta f = 0$. Consider the following diagram



basically we have to show the existence of a γ such that $\gamma g = \eta$. As g is onto, we have that $C \cong B/\ker(g) = B/\mathrm{im}(f)$. So we (need to) have



We define γ by $\gamma(b + \ker(g)) = \eta(b)$. Note if $b \in \ker(g) = \text{im}(f)$ then $\eta(b) = \eta f(a) = 0$ so this map is well-defined. It is also easy to verify that this is a homomorphism. Finally note that the diagram commutes since if $b \in B$ then $\gamma g(b) = \gamma(g(b) + \ker(g)) = \eta(b)$.

This shows that the exactness of the original sequence gives the exactness of the "Hom" sequence. The other direction is an exercise.

□

Example 6.7.2. *Hom the sequences of* $\mathbb{Z}-$*modules* $0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}_2 \longrightarrow 0$ *and* $0 \longrightarrow \mathbb{Z} \xrightarrow{incl} \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$.

We will see in the next thereom that split exact sequences are decidedly more well-behaved.

Theorem 6.7.3. *The following conditions on* $R-$*modules are equivalent.*

a) $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *is split exact.*

b) $0 \longrightarrow Hom_R(D, A) \xrightarrow{\overline{f}} Hom_R(D, B) \xrightarrow{\overline{g}} Hom_R(D, C) \longrightarrow 0$ *is split exact for every* D.

c) $0 \longrightarrow Hom_R(C, D) \xrightarrow{\overline{g}} Hom_R(B, D) \xrightarrow{\overline{f}} Hom_R(A, D) \longrightarrow 0$ *is split exact for every* D.

Proof. We will show the equivalence of a) and c), the other equivalence being left as an exercise.

For the implication a) implies b) if suffices to show that there is an $\overline{h}$ such that $\overline{g}\overline{h}$ is the identity on $\text{Hom}_R(D, C)$. Since the original sequence is split exact there exists $h : C \longrightarrow B$ such that $gh = 1_C$. It is easy to see that the induced homomorphism $\overline{gh} = \overline{g}\overline{h} = 1_{\text{Hom}_R(D,C)}$ hence $\overline{g}$ is onto and the Hom sequence is split exact.

On the other hand, assume that the Hom sequence is split exact for all D. Let $D = C$ and $\phi : C \longrightarrow B$ be such that $\overline{g}(\phi) = 1_C = g\phi$. Note that this implies that $0 \longrightarrow A \longrightarrow B \xrightarrow{g} C \longrightarrow 0$ is split exact. The equivalence of a) and c) is similar.

□

Theorem 6.7.4. *The following conditions on the* $R-$*module* P *are equivalent.*

a) P *is projective.*

b) If $\phi : B \longrightarrow C$ *is onto then* $\overline{\phi} : Hom_R(P, B) \longrightarrow Hom_R(P, C)$ *is onto.*

c) If $0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$ *is a short exact sequence then* $0 \longrightarrow Hom_R(P, A) \xrightarrow{\overline{\psi}} Hom_R(P, B) \xrightarrow{\overline{\phi}} Hom_R(P, C) \longrightarrow 0$ *is a short exact sequence.*

Theorem 6.7.5. *The following conditions on the $R-$module I are equivalent.*

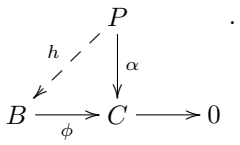
a) I is injective.

b) If $\xi : A \longrightarrow B$ is one to one then $\overline{\xi} : Hom_R(B, I) \longrightarrow Hom_R(A, I)$ is onto.

c) If $0 \longrightarrow A \xrightarrow{\xi} B \xrightarrow{\eta} C \longrightarrow 0$ is a short exact sequence then $0 \longrightarrow Hom_R(C, I) \xrightarrow{\overline{\eta}} Hom_R(B, I) \xrightarrow{\overline{\xi}} Hom_R(A, I) \longrightarrow 0$ is a short exact sequence.

We will prove the first "projective" result.

Proof. For a) implies b) we assume that P is projective and $\phi : B \longrightarrow C$ is onto and $\alpha \in \mathrm{Hom}_R(P, C)$. Consider the diagram



That is there is an h such that $\phi h = \alpha$ and hence $\overline{\phi}$ is onto.

For the implication b) implies a), given $\alpha \in \mathrm{Hom}_R(P, C)$ there exists $h \in \mathrm{Hom}_R(P, B)$ such that $\phi h = \alpha$ which is precisely what it means for P to be projective.

The implication b) implies c) is easy and so we will establish the converse. Suppose $\phi : B \longrightarrow C$ is onto and so we have the short exact sequence $0 \longrightarrow \ker(\phi) \longrightarrow B \longrightarrow C \longrightarrow 0$. This gives rise to the short exact sequence $0 \longrightarrow \mathrm{Hom}_R(P, \ker(\phi)) \longrightarrow \mathrm{Hom}_R(P, B) \longrightarrow \mathrm{Hom}_R(P, C) \longrightarrow 0$. Hence $\overline{\phi}$ is onto.

□

We conclude this section with a final functorial fact about Hom (the proof will be left as an exercise).

Theorem 6.7.6. *Let $A, B, \{A_i | i \in I\}, \{B_j | j \in J\}$ be $R-$modules. Then we have the following isomorphisms.*

a) $Hom_R(\oplus_{i \in I} A_i, B) \cong \prod_{i \in I} Hom_R(A_i, B)$.

b) $Hom_R(A, \prod_{j \in J} B_j) \cong \prod_{j \in J} Hom_R(A, B_j)$.

6.8 The Tensor Product

Although it can be done in much more generality, here we will (at least begin with) the tensor product of modules over a commutative ring with identity. The tensor product can be done in the more general case (but care must be taken using left, right, and bi-modules when necessary). The tensor product is a universal construction (it is the solution to a certain univeral mapping problem involving bilinear maps) and it crops up all over commutative algebra and mathematics in general (Einstein used them for example).

Definition 6.8.1. *Let A, B, C be $R-$ modules. A bilinear map $F : A \times B \longrightarrow C$ is a function such that for all $a, a_i \in A$, $b, b_i \in B$ and $r \in R$ we have*

a) $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$.

b) $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$.

c) $f(ra, b) = f(a, rb) = rf(a, b)$.

We now define the tensor product of two modules.

Definition 6.8.2. *Let A and B be modules over R and let F be the free abelian group on the set $A \times B$. Let K be the subgroup of F generated by all elements of the form*

a) $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$

b) $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$

c) $(ra, b) - (a, rb)$

where $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$ and $r \in R$.

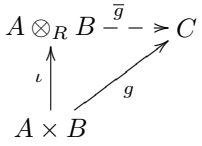
The quotient F/K is called the tensor product (over R) of A and B and is denoted $A \otimes_R B$.

We denote the coset $(a, b) + K$ by $a \otimes b$ (and this is called a tensor). Practically, think of $A \otimes_R B$ as generated by tensors of the form $a \otimes b$ subject the the relations a), b), and c) above.

We also point out that the map $\iota : A \times B \longrightarrow A \otimes_R B$ given by $(a, b) \mapsto a \otimes b$ is a bilinear map (verify this).

Here is a theorem which shows where tensor product "came from." This theorem shows that the tensor product is the unique solution to a mapping problem concerning bilinear maps.

Theorem 6.8.3. *If A, B, C are $R-$modules and $g : A \times B \longrightarrow C$ is a bilinear map then there exists a unique $R-$module homomorphism $\overline{g} : A \otimes_R B \longrightarrow C$ such that $\overline{g}\iota = g$ (where $\iota(a, b) = a \otimes b$ is the canonical bilinear map). $A \otimes_R B$ is uniquely determined up to isomorphism by this property.*



Proof. Let F be free abelian on $A \times B$ and K the subgroup described above. The map $g : A \times B \longrightarrow C$ is bilinear and induces a homomorphism $g^* : F \longrightarrow C$. The fact that g is bilinear shows that g^* takes every element of K to 0 (that is, $K \subseteq \ker(g^*)$). So g^* induces $\overline{g} : F/K \longrightarrow C$, that is $\overline{g} : A \otimes_R B \longrightarrow C$. Note that $\overline{g}\iota(a, b) = \overline{g}(a \otimes b) = g(a, b)$ and hence $\overline{g}\iota = g$.

Now if $h : A \otimes_R B \longrightarrow C$ is another such homomorphism then

$$h(a \otimes b) = g(a, b) = \overline{g}(a \otimes b)$$

and hence h and $\overline{g}$ agree on tensors. Therefore $h = \overline{g}$. □

Here is a useful corollary which we will be building upon.

Corollary 6.8.4. *Let A, A', B, B' be $R-$modules and $f : A \longrightarrow A'$ and $g : B \longrightarrow B'$ be $R-$module homomorphisms, then there exists a unique homomorphism*

$$A \otimes_R B \longrightarrow A' \otimes B'$$

such that $a \otimes b \mapsto f(a) \otimes g(b)$ for all $a \in A$ and $b \in B$.

Proof. One merely needs to verify that $(a, b) \mapsto (f(a) \otimes g(b))$ is a bilinear map. □

This next result is the "right exactness" of tensor product.

Theorem 6.8.5. *If D is an $R-$module then $- \otimes_R D$ is right exact. That is, if*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is exact, then so is

$$A \otimes_R D \xrightarrow{f \otimes 1_D} B \otimes_R D \xrightarrow{g \otimes 1_D} C \otimes_R D \longrightarrow 0$$

Proof. Since g is onto, every generator $c \otimes d$ of $C \otimes_R D$ is of the form $g(b) \otimes d = (g \otimes 1_D)(b \otimes d)$ and hence every generator of $C \otimes_R D$ is in the image of $g \otimes 1_D$. So $g \otimes 1_D$ is onto.

Now note that $(g \otimes 1_D)((f \otimes 1_D)(\sum_{i=1}^n (a_i \otimes d_i))) = (g \otimes 1_D)(\sum_{i=1}^n (f(a_i) \otimes d_i) = \sum_{i=1}^n (gf(a_i) \otimes d_i)$. Since $gf = 0$, we have that this is a sum of zeros and hence $\text{im}(f \otimes 1_D) \subseteq \ker(g \otimes 1_D)$.

For the last bit, we have to show that $\ker(g \otimes 1_D) \subseteq \text{im}(f \otimes 1_D)$. To this end we consider

$$\pi : B \otimes_R D \longrightarrow (B \otimes_R D)/(\text{im}(f \otimes 1_D)$$

and we note that there exists a homomorphism $\xi : (B \otimes_R D)/(\text{im}(f \otimes 1_D) \longrightarrow C \otimes_R D$ such that $\xi(\pi(b \otimes d)) = (g \otimes 1_D)(b \otimes d) = g(b) \otimes d$. It suffices to show that ξ is an isomorphism.

Consider $\eta : C \times D \longrightarrow (B \otimes_R D)/(\text{im}(f \otimes 1_D)$ given by $(c, d) \mapsto \pi(b \otimes d)$ where $g(b) = c$. (Note if $g(b_1) = c$ then $g(b - b_1) = 0$ and there is an $a \in A$ such that $f(a) = b - b_1$; since $f(a) \otimes d \in \text{im}(f \otimes 1_D$, $\pi(f(a) \otimes d) = 0$ and hence $\pi(b \otimes d) = \pi((f(a) + b_1) \otimes d) = \pi(b_1 \otimes d)$ and so the map is well-defined). It is easy to see that η is bilinear and so there exists a unique $\overline{eta} : C \otimes_R D \longrightarrow (B \otimes_R D)/\text{im}(f \otimes 1_D)$ such that $\overline{\eta}(c \otimes d) = \pi(b \otimes d)$. Hence given any generator $c \times d$, we have

$$\xi\overline{\eta}(c \otimes d) = \xi(\pi(b \otimes d)) = g(b) \otimes d = c \otimes d$$

and hence $\xi\overline{\eta}$ is the identity. In a similar fashion $\overline{\eta}\xi$ is the identity and the proof is complete.

□

Theorem 6.8.6. *There is an $R-$module isomorphism*

$$A \otimes_R R \cong A.$$

Proof. The assignment $(a, r) = ra$ is a bilinear map and so we obtain the $R-$module homomorphism $f : A \otimes_R R \longrightarrow A$ with $f(a \otimes r) = ra$. We now consider the $R-$module homomorphism $g : A \longrightarrow A \otimes_R R$ given by $g(a) = a \otimes 1$. Note that $gf = 1_{A \otimes_R R}$ and $fg = 1_A$, and hence f is an isomorphism. □

Other properties such as (adjoint) associativity will be discussed in exercises. We end with a couple of theorems concerning the behavior of tensor product with free modules.

Theorem 6.8.7. *Let A, A_i, B, B_j be $R-$modules. Then there are isomorphisms*

a) $(\oplus_{i \in I} A_i) \otimes_R B \cong \oplus_{i \in I}(A_i \otimes_R B)$.

b) $A \otimes_R (\oplus_{j \in J} B_j) \cong \oplus_{j \in J}(A \otimes_R B_j)$.

Proof. For a) consider the bilinear map $(\{a_i\}, b) \mapsto \{a_i \otimes b\}$ (note that almost every $a_i = 0$). Show this induces the relevant isomorphism. The proof for b) is simliar. □

Corollary 6.8.8. *Let F be a free $R-$module then*

$$F \otimes_R B \cong \oplus i \in IB$$

where $|I| = rank(F)$.

Proof. Note that $F \otimes_R B \cong (\oplus_{i \in I} R) \otimes_R B \cong \oplus_{i \in I}(R \otimes_R B) \cong \oplus_{i \in I} B$. □

6.9 Flatness

Flatness is a certain generalization of freeness (and projectivity). A flat module is a module that makes tensoring exact. More precisely, we have the following definition.

Definition 6.9.1. *We say that the $R-$module M is flat if given any short exact sequence*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

the corresponding sequence

$$0 \longrightarrow A \otimes_R M \xrightarrow{f \otimes 1_M} B \otimes_R M \xrightarrow{g \otimes 1_M} C \otimes_R M \longrightarrow 0$$

is exact.

We note that since tensoring gets you "most" of the exact sequence for free anyway, an equivalent characterization of a flat module M is one for which given any one to one map $f : A \longrightarrow B$, the corresponding map $f \otimes 1_M : A \otimes_R M \longrightarrow B \otimes_R M$ is one to one.

Here is a theorem that we record to show the pecking order.

Theorem 6.9.2. *Let M be an $R-$module. For the following list of properties, we have the implications a) $\Longrightarrow$ b) $\Longrightarrow$ c).*

a) M is free.

b) M is projective.

c) M is flat.

We leave the proof of the previous result and the next corollary as exercises.

Corollary 6.9.3. *Let M_i be a family of $R-$modules. $\oplus_{i \in I} M_i$ is flat if and only if M_i is flat for each i.*

Chapter 7

Modules over a PID and the Canonical Forms

7.1 Structure of finitely generated modules over a PID

In this section, R will be commutative with 1 (if not a PID) and all modules are unitary.

Theorem 7.1.1. *Let A be an $R-$module where R is an integral domain, $a \in A$ and $\mathfrak{O}_a = \{r \in R | ra = 0\}$.*

a) $\mathfrak{O}_a$ is an ideal of R.

b) $A_t = \{a \in A | \mathfrak{O}_a \neq 0\}$ is a submodule of A.

c) $R/\mathfrak{O}_a \cong Ra$.

And if R is a PID and $p \in R$ is a nonzero prime.

d) If $p^i a = 0$ (that is, $(p^i) \subseteq \mathfrak{O}_a$) then $\mathfrak{O}_a = (p^j)$ for some $0 \leq j \leq i$.

e) If $\mathfrak{O}_a = (p^i)$ then $p^j \neq 0$ for all $j < i$.

Theorem 7.1.2. *Let F be a free module over a PID and M a submodule of F. Then M is free and rank$(M) \leq$ rank(F).*

Corollary 7.1.3. *Let R be a PID and A an $n-$generated $R-$module. Then any submodule of A may be generated with $m \leq n$ elements.*

Corollary 7.1.4. *Let P be a module over a PID. Then P is projective if and only if P is free.*

Theorem 7.1.5. *Any finitely generated torsion free module over a PID is free.*

Proof. Let $X = \{x_1, x_2, \cdots, x_n\}$ be a finite set of generators of our module A. Since A is torsion free, each x_i is a singleton linearly independent subset of A. Let $\{x_1, x_2, \cdots, x_k\}$ (after reordering perhaps) be a maximal linearly independent subset of A. So $F = \langle x_1, x_2, \cdots, x_k \rangle$ is a free submodule of A. If $F = A$ then we can go to the house. So we will suppose that $x_j \notin F$ for all $k+1 \leq j \leq n$. Note for all $k+1 \leq j \leq n$ there is an $r_j \in R$ such that $r_j x_j = \sum_{i=1}^{n} r_{j,i} x_i$ (and note that $r_j \neq 0$).

Let $r = \prod_{j=k+1}^{n} r_j$ and note that $rX \subseteq F$. So we have that $rA \subseteq F$. We now have the map

$$\phi : A \longrightarrow F$$

given by $\phi(a) = ra$. This map is 1-1 and hence A is isomorphic to a submodule of a free module and is free. □

Corollary 7.1.6. *Let A be a finitely generated module over a PID, then*

$$A \cong F \oplus A_t$$

where A_t is torsion and finitely generated, F is free of finite rank and $F \cong A/A_t$.

So at this point it is clear that all we have to do is to understand how the "torsion part" works.

Here is a general theorem.

Theorem 7.1.7. *Let A be a torsion module over a PID, R, and let $p \in R$ a nonzero prime and $A_p = \{a \in A | p^k a = 0 \text{ for some } k\}$. Then $A \cong \sum_{p:prime} A_p$ and if A is finitely generated then $A_p = 0$ almost everywhere.*

Theorem 7.1.8. *Every finitely generated torsion module, M, over a PID can be written as $\oplus_{i=1}^{k} M_i$ where each M_i is cyclic and $p_i^{n_i}$ annihilates M_i (that is $M_i \cong R/p_i^{n_i}$).*

Next we have the big structure theorem.

Theorem 7.1.9. *Let A be a finitely generated module over a PID, R.*

a) A is the direct sum of a free module of finite rank and a finite number of cyclic torsion modules. These cyclic torsion summands (if any) are isomorphic to R/t_iR where the t_i's are nonzero nonunits of R with $t_1 | t_2 | \cdots | t_n$ (these t_i's are called the invariant factors). The free modules and the list of invariant factors are uniquesly determined by A.

b) The torsion part of A is a direct sum of cyclic torsion modules each isomorphic to $R/p_i^{s_i}R$ (with each p_i a prime of R). The list of primes $\{p_1, \cdots, p_k\}$ and exponents $\{s_1, \cdots, s_k\}$ are uniquely determined by A (the elements $\{p_i^{s_i}$ are called elementary divisors).

7.2 Decomposition of a Linear Transformation (the Canonical Forms)

Definition 7.2.1. *We say that two matrices, A and B, over a field are similar if there is an invertible matrix P such that $P^{-1}AP = B$.*

Note that similarity is an equivalence relation. Two matrices that are equivalent share many important invariants (eigenvalues etc.). Similar matrices can be viewed as essentially the same linear transormation after a change of basis.

Theorem 7.2.2. *Let E be an $n-$dimensional vector space over the field K, $\phi : E \longrightarrow E$ a linear transformation and A an $n \times n$ matrix over K.*

a) There is a unique monic polynomial $q_\phi \in K[x]$ such that $q_\phi(\phi) = 0$ and $q_\phi | f$ for all $f \in K[x]$ such that $f(\phi) = 0$.

b) There is a unique monic polynomial $q_A \in K[x]$ such that $q_A(A) = 0$ and $q_A | f$ for all $f \in K[x]$ such that $f(A) = 0$.

c) If A is the matrix of ϕ relate to some basis of E then $q_A = q_\phi$.

We first remark that $K[x]$ is an infinite dimensional $K-$vector space whereas $M_n(K)$ and $\mathrm{Hom}(E, E)$ are both finite dimensional $K-$vector spaces.

Proof. We will show a) leaving the rest as exercises.

Consider the map $\xi_\phi : K[x] \longrightarrow \mathrm{Hom}_K(E, E)$ given by $\xi_\phi(f) = f(\phi)$. Since $\mathrm{Hom}_K(E, E)$ is finite dimensional, $\ker(\xi_\phi) \neq 0$. So $\ker(\xi_\phi) = (p)$ where $p \in K[x]$. Choose a monic generator q_ϕ of (p) and this establishes a). □

At this stage, we remark that q_ϕ (q_A) is the minimal polynomial of ϕ (A). We also remark that ϕ induces a (left) $K[x]-$module structure on E. The action is given by (with $f \in K[x]$ and $e \in E$)

$$f \circ e = f(\phi)(e).$$

A $K-$subspace $F \subseteq E$ is said to be $\phi-$invariant if $\phi(F) \subseteq F$ (equivalently, F is a $K[x]-$submodule of E).

Given $v \in E$, the subspace spanned by $\{\phi^i(v) | i \geq 0\}$ is $\phi-$invariant. We call this space, $E(v, \phi)$, a $\phi-$cyclic subspace of E.

Theorem 7.2.3. *Let $\phi : E \longrightarrow E$ be a linear transformation of a finite dimensional vector space E over K.*

a) There are monic polynomials $q_1, q_2, \cdots, q_t \in K[x]$ and $\phi-$cyclic subspaces $E_1, \cdots, E_t$ of E such that $E = E_1 \oplus \cdots \oplus E_t$ and $q_1 | q_2 | \cdots | q_t$. Furthermore q_i is the minimal polynomial of $\phi | E_i : E_i \longrightarrow E_i$. The sequence $(q_1, q_2, \cdots q_t)$ is uniquely determined by E and ϕ and the minimal polynomial of ϕ is q_t.

b) There exist monic irreducible polynomials $p_1, \cdots, p_s \in K[x]$ *and* $\phi-$*cyclic subspaces* $E_{1,1}, \cdots, E_{1,k_1}, E_{2,1}, \cdots, E_{2,k_2}, E_{3,1}, \cdots, E_{s,k_s}$ *of* E *such that* E *is the direct sum of these subspaces and for each* i *there is a nonincreasing sequence of integers* $m_{i,1}$

Chapter 8

Fields and Galois Theory

8.1 Field Extensions and Basic Concepts

We have seen fields before as a special (very nice) case of commutative rings with identity. A field is a ring whose nonzero elements form an abelian group under multiplication.

Definition 8.1.1. *A field, F, is a commutative ring with identity such that* (0) *is a maximal ideal.*

The above definition means (as was stated before) that a field is a domain in which every nonzero element has an inverse. Any field contains 1_F and at this juncture there are two important cases to consider. The first case is where $n1_F \neq 0$ for any nonzero $n \in \mathbb{Z}$. In this case we say that the characteristic of the field is 0 (and note that such a field must contain the rational numbers $\mathbb{Q}$.

The other case to consider is when there exists a nonzero integer n such that $n1_F = 0$. Since our field is a domain, it is easy to see that the minimal positive such n must be prime in $\mathbb{Z}$ and in this case we say that the characteristic of F is p ($\text{char}(F) = p$). In this case F muct contain $\mathbb{Z}_p$.

In these two cases we say that the prime subfield of F (the intersection of all subfields of F) is $\mathbb{Q}$ (if $\text{char}(F) = 0$) or $\mathbb{Z}_p$ (if $\text{char}(F) = p$). We now go the other way and consider extensions of a field F.

Definition 8.1.2. *A field K is said to be an extension field of a field F if $F \subseteq K$. The dimension of K over F as a vector space is $[K : F]$. If E is a field such that $F \subseteq E \subseteq K$ then we call E an intermediate field.*

Theorem 8.1.3. *Let $F \subseteq E \subseteq K$ be fields, then $[K : F] = [K : E][E : F]$.*

Proof. Let $U = \{u_i | \in I\}$ be a basis of E over F and $V = \{v_j | j \in J\}$ a basis of K over E. It will suffice to show that the set $X = \{u_i v_j | i \in I, j \in J\}$ is a basis for K over F. To see that X spans K over F, first write an arbitrary $k \in K$ as

$$k = e_1 v_1 + e_2 v_2 + \cdots + e_n v_n$$

with $v_i \in V$ and each $e_i \in E$. Since each e_i is in E we can write

$$e_i = a_{i,1}u_1 + e_{i,2}u_2 + \cdots + e_{i,m}u_m$$

with each $a_{i,k} \in F$ and $u_j \in U$. Substituting we get that

$$k = e_1v_1+e_2v_2+\cdots+e_nv_n = (a_{1,1}u_1+e_{1,2}u_2+\cdots+e_{1,m}u_m)v_1+\cdots+(a_{n,1}u_1+e_{n,2}u_2+\cdots+e_{n,m}u_m)v_n$$

and so the set X spans K over F.

To see that X is linearly independent, assume that $\sum_{i,j} r_{i,j}u_iv_j = 0$. We rewrite this sum as

$$0 = \sum_{i,j} r_{i,j}u_iv_j = \sum_i = \sum_j (\sum_i r_{i,j}u_i)v_j$$

since the v_j's are linearly independent over E, this means that (for all j) each $\sum_i r_{i,j}u_i = 0$, but the u_i's are linearly independent over F and hence for all i, j, $r_{i,j} = 0$. This completes the proof.

□

We now introduce some terminology. If $X \subseteq F$ is a subset of the field F, then the subfield of F generated by X is the intersection of all subfields of F that contain X. In the case where X is finite (say $X = \{a_1, \cdots, a_n\}$), and K is a subfield of F then $K[a_1, \cdots, a_n]$ (respectively, $K(a_1, \cdots, a_n]$)) is the set of all $f(a_1, \cdots, a_n)$ where f is a polynomial (respectively, rational function) in n variables over K. This can be extended to the case where $|X| = \infty$. If $n = 1$ the extension the extension $K(a)$ is called a simple extension of K. Finally if L and M are subfields of F then the composite of L and M is the subfield generated by $L \bigcup M$ and is denoted LM.

Definition 8.1.4. *Let $K \subseteq F$ be fields and let $u \in F$. We say that u is algebraic over K if u is a root of some nonzero polynomial over K. If u is not algebraic, we say that u is transcendental over K. If every element of F is algebraic over K, we say that F is an algebraic extension of K. If F contains at least one transcendatal element, we say that F is transcendental over K.*

Example 8.1.5. *Any field is algebraic over itself. $\mathbb{R}$ is trancendental over $\mathbb{Q}$, but $\mathbb{C}$ is algebraic over $\mathbb{R}$. If x is an indeterminate and K is a field, then $K(x)$ is transcendental over K.*

Theorem 8.1.6. *If $K \subseteq F$ and $u \in F$ is transcendental over K then $K(u) \overset{\phi}{\cong} K(x)$ where ϕ is the identity on K.*

Proof. Since any element of $K(x)$ can be written as $\frac{f(x)}{g(x)}$ with $f(x), g(x) \in K[x]$, we consider the map $\phi : K(x) \longrightarrow K(u)$ given by

$$\phi(\frac{f(x)}{g(x)}) = \frac{f(u)}{g(u)}.$$

We first note that ϕ is indeed the identity on K. Additionally, we should worry a bit the denominator in the image. But note that if $g(u) = 0$ then (since u is transcendental over K) $g(x)$ must be the zero polynomial which is a contradiction. It is also clear that ϕ is onto. For one to oneness, note that if $\frac{f(u)}{g(u)} = 0$ then (again, since u is transcendental) that $f(x) = 0$ and we have injectivity. □

Here are some results that deal with algebraic extensions.

Theorem 8.1.7. *Let $K \subseteq F$ and $u \in F$ algebraic over K, then*

a) $K(u) \cong K[u]$.

b) $K(u) \cong K[x]/(f)$ *where $f(x)$ is the minimal (irreducible) polynomial (of degree n) in $K[x]$ such that $f(u) = 0$.*

c) $[K(u) : K] = deg(f) = n$.

d) Every element of $K(u)$ can be written uniquely in the form $\sum_{i=o}^{n-1} k_i u^i$ with $k_i \in K$ where $n = deg(f)$.

Proof. We begin with a). Note that $K[u] \subseteq K(u)$ so we only have to show the other containment. To this end it suffices to show that $K[u]$ is a field (since $K(u)$ is the quotient field of $K[u]$, if $K[u]$ is a field then we have equality). Let $I = \{g(x) \in K[x] | g(u) = 0\}$. It is easy to see that I is a nonzero (since u is algebraic) ideal of $K[x]$. Since $K[x]$ is a PID, I is generated by an irreducible polynomial $f(x) \in K[x]$; that is, $I = (f(x))$. Consider the map

$$\phi : K[x] \longrightarrow K[u]$$

given by $\phi(k(x)) = k(u)$. This map is a surjective ring homomorphism with kernel I and hence induces an isomorphism

$$K[x]/I \cong K[u].$$

Since I is generated by an irreducible (prime, since $K[x]$ is a PID) polynomial $K[x]/I$ is an integral domain. But more is true. Since I is a nonzero prime ideal and $K[x]$ is a PID, I must be maximal and hence $K[x]/I \cong K[u]$ is a field, and hence a) is established.

Part b) is a shameless rip-off of a). We already know that $K[u] \cong K[x]/(f)$ from the proof of part a), but also from part a) we have that $K(u) \cong K[u]$.

Part c) follows from part d) and so we will show part d). Of course any element of $K(u) \cong K[u]$ can be written as a $K-$linear combination of powers of u. It suffices to show that the set $S := \{1, u, u^2, \cdots, u^{n-1}\}$ is a basis of $K[u]$ over K. We first claim that any power of u is a $K-$linear combination of elements of S (note that this is clear for the first $n-1$ powers of u). we show by induction on k that u^{n+k} is a $K-$linear combination of elements of S.

Let $f(x) = k_n x^n + \cdots + k_1 x + k_0$ with $k_n \neq 0$. Note that since $f(u) = 0$ we have that

$$u^n = -\frac{k_{n-1}}{k_n}u^{n-1} + \cdots - \frac{k_1}{k_n}u - \frac{k_0}{k_n}$$

and hence u_n is generated by S over K.

Assume that the statement is true for k and consider u^{n+k+1}. Note that $u^{n+k+1} = u(u^{n+k})$ and by induction $u^{n+k} = \sum_{i=0}^{n-1} a_i u^i$ with $a_i \in K$. This gives

$$u(u^{n+k}) = u(\sum_{i=0}^{n-1} a_i u^i) = \sum_{i=0}^{n-1} a_i u^{i+1} = a_{n-1}u^n + \sum_{i=0}^{n-2} a_i u^i.$$

Replacing u^n by $-\frac{k_{n-1}}{k_n}u^{n-1} + \cdots - \frac{k_1}{k_n}u - \frac{k_0}{k_n}$, we obtain

$$u(u^{n+k}) = -\frac{k_{n-1}}{k_n}u^{n-1} + \cdots - \frac{k_1}{k_n}u - \frac{k_0}{k_n} + \sum_{i=0}^{n-2} a_i u^i$$

which is a $K-$linear combination of elements of S and our induction is complete.

To finish off the proof, we note that the previous argument shows that $K[u]$ is spanned by the set S. For linear independence, assume that we have the relation

$$a_0 + a_1 u + \cdots + a_{n-1}u^{n-1} = 0$$

with each $a_i \in K$. This implies that u is a root of the polynomial $g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in K[x]$. But our $f(x)$ of degree n was the minimal nonzero polynomial for u and hence $g(x) = 0$. So $a_i = 0$ for $0 \leq i \leq n-1$ and the proof is complete. □

Here is an interesting example.

Example 8.1.8. *Let u be the real root of the polynomial $x^5 - 2$ over the rationals. Consider the field $\mathbb{Q}(u)$. This field is of degree 5. Now consider one of the complex roots (say z) of the polynomial $x^5 - 2$. The content of the previous theorem shows that $\mathbb{Q}(z) \cong \mathbb{Q}(u)$, but it is interesting to note that $\mathbb{Q}(u)$ is a subfield of $\mathbb{R}$ and $\mathbb{Q}(z)$ is not.*

Theorem 8.1.9. *Let $\xi : K \longrightarrow L$ be an isomorphism of fields, u in some extension field of K and v in some extension field of L. Then ξ extends to an isomorphism $K(u) \cong L(v)$ taking u to v if and only if one of the following holds.*

a) u is transcendental over K and v is trancendental over L.

b) u is a root of $f \in K[x]$ and v is a root of $\xi(f) \in L[x]$.

Proof. In any case, note that ξ can be extended to $\xi^* : K(x) \cong L(x)$ (where ξ^* takes x to x). If the first condition holds then $K(u) \cong K(x) \cong L(x) \cong L(v)$ and the composite isomorphism takes u to v.

If the second condition holds, it is easy to see that the composite isomorphism

$$K(u) \longrightarrow K[x]/(f) \xrightarrow{\xi^*} L[x]/\xi(f) \longrightarrow L(v)$$

takes u to v.

The necessity of the conditions is an exercise.

□

It is worth noting that if u and v are roots of $f(x) \in K[x]$ where $f(x)$ is irreducible, then $K(u) \cong K(v)$.

Example 8.1.10. *Let α be the real cube root of 2 and $\omega = \frac{-1+\sqrt{-3}}{2}$ be the primitive 3^{rd} root of unity ($\omega^2 + \omega + 1 = 0$). The fields $\mathbb{Q}(\alpha), \mathbb{Q}(\omega\alpha)$, and $\mathbb{Q}(\omega^2\alpha)$ are distinct, but isomorphic. Additionally, the intersection of the fields is $\mathbb{Q}$.*

Theorem 8.1.11. *Let K be a field and $f \in K[x]$ a polynomial of degree n. Then there is a simple extension field $F = K(u)$ such that the following hold.*

a) There exists $u \in F$ such that $f(u) = 0$.

b) $[K(u) : K] \leq n$ and equality holds if and only if f is irreducible in $K[x]$.

c) If f is irreducible in $K[x]$ then $K(u)$ is unique up to $K-$isomorphism (and $K(u)$ is called the field obtained by adjoining a root of f to K).

Proof. Suppose that in $K[x]$ we can factor $f(x)$ as

$$f(x) = p_1(x) \cdots p_m(x)$$

where each $p_i(x) \in K[x]$ is irreducible of degree at least 1. Consider the field $K[x]/(p_1(x))$ (note that this is a field since $p_1(x)$ is a nonzero prime and $K[x]$ is a PID).

The canonical injection $K \longrightarrow K[x]/(p_1(x))$ given by $k \mapsto k + (p_1(x))$ shows that K is a subfield of $K[x]/(p_1(x))$. To find our root u that was claimed to exist in part a) we consider the epimorphism

$$\pi : K[x] \longrightarrow K[x]/(p_1(x))$$

given by $g(x) \mapsto g(x) + (p_1(x))K[x]$. Note that $\pi(p_1(x)) = 0 = p_1(\pi(x))$ and so $u := \pi(x)$ is an element of $F = K[x]/(p_1(x))$ such that $p_1(u) = 0$. Since $p_1(x)$ divides $f(x)$, u is a root of $f(x)$ as well.

For part b) we see that $[K(u) : K] = \deg(p_1(x)) \leq \deg(f) = n$. If f is irreducible, we see that $p_1 = f$ and hence we have equality. On the other hand, if we have equality, we see that $\deg(p_1) = \deg(f)$ and since p_1 divides f we have equality and hence f is irreducible. The proof of c) is an exercise. □

The following theorem shows that "small" field extensions behave nicely.

Theorem 8.1.12. *Let $K \subseteq F$ be finite-dimensional, then F is finitely-generated and algebraic over K.*

Proof. Let $u \in F$ and let $[F : K] = n$. This implies that the set $\{1, u, u^2, \cdots, u^n\}$ is linearly dependent over K. Hence

$$u^n = \sum_{i=0}^{n-1} k_i u^i$$

and hence u is algebraic over K. Also note that if $\{a_1, a_2, \cdots, a_n\}$ is a basis of F over K, then $F = K(a_1, a_2, \cdots, a_n)$ and hence F is finitely-generated over K. □

The next result shows that the property "algebraic" is transitive. It is also quite useful in that it will help to show that algebraic elements are closed under the standard operations (and hence algebraic elements tend to form fields).

Theorem 8.1.13. *If F is algebraic over E and E is algebraic over K, then F is algebraic over K.*

Proof. Let $u \in F$. Since u is algebraic over E, we have that

$$e_n u^n + e_{n-1} u^{n-1} + \cdots + e_1 u + e_0 = 0$$

for some (not all zero) $e_i \in E$. Note that the equation above actually shows that u is algebraic over $K(e_n, \cdots, e_1, e_0)$. Consider the tower of fields

$$K \subseteq\subseteq K(e_0) \subseteq K(e_0, e_1) \subseteq K(e_0, e_1, \cdots, e_n) \subseteq K(e_0, e_1, \cdots, e_n)(u).$$

Note that every extension above is finite-dimensional and hence the extension $K(e_0, \cdots, e_n)(u)$ is finite diemsional over K. Hence u is algebraic over K. □

Corollary 8.1.14. *Let α, β be algebraic over K. Then $\alpha + \beta, \alpha\beta$, and $\frac{alpha}{\beta}$ (if $\beta \neq 0$) are algebraic over K. In particular, if F is an extension field of K then the set of all elements of F which are algebraic over K is a subfield of F containing K.*

Proof. Consider the tower of fields

$$K \subseteq K(\alpha) \subseteq K(\alpha, \beta).$$

Since $K(\alpha)$ is algebraic over K and $K(\alpha, \beta)$ is algebraic over $K(\alpha)$, the previous theorem, shows that $K(\alpha, \beta)$ is algebraic over K. In particular, $\alpha + \beta, \alpha\beta$, and $\frac{\alpha}{\beta}$ (if $\beta \neq 0$) are all algebraic over K. □

8.2 The Fundamental Theorem of Galois Theory

In this section, we will see the biggie, but it ain't so bad and is totally cool.

We begin with some set-up. Let E and F be field extensions of K. We will call $\sigma : E \longrightarrow F$ a $K-$homomorphism (resp. $K-$automorphism) if σ is a $K-$module homomorphism (resp. automorphism) and a field homomorphism (resp. automorphism).

The group of all $K-$automorphisms of F is called the Galois group of F over K and is denoted $\mathrm{Gal}(F/K) = \mathrm{Aut}(F/K) = G(F/K)$.

Example 8.2.1. *Let $F = \mathbb{Q}(\sqrt{d})$ where d is a square free integer. Then $Gal(F/K) \cong \mathbb{Z}_2$.*

The next example contains almost all of the pieces of (finite) Galois theory.

Example 8.2.2. *Let α be the real cube root of 2 and ω the primitive 3^{rd} root of 1 ($\omega = \frac{-1+\sqrt{-3}}{2}; \omega^2 + \omega + 1 = 0$). Let $F = \mathbb{Q}(\alpha, \omega)$ be the (smallest) field extension of $\mathbb{Q}$ containing α and ω. It is worth noting this this is precisely the smallest field extension of the rationals where the polynomial $x^3 - 2$ has all of its roots.*

Verify that a basis of F over $\mathbb{Q}$ is given by $\{1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2\}$. Consider the following table

Automorphisms of F

	ϕ_{id}	$\phi_{(12)}$	$\phi_{(13)}$	$\phi_{(23)}$	$\phi_{(123)}$	$\phi_{(132)}$
1	*1*	*1*	*1*	*1*	*1*	*1*
α	α	$\omega\alpha$	$\omega^2\alpha$	α	$\omega\alpha$	$\omega^2\alpha$
α^2	α^2	$\omega^2\alpha^2$	$\omega\alpha^2$	α^2	$\omega^2\alpha^2$	$\omega\alpha^2$
ω	ω	ω^2	ω^2	ω^2	ω	ω
$\omega\alpha$	$\omega\alpha$	α	$\omega\alpha$	$\omega^2\alpha$	$\omega^2\alpha$	α
$\omega\alpha^2$	$\omega\alpha^2$	$\omega\alpha^2$	α^2	$\omega^2\alpha^2$	α^2	$\omega^2\alpha^2$

Note that each automophism ϕ induces a permutation of the roots of the polynomial $x^3 - 2$ (and since the action of ϕ on these roots completely determine the automorphism, there are at most 6). From the table above, we see that there are precisely 6 automorphisms (the most allowable by law here) and the Galois group is isomorphic to S_3. It is important to note that each permutation of the roots is reflected in the subscripting in the table (the roots $\alpha, \omega\alpha$, and $\omega^2\alpha$ are numbered 1,2,3 respectively and, for example, the automorphism ϕ_{12} is the one that interchanges roots 1 and 2 and fixes root 3). The reader is strongly encouraged to wangle and dink with the example above to get a feel for the interplay of permutations of roots and field automorphisms.

As a final addendum to the above example, note that if σ is a $K-$automorphism of F, and r is a root in F of $f(x) \in K[x]$, then $\sigma(r)$ is also a root of $f(x)$.

Example 8.2.3. *Compute $Gal(F/F)$, $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ and $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$.*

We now introduce the "prime" notation and some theorems that we will use in the fundamental theorem of Galois theory.

Theorem 8.2.4. *Let $K \subseteq E \subseteq F$ be fields and H a subgroup of $Gal(F/K)$.*

a) $H' = \{v \in F | \sigma(v) = v \text{ for all } \sigma \in H\}$ is an intermediate field of the extension $K \subseteq F$.

b) $E' = \{\sigma \in Gal(F/K) | \sigma(e) = e \text{ for all } e \in E\}$ is a subgroup of $Gal(F/K)$.

Proof. Exercise. □

We remark that H' is called the fixed field of H in F. Note that $1' = F$ but it is not necessarily true that $\mathrm{Gal}(F/K)' = K$ (for an example of this, consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$).

Definition 8.2.5. *Let $K \subseteq F$ be fields. We say that F is Galois over K if the fixed field of $Gal(F/K)$ is K. Equivalently, F is Galois over K if for all $\alpha \in F \setminus K$ there is a $\sigma \in Gal(F/K)$ such that $\sigma(\alpha) \neq \alpha$.*

We remark, that we will also see later that if $F = K(u)$ where u is a root of some $f \in K[x]$, then F is Galois over K if and only if F is seperable over K (which will be defined later) and *all* roots of f are in F.

Example 8.2.6. *Let $\omega = \frac{-1+\sqrt{-3}}{2}$ (the primitive cube root of unity) and $\alpha = \sqrt[3]{2}$. As it turns out, the intermediate fields of the extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \omega)$ are $\mathbb{Q}, \mathbb{Q}(\omega), \mathbb{Q}(\alpha), \mathbb{Q}(\omega\alpha), \mathbb{Q}(\omega^2\alpha)$, and $\mathbb{Q}(\alpha, \omega)$. The big one ($\mathbb{Q}(\alpha, \omega)$) is Galois over all the intermediate fields and $\mathbb{Q}(\omega)$ is Galois over $\mathbb{Q}$, but the other three are not Galois over $\mathbb{Q}$.*

We now state the fundamental theorem of Galois theory. After the statement of the theorem, most of the rest of the section will be devoted to developing needed but routine technical machinery and proving the theorem.

Theorem 8.2.7. *If $K \subseteq F$ is finite and Galois, then there is a one to one correspondence between the set of intermediate fields of the extension $K \subseteq F$ and the set of subgroups of $Gal(F/K)$ (given by $E \mapsto E' = Gal(E/K)$) such that the following hold.*

a) If $L \subseteq M$ are intermediate fields then $[M : L] = [L' : M']$ (in particular, $|Gal(F/K)| = [F : K]$).

b) F is Galois over ever intermediate field E, but E is Galois over K if and only if $Gal(F/E) \lhd Gal(F/K)$ and in this case $Gal(F/K)/Gal(F/E) \cong Gal(E/K)$.

It would be instructive here for the student to make a "schematic" diagram of the Galois correspondence.

Lemma 8.2.8. *Let $K \subseteq F$ be a Galois extension with intermediate fields L and M. Let $G = Gal(F/K)$ and let H and N be subgroups of G. The following conditions hold.*

a) $F' = 1$ and $K' = G$.

b) $1' = G$.

c) If $L \subseteq M$ *then* $M' \subseteq L'$.

d) If $H \subseteq N$ *then* $N' \subseteq H'$.

e) $L \subseteq L''$ *and* $H \subseteq H''$.

f) $L' = L'''$ *and* $H' = H'''$.

Proof. We leave a) and b) as exercises. For c) let $\sigma \in M'$. Then σ fixes all of M and since $L \subseteq M$, σ fixes all of L. Hence $\sigma \in L'$.

For d), suppose that $n \in N'$. Hence $\sigma(n) = n$ for all $\sigma \in N$. In particular, since $H \subseteq N$, we must have that $\sigma(n) = n$ for all $\sigma \in H$ and therefore $n \in H'$. We conclude that $N' \subseteq H'$.

For e), note that $L' = \{\sigma \in G | \sigma(l) = l \text{ for all } l \in L\}$ and $L'' = \{l \in F | \sigma(l) = l \text{ for all } \sigma \in L'\}$. So if $l \in L$ we have by the definitions above that $\sigma(l) = l$ for all $\sigma \in L'$ and hence $l \in L''$. The other statement from e) is a similar manipulation of the definitions.

Finally for f) Note that we have that $L \subseteq L''$ and so we apply primes and utilize part c) to obtain that $L' \supseteq L'''$. To get the other containment note that $(L') \subseteq (L')''$ by part e). The other statement is analogous and this concludes the proof. □

It should be noted here that F is Galois over K if and only if $K = K''$. More generally, F is Galois over an intermediate field E if and only if $E = E''$.

Here is a definition that serves to define an important class of intermediate extensions and an important class of subgroups of the Galois group.

Definition 8.2.9. *If* X *is a subgroup of the Galois group,* G *or an intermediate field of the extension* $K \subseteq F$ *we say that* X *is closed if* $X = X''$.

As a final remark, we note that the previous lemma gives a one to one correspondence between the *closed* subgroups of G and the *closed* subfields of F. This correspodence is given by $E \mapsto E' = \text{Gal}(F/E)$. So we have almost got the first statement of the fundamental theorem of Galois theory. Our strategy from here will be to show that if F is algebraic and Galois over K then all intermediate fields are closed and that if F is finite dimensional then all subgroups of the Galois group are closed.

Lemma 8.2.10. *Let* $K \subseteq L \subseteq M \subseteq F$ *be fields. If* $[M : L] < \infty$ *then* $[L' : M'] \leq [M : L]$. *In particular, if* $[F : K] < \infty$ *then* $|Gal(F/K)| \leq [F : K]$.

Proof. We will proceed by induction on $n = [M : L]$ (and note that the result is easy if $n = 1$). If $n > 1$ we will assume the conclusion for all $i < n$.

We now reduce the problem to a simpler case. Begin by selecting $u \in M \setminus L$. Since $[M : L] < \infty$ this implies that u is algebraic over L with irreducible polynomial $f \in L[x]$ of degree $k > 1$. Therefore $[L(u) : L] = k$ and $[M : L(u)] = \frac{n}{k}$. If $k < n$ (and so $1 < \frac{n}{k} < n$) then

$$[L' : M'] = [L' : (L(u))'][(L(u))' : M'] \leq \frac{n}{k}k = n$$

and hence the only case to worry is if $k = n$ (which means that $M = L(u)$). We will make this reduction and proceed.

To tackle this case, we will construct a one to one map from the set of left cosets of M' in L' (we will call this set of cosets S) to the set, T, of distinct roots of f in L (which is of cadinality no more than n).

Let $\tau M'$ be a coset of M' in L' and $\sigma \in \text{Gal}(F/M)$. Since $u \in M$, $\tau\sigma(u) = \tau(u)$. This means that every element of the coset $\tau M'$ has the same effect on u and takes u to $\tau(u)$. This is the spark that allows us to define our map.

We define the map $S \longrightarrow T$ by $\tau M' = \tau(u)$. By the above argument, this map is well-defined. To see that the map is one to one, consider that if $\tau(u) = \tau_0(u)$ then $\tau_0^{-1}\tau(u) = u$ and hence (since $M = L(u)$) we have that $\tau_0^{-1}\tau$ fixes all of M. So $\tau_0^{-1}\tau \in M'$ and $\tau_0 M' = \tau M'$. This shows that the map is one to one and completes the proof. □

Here is the analogous result for the behavior of the prime operation on subgroups of the Galois group.

Lemma 8.2.11. *Let $K \subseteq F$ be fields and $H \subseteq N \subseteq Gal(F/K)$. If $[J : H] < \infty$ then $[H' : J'] \leq [J : H]$.*

Proof. Many of the same ideas that worked in the previous proof are (can be) utilized here and the proof is left as an exercise. □

The next result ties together the previous lemmata and underscores our direction.

Lemma 8.2.12. *Let $K \subseteq L \subseteq M \subseteq F$ are fields and $H \subseteq J \subseteq Gal(F/K)$.*

a) If L is closed and $[M : L] < \infty$ then M is closed and $[L' : M'] = [M : L]$.

b) If H is closed and $[J : H] < \infty$ then J is closed and $[H' : J'] = [J : H]$.

c) If F is finite-dimensional and Galois over K then all intermediate fields and all subgroups of the Galois group are closed and $|Gal(F/K)| = [F : K]$.

We remark here that condition b) shows that all finite subgroups of $\text{Gal}(F/K)$ are closed (take $H = 1$ and J finite).

Proof. Exercise. □

At this point we have shown "most" of the fundamental theorem of Galois theory. To deal with the second statement, we will need a couple of definitions and results.

Definition 8.2.13. *Let $\sigma \in Gal(F/K)$ and let $K \subseteq E \subseteq F$. We say that:*

a) E is stable if $\sigma(E) \subseteq E$ for all $\sigma \in Gal(F/K)$.

b) $\tau \in Gal(E/K)$ is extendible to F if there is a $\sigma \in Gal(F/K)$ such that $sigma|_E = \tau$.

It should be noted in b) that E would be stable relative to this σ.

Lemma 8.2.14. *Let $K \subseteq E \subseteq F$ be fields*

a) If E is stable, then $E' = Gal(F/E) \lhd Gal(F/K)$.

b) If $H \lhd Gal(F/K)$ then H' is a stable intermediate extension.

Proof. For a), let $u \in E$, $\sigma \in \mathrm{Gal}(F/K)$ and $\xi \in \mathrm{Gal}(F/E)$. We wish to show that $sigma^{-1}\xi\sigma \in \mathrm{Gal}(F/E)$ (that is, for arbitrary $u \in E$, $\sigma^{-1}\xi\sigma(u) = u$). Since E is stable, $\sigma(u) \in E$ and therefore $\xi\sigma(u) = \sigma(u)$ and the result follows.

For part b), let $\sigma \in \mathrm{Gal}(F/K)$ and $v \in H'$. In this case, we wish to show that $\sigma(v) \in H'$; that is, for all $\xi \in H$, $\xi\sigma(v) = \sigma(v)$. Note that by the normality of H, we have that $\sigma^{-1}\xi\sigma \in H$ and hence $\sigma^{-1}\xi\sigma(v) = v$. Composing both sides with σ we get $\xi\sigma(v) = \sigma(v)$ as desired. □

Lemma 8.2.15. *If F is Galois over K and E is a stable intermediate extension, then E is Galois over K.*

Proof. Let $u \in E \setminus K$. Since F is Galois over K, then there is a $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma(u) \neq u$. Note that $\sigma|_E Gal(E/K)$ since E is stable. Since $\sigma|_E(u) \neq u$, we obtain that E is Galois over K. □

Lemma 8.2.16. *If $K \subseteq E \subseteq F$ are fields such that E is algebraic and Galois over K then E is stable.*

Proof. Let $u \in E$ and $f \in K[x]$ the minimal irreducible polynomial of u over K. We list the distinct roots of f in E:

$$u = u_1, u_2, \cdots, u_r$$

and note that $r \leq n\deg(f)$.

If $\xi \in \mathrm{Gal}(E/K)$ then ξ permutes the roots listed above which implies that the coefficients of the monic polynomial

$$g = (x - u_1)(x - u_2)\cdots(x - u_r)$$

are fixed by every $\xi \in \mathrm{Gal}(E/K)$. Since E is Galois over K, we have that $g \in K[x]$ and hence f divides g. Since f is irreducible, we must have that $f = g$ (up to a multiple from the field K). This implies that all of the roots of f are distinct and lie in E, hence $\sigma(u) \in E$. □

The proof of the previous result was rather important and will be used later. One should note that the assumption that E was Galois over K bought us that the roots of the polynomial f were all *distinct* and in E.

Here is the final tool that we will use in the Fundamental Theorem of Galois Theory.

Lemma 8.2.17. *Let $K \subseteq E \subseteq F$ be fields with E stable. Then $Gal(F/K)/Gal(F/E)$ is isomorphic to the group of $K-$automorphisms of E that are extendible to F.*

Proof. We define the map $f : \mathrm{Gal}(F/K) \longrightarrow \mathrm{Gal}(E/K)$ by $\sigma \mapsto \sigma|_E$. The image of this map is the subgroup of $\mathrm{Gal}(E/K)$ consisting of those automorphisms of E that are extendible to F. Observe that the kernal of this map is precisely $\mathrm{Gal}(F/E)$; apply the first isomorphism theorem. □

We close with some remarks to explain why this finishes our proof. If E is an intermediate field that is Galois over K (that is $E' \lhd \mathrm{Gal}(F/K)$). Since E and E' are closed and $G' = K$ ($G := \mathrm{Gal}(F/K)$), we have $|G/E'| = [G : E'] = [E'' : G'] = [E : K]$. What we have shown is that $G/E' = \mathrm{Gal}(F/K)/\mathrm{Gal}(F/E)$ is isomorphic to a subgroup of $\mathrm{Gal}(E/K)$ of order $[E : K]$. Hence $G/E' \cong \mathrm{Gal}(E/K)$.

Here is a more general statement to conclude this section.

Theorem 8.2.18. *Let F be a field, G a group of automorphisms of F and K the fixed field of G in F. Then F is Galois over K, and if G is finite, then F is a finite dimensional Galois extension of K with Galois group G.*

8.3 Splitting Fields and Algebraic Closures

we have already encountered the notion of an algebraic closure of a specific field. Indeed, the subset of the complex numbers $\mathbb{C}$ consisting of all $z \in \mathbb{C}$ such that z is algebraic over $\mathbb{Q}$ is a (countable) subfield of $\mathbb{C}$ and is an "algebraic closure" of $\mathbb{Q}$. This field has the property that every polynomial with coefficients in $\mathbb{Q}$ has a root in this field. Such a construction can be made for any field (not just $\mathbb{Q}$) and this section will outline this via splitting fields.

Definition 8.3.1. *Let $f \in F[x]$ be a polynomial of positive degree. We say that f splits in $F[x]$ if*

$$f = u(x - r_1)(x - r_2) \cdots (x - r_n)$$

with $r_i, u \in F$. We say that an extension field $F \subseteq F'$ is a splitting field for $f \in F[x]$ if f splits in $F'[x]$ and $F' = F(r_1, r_2, \cdots, r_n)$.

We make a couple of remarks here. Firstly, the splitting field of $f \in F[x]$ is a field where f splits into linear factors, but the condition $F' = F(r_1, r_2, \cdots, r_n)$ is a sort of "minimality" condition (that is, F' is the smalest field containing F where the polynomial f splits). We also note that we can define a splitting field for a set, S, of polynomials in an analogous fashion (and note if the set S is finite, then we can consider the set to be a single polynomial).

Theorem 8.3.2. *If K is a field and $f \in K[x]$ has degree $n \geq 1$, then there is a splitting field F of f such that $[F : K] \leq n!$.*

Proof. We proceed by induction on $n = \deg(f)$. The case $n = 1$ being quite easy, we will assume that if f has degree not exceeding $n - 1$ then there is a splitting field for f of degree no more than $(n - 1)!$.

Assume $\deg(f) = n$ and let g be an irreducible factor of f of degree more than 1 ($1 < \deg(g) \leq n$...note that if all irreducible factors of g are degree 1, then the result follows easily). If u is a root of g then we know that there is an extension $K(u)$ of K such that $[K(u) : K] = \deg(g) > 1$. Over the field $K(u)$ the polynomial f factors:

$$f = (x - u)h$$

where $h \in K(u)[x]$ is of degree $n - 1$. By induction, there is a splitting field F of h that contains $K(u)$ such that $[F : K(u)] \leq (n - 1)!$. Hence f splits in F and

$$[F : K] = [F : K(u)][K(u) : K] \leq (n - 1)!\deg(g) \leq n!$$

and this completes the proof. □

The next theorem (equivalent conditions) will be the result that we use to define "algebraically closed field". Intuitively, this is a field where all roots of polynomials are "already there" (or equivalently, every polynomial splits into linear factors).

Theorem 8.3.3. *Let F be a field. The following conditions are equivalent.*

a) Every nonconstant polynomial $f \in F[x]$ has a root in F.

b) Every nonconstant polynomial $f \in F[x]$ splits over F.

c) A nonconstant polynomial $f \in F[x]$ is irreducible if and only if $deg(f) = 1$.

d) There is no nontrivial algebraic extension field of F.

e) There is a field $K \subseteq F$ such that F is algebraic over K and every polynomial in $K[x]$ splits in $F[x]$.

Proof. Exercise. □

We remark here that if the extension $K \subseteq F$ is algebraic and F is algebraically closed, then F is the splitting field of the set of all polynomials in $K[x]$.

We now continue with some results concerning algebraic closures and splitting fields.

Theorem 8.3.4. *Every field K has an algebraic closure and any two algebraic closures of K are $K-$isomorphic.*

Proof. We leave most of this as an exercise. We remark that the uniqueness will follow from a theorem that we will see shortly. As a hint, to construct the algebraic closure of K, consider the splitting field of the set of all (nonconstant) polynomials in $K[x]$. □

We list the following as a corollary, but the excited reader could prove it first to derive the previous theorem.

Corollary 8.3.5. *If K is a field and S a set of polynomials in $K[x]$, then there is a splitting field of S over K.*

Chapter 9

Arithmetic Rings

9.1 Integral Closure

In this chapter, all rings are integral domains unless specifically stated otherwise. In this section we will delve into some of the structures that are on the boundary of commutative algebra and number theory. We first explore a central notion referred to as "integral closure."

Definition 9.1.1. *Let $R \subseteq T$ be a domains we say that $t \in T$ is integral over R if t is the root of a monic polynomial*

$$x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 \in R[x].$$

Example 9.1.2. *If R is a field, then t being integral is equivalent to t being algebraic.*

Example 9.1.3. *Consider the ring $\mathbb{Z}[\sqrt{-5}]$. Every element of this ring is integral over $\mathbb{Z}$.*

The previous two examples (and what we have done with fields) demands an answer to the question "do elements integral over R form a ring"? The answer to the question is yes and we will begin to develop this now.

Lemma 9.1.4. *Let $R \subseteq T$ be domains and $u \in T$. TFAE.*

a) u is integral over R.

b) There is a finitely-generated $R-$submodule of $A \subseteq T$ such that $uA \subseteq A$.

Proof. For the a) implies b) direction, suppose that u is a root of $x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 \in R[x]$. Take A to be the module generated by $\{1, u, \cdots, u^{n-1}\}$.

For the other direction, assume A is generated by $\{a_1, a_2, \cdots, a_n\}$. We obtain the system of equations

$$ua_i = \sum \lambda_{ij} a_j.$$

Bringing the right side to the left above, we get a matrix equation which has u as an eigenvalue. The equation is monic and hence u is integral. □

Theorem 9.1.5. *Let $R \subseteq T$ be domains. If $u, v \in T$ are integral over R, then so are $u + v$ and uv.*

Proof. Let A and B be finitely generated modules (as per the previous) such that $uA \subseteq A$ and $vB \subseteq B$. Note that AB is also finitely generated and note that $(u + v)AB \subseteq AB$ and $uvAB \subseteq AB$. □

Corollary 9.1.6. *If $R \subseteq T$ are domains then $\overline{R} = \{z \in T | z \text{ is integral over } R\}$ is a subring of T containing R.*

Proof. Follows directly from above. □

Definition 9.1.7. *Let $R \subseteq T$ be domains. We say that $\overline{R}_T = \{z \in T | z \text{ is integral over } R\}$ is the integral closure of R in T. If $\overline{R}_T = R$ then we say that R is integrally closed in T. If T is the quotient field of R and R is integrally closed in T then we say that R is integrally closed.*

Integrally closed rings are in general much nicer than their non-integrally closed counterparts. Here are some basic theorems (most without proof for now).

Theorem 9.1.8. *If R is integrally closed, then so is $R[x]$.*

Theorem 9.1.9. *Any UFD is integrally closed.*

Proof. Let $\omega = \frac{a}{b} \in \mathbb{Q}$ with a and b having no common prime factors. Suppose that ω is a root of the polynomial

$$x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 \in R[x].$$

Plugging in $\frac{a}{b}$ and normalizing we get

$$a^n + br_{n-1}a^{n-1} + \cdots + b^{n-1}r_1 a + b^n r_0 = 0.$$

Now suppose that p is a prime dividing b. It is easy to see that p divides a^n and hence a. This would contradict the "relative primeness" of a and b, and hence there are no primes dividing b. So b is a unit and $\omega \in R$. □

Here is a lemma that is sometimes useful for when working with integral elements.

Lemma 9.1.10. *Let $R \subseteq T$ be domains and $u \in U(T)$ (that is, u is a unit of T). Then u^{-1} is integral over R if and only if $u^{-1} \in R[u]$.*

Proof. If u^{-1} is integral over R then we have the equation

$$u^{-n} + r_{n-1}u^{-n+1} + \cdots + r_1 u^{-1} + r_0 = 0$$

with each $r_i \in R$. Multiply this sucker by u^n and rearrange to obtain

$$u(r_{n-1} + r_{n-2}u + \cdots + r_0 u^{n-1}) = -1$$

and we see that $u^{-1} \in R[u]$. The other direction is this in reverse. □

Lemma 9.1.11. *An arbitrary intersection of integrally closed domains is integrally closed.*

Proof. Let R_i be integrally closed for all i and let $R := \bigcap_i R_i$. Let ω be an element of the quotient field of R that is integral over R. Then ω is integral over each R_i and hence contained in each R_i. So $\omega \in R$. □

9.2 Valuation domains

In a certain sense valuation domains are the next best thing to fields. They are central in the theory of commutative algebra (and are especially important in their own right). The term "valuation" domain comes from a map that is associated with a valuation domain that, in some sense, behaves like a measure of size of the elements in the valuation domain. We will ignore this aspect (at least at first) but the interested student is pointed to Gilmer's book on Multiplicative Ideal Theory which gives a more thorough treatment than we have time for now.

Proposition 9.2.1. *Let V be an integral domain with quotient field K. The following conditions are equivalent.*

a) For all nonzero $a, b \in V$, either a divides b or b divides a.

b) For all $\alpha \in K \setminus \{0\}$, either α or α^{-1} is an element of V.

Any domain satisfying one (hence both) of the previous conditions is called a *valuation domain*.

Proof. Exercise. □

We will now develop some of the fundamental properties of valuation domains. We begin with a result in the spirit of the previous section.

Proposition 9.2.2. *Any valuation domain is integrally closed.*

Proof. Let V be our valuation domain with quotient field K and let $\alpha \in K$ be integral (and nonzero) over V. If $\alpha \in V$ then we are done, so we will assume that $\alpha \notin V$. Since $\alpha \notin V$ and V is a valuation domain, $\alpha^{-1} \in V$. Hence by an earlier lemma, $\alpha \in V[\alpha^{-1}] = V$ which is our contradiction. □

Theorem 9.2.3. *Let V be a valuation domain. Then V has the following properties.*

a) The ideals of V are linearly ordered.

b) V is quasilocal.

c) Any radical ideal of V is prime.

d) Any finitely generated ideal is principal.

Proof. For part a) let I, J be ideals of V and suppose that there is an element $x \in I \setminus J$. Our claim is that $J \subseteq I$. Select $y \in J$ and suppose that $y \notin I$. In particular, this means that x does not divide y (if $x|y$ then $y = vx \in I$). Since V is a valuation domain, it must therefore be the case that $y|x$. Hence $x = vy \in J$ and this is our desired contradiction.

Part b) follows from a) since any two maximal ideals are comparable.

For part c), let $I \subseteq V$ be a radical ideal and suppose that $xy \in I$. We will say without loss of generality that x divides y in V (and write $y = vx$ for some $v \in V$). Since $xy \in I$ and $\frac{y}{x} = v \in V$ then $\frac{y}{x}yx = y^2 \in I$. Since I is radical, $y \in I$ and we are done.

We leave d) as an (inductive) exercise. □

For our next result we will require the following lemma.

Lemma 9.2.4. *Let $R \subseteq T$ be domains and u a unit in T. If I is a proper ideal of R then I survives in either $R[u]$ or $R[u^{-1}]$.*

Proof. Suppose not, then we will have the following two equations:

$$a_0 + a_1u + \cdots + a_nu^n = 1$$

and

$$b_0 + b_1u^{-1} + \cdots + b_mu^{-m} = 1$$

with each a_i, b_j in I. We can assume that $n \geq m$ and that n is chosen to be minimal. Multiply the second equation by u^n and rearrange to get

$$(1 - b_0)u^n = b_1u^{n-1} + \cdots + b_mu^{n-m}.$$

Now multiply the first equation by $(1 - b_0)$ and substitute for $(1 - b_0)u^n$ to get

$$(1 - b_0)a_0 + (1 - b_0)a_1u + \cdots + a_n(b_1u^{n-1} + \cdots + b_mu^{n-m}) = 1 - b_0.$$

Taking the b_0 to the left side gives an equation like the first with a smaller exponent which contradicts minimality. This concludes the proof. □

Here is a rather important result about the existence of valuation overrings.

Theorem 9.2.5. *Let R be a domain with quotient field K and $I \subseteq R$ a proper ideal. Then there is a valuation overring of R (that is, a valuation domain V such that $R \subseteq V \subseteq K$) such that I survives in V ($IV \neq V$).*

Proof. we will first show the existence of a maximal overring of R where I survives. Consider the set of pairs (R_j, I_j) where each R_j is an overring of R and each I_j is a proper ideal of R_j containing I. We partially order this set by declaring $(R_a, I_a) \geq (R_b, I_b)$ if and only if $R_b \subseteq R_a$ and $I_b \subseteq I_a$. It is easy to see that any chain in this partially ordered set has an upper bound and so by Zorn, there is a maximal element (we will call it (V, J)).

We finish u by showing that V is a valuation domain. Indeed, suppose that $\alpha \in K$ and neither α nor α^{-1} is an element of V. Note that J must survive in either $V[\alpha]$ or $V[\alpha^{-1}]$ and this contradicts the maximality of V. □

We close this section (for now) with an important characterization of the integral closure of R.

Theorem 9.2.6. *Let R be an integral domain with quotient field K and integral closure $\overline{R}$. Then*

$$\overline{R} = \bigcap_{R \subseteq V \subseteq K} V$$

where the intersection ranges over all valuation overrings of R.

Proof. Exercise. □

9.3 Invertible ideals and Dedekind domains

Definition 9.3.1. *Let R be a domain with quotient field K. We say that an $R-$submodule of the quotient field (say I) is a fractional ideal if there is a nonzero $r \in R$ such that $rI \subseteq R$.*

Definition 9.3.2. *Let I be a fractional ideal. We define $I^{-1} = \{k \in K | kI \subseteq R\}$.*

Note that $II^{-1} \subseteq R$ by the very definition of I^{-1}.

Definition 9.3.3. *Let R be a domain with quotient field K and I a fractional ideal of R. We say that I is invertible if $II^{-1} = R$*

Here are some important examples of invertible ideals.

Example 9.3.4. *Let R be a domain with quotient field K and let a be a nonzero element of K. The $R-$module aR is a fractional ideal with inverse $a^{-1}R$. And, in fact, $aRa^{-1}R = R$. This example shows that any principal fractional ideal is an invertible ideal.*

Theorem 9.3.5. *The collection of invertible ideals of R forms an abelian group under ideal multiplication.*

Proof. It is easy to see once you realize that the multiplicative identity is R and the inverse of I is I^{-1}. □

Proposition 9.3.6. *Let I be a fractional ideal of the domain R. The following conditions are equivalent.*

a) I is invertible.

b) There is a fractional ideal J such that IJ is principal.

Proof. a) implies b) is easy. So suppose that there is a fractional J such that $IJ = aR$ with a a nonzero element of K. Note that $I(Ja^{-1}R) = aRa^{-1}R = R$ and I is invertible. □

This next theorem totally rocks since it is not obvious at first blush and gives a very restrictive necessary condition for an ideal to be invertible.

Theorem 9.3.7. *Any invertible ideal is finitely generated.*

Proof. Let I be an invertible ideal and $J = I^{-1}$. Since $IJ = R$, we can find $a_1, a_2, \cdots, a_n \in I$ and $b_1, b_2, \cdots, b_n \in J$ such that

$$a_1b_1 + a_2b_2 + \cdots + a_nb_n = 1.$$

Let $x \in I$ and multiply the above equation by x. This gives

$$a_1(xb_1) + a_2(xb_2) + \cdots + a_n(xb_n) = x$$

and note that since each $b_i \in J = I^{-1}$ and $x \in I$, each $xb_i \in R$. Hence the above equation shows that each $x \in I$ is an $R-$linear combination of the elements $a_1, \cdots, a_n$ and hence $I = (a_1, a_2, \cdots, a_n)$ and so is finitely generated. □

Here is a last useful lemma.

Lemma 9.3.8. *Let R be a domain and I a fractional ideal. I is invertible if and only if it is locally principal (principal in $R_{\mathfrak{P}}$ for all primes $\mathfrak{P}$).*

Proof. It is easy to see that if I is an invertible ideal of R and S is a multiplicative set (not containing 0) then I_S is invertible in R_S. This reduces to showing that a fractional ideal of $R_{\mathfrak{P}}$ is invertible if and only if it is principal. If it is principal, we have seen that it is invertible. If I is invertible in $R_{\mathfrak{P}}$ then I is generated by $a_1, a_2 \cdots, a_n$. And the generators of I^{-1} $(b_1, b_2, \cdots, b_n)$ can be chosen so that

$$a_1b_1 + \cdots + a_nb_n = 1.$$

Note that not all of the elements a_ib_i can be in the maximal ideal of $R_{\mathfrak{P}}$ and so at least one of them has to be a unit (since $R_{\mathfrak{P}}$ is quasilocal). WLOG, we will say that a_1b_1 is a unit in R and claim that $I = (a_1)$. One containment is easy and note that if $x \in I$ and $a_1b_1 = u$ is a unit then $x = xu^{-1}a_1b_1 = (xu^{-1}b_1)a_1 \in (a_1)$. This completes the proof. □

We now introduce Dedekind domains via the following theorem.

Theorem 9.3.9. *Let R be an integral domain. The following conditions are equivalent.*

a) EVery fractional ideal of R is invertible.

b) Every proper nonzero ideal of R is invertible.

c) Every nonzero proper ideal of R is a product of prime ideals.

d) R is (no more than) one-dimensional, Noetherian, and integrally closed.

e) R is Noetherian and $R_{\mathfrak{M}}$ is a Noetherian valuation domain for all maximal ideals $\mathfrak{M}$.

Any domain satifying one hence all of the above conditions is called a Dedekind domain.

Proof. In condition d) we will ignore the zero-dimensional situation since this is the field case!

We will skip the equivalence of a) and b) since the proof is pretty straightforward.

b)$\Longrightarrow$ c): Note that since we know that every ideal is invertible, this means that every ideal is finitely generated and R is Noetherian. We will show that the nonzero $I \subseteq R$ is a product of prime ideals. Note that since I is proper, I is contained in a prime ideal $\mathfrak{P}_1$, so $I \subseteq \mathfrak{P}_1$. Since $\mathfrak{P}_1$ is invertible we obtain $I\mathfrak{P}_1^{-1} \subseteq R$ (if we have equality, we are done and $I = \mathfrak{P}_1$). If $I\mathfrak{P}_1^{-1} \subsetneq R$ then this ideal must be contained in a prime ideal $\mathfrak{P}_2$ and as before we get $I\mathfrak{P}_1^{-1}\mathfrak{P}_2^{-1} \subseteq R$. Continuing this process, we obtain the increasing sequence of ideals

$$I \subseteq I\mathfrak{P}_1^{-1} \subseteq I\mathfrak{P}_1^{-1}\mathfrak{P}_2^{-1} \subseteq \cdots .$$

But, as we have observed, R is Noetherian and so this increasing chain must stabilize (and by our construction, this chain must reach R). We obtain

$$I\mathfrak{P}_1^{-1}\mathfrak{P}_2^{-1}\cdots\mathfrak{P}_n^{-1}$$

or

$$I = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_n$$

and I is a product of prime ideals.

c)$\Longrightarrow$ b): For this implication assume that each nonzero ideal of R is a product of primes. We will show that every prime ideal is invertible (and hence each ideal is invertible). Suppose that $\mathfrak{Q}$ is a prime ideal of R. Select a nonzero $q \in \mathfrak{Q}$. The ideal (q) is, by assumption a product of prime ideals. We write

$$(q) = \mathfrak{Q}\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_n.$$

Note that (q) is principal and hence invertible. This implies that each prime ideal in the product (and hence $\mathfrak{Q}$) is invertible by a previous lemma.

d)$\Longrightarrow$ e): Suppose that R is one-dimensional, Noetherian and integrally closed. Since we have "Noetherian" as an assumption, we merely need to show that $R_{\mathfrak{M}}$ is a Noetherian valuation domain for all maximal $\mathfrak{M}$. First note that the set of elements $I = \{a \in K | a\mathfrak{M} \subseteq \mathfrak{M}\}$ is precisely R (I is a fractional ideal since $\mathfrak{M}$ is finitely generated and hence I is finitely generated as R is Noetherian...every element of I is integral over R by the characterization of integral elements and hence, since R is integrally closed, $I = R$).

We now claim that $\mathfrak{M}^{-1}$ properly contains R. Note that, in any case, $R \subseteq \mathfrak{M}^{-1}$ and there are ideals (e.g. the principal ones) that have the property that their inverses properly contain R. A Zorn's lemma argument shows that there is a maximal such ideal with this property and this ideal must be prime. We obtain from this that $R \subsetneq \mathfrak{M}^{-1}$.

With this in hand, we note that $\mathfrak{M}\mathfrak{M}^{-1}$ must properly contain $\mathfrak{M}$ and be in R. Hence $\mathfrak{M}\mathfrak{M}^{-1} = R$ and $\mathfrak{M}$ is invertible.

Now localize R at the ideal $\mathfrak{M}$. This ring is clearly local (quasi-local and Noetherian). Since $\mathfrak{M}$ is invertible in R, $\mathfrak{M}R_{\mathfrak{M}}$ is invertible (hence principal) in $R_{\mathfrak{M}}$. Hence R is a local domain with a unique principal prime and hence a PID (and hence a NOetherian valuation domain).

e)$\Longrightarrow$ d): If R is Noetherian and $R_{\mathfrak{M}}$ is a Noetherian valuation domain for all maximal $\mathfrak{M}$ it suffices to show that R is integrally closed and one dimensional.

The one-dimensional follows rather easily since if $\mathfrak{P} \subsetneq \mathfrak{Q}$ are two nonzero priime ideals of R then both of these primes survive and are principal in the PID R which is a contradiction.

For integrally closed, observe that $R = \bigcap_{\mathfrak{M}} R_{\mathfrak{M}}$ and the intersection of a family of integrally closed domains is integrally closed.

a), b), c) $\Longrightarrow$ d), e): If every ideal of R is invertible, then R is Noetherian. It suffices to show that $R_{\mathfrak{M}}$ is a Noetherian valuation domain. But in $R_{\mathfrak{M}}$ every ideal is invertible and hence principal. So $R_{\mathfrak{M}}$ is a PID with a unique nonzero prime ideal, it is easy to see that this is a Noetherian valuation domain.

d), e) $\Longrightarrow$ a), b), c): For this direction, note that since $R_{\mathfrak{M}}$ is a Noetherian valuation domain for all maximal $\mathfrak{M}$, every ideal of R is locally principal and hence invertible. □

Here is a last result of this ilk.

Proposition 9.3.10. *Let R be a domain and I a fractional ideal. Then I is invertible if and only if I is a projective $R-$module.*

These observations allow us to make an interesting construction known as the class group.

Definition 9.3.11. *Consider the set $Inv(R)$ of invertible ideals of R. The collection $Prin(R)$ is a subgroup. The quotient $Inv(R)/Prin(R) = Cl(R)$ is called the class group of R.*

More generally the Picard group of R is the collection of rank 1 projective R modules with multiplication given by $\otimes_R$.

Here is an application. This is a famous theorem due to L. Carlitz.

Theorem 9.3.12. *Let R be a ring of algebraic integers. Then R is an HFD if and only if the class number of the ring of integers does not exceed 2.*

Bibliography