Algebra I

Jonathan Ma
johnma@udel.edu

May 15, 2024

Contents

1 Preface **4**

2 Isaacs, Algebra: A Graduate Course **5**
2.1 Group Preliminaries . . . 5
2.2 Examples of Groups . . . 6
2.2.1 Dihedral Groups, Rotation Groups, Symmetries . . . 6
2.2.2 The Cube . . . 6
2.2.3 General Linear Group . . . 7
2.2.4 Affine Group of the Line . . . 7
2.2.5 Rubik Cube . . . 7
2.3 Groups . . . 7
2.4 Isomorphism . . . 9
2.5 Examples of Group Isomorphisms . . . 9
2.6 Subgroups and Cosets . . . 10
2.6.1 Properties of Subgroups . . . 10
2.6.2 Construction of Subgroups . . . 10
2.7 Cyclic Groups . . . 11
2.7.1 Cyclic Group Isomorphisms . . . 13
2.8 Centralizers . . . 13
2.9 Automorphism . . . 14
2.9.1 Characteristic Subgroups . . . 14
2.9.2 Inner Automorphism . . . 14
2.10 Normal Subgroups . . . 15
2.11 Subgroup Composition . . . 16
2.12 Cosets . . . 16
2.12.1 Lagrange Theorem . . . 17
2.13 Properties of Normality of a Subgroup . . . 18
2.14 Quotient Groups . . . 18
2.15 Normalizers . . . 19
2.16 Homomorphism . . . 19
2.16.1 Canonical Homomorphism . . . 20
2.17 Properties of Homomorphism . . . 20
2.17.1 Isomorphism Theorem . . . 21
2.18 Correspondence . . . 22

2.18.1 Lattice Diagram Digression . . . 23
2.18.2 Correspondence Theorem . . . 24
2.19 Commutators . . . 25
2.20 Simple Groups . . . 26
2.21 Group Actions . . . 27
2.21.1 Normal Subgroups and Group Action . . . 29
2.22 Stabilizers . . . 30
2.23 Transitivity and Orbit . . . 30
2.23.1 Orbit Stabilizer Theorem . . . 31
2.24 Direct Product . . . 31
2.25 Fundamental Theorem of Finite Abelian Groups . . . 35

3 Lecture 1: Mon. Feb 5. 2024 36
3.1 The Dihedral Group: Isaacs 3A . . . 36
3.2 Fundamental Relation . . . 36
3.3 Group Homomorphisms . . . 36
3.4 Group Isomorphism and Automorphism . . . 37
3.5 Normal Subgroups . . . 37
3.6 The Isomorphism Theorems (I) . . . 37

4 Lecture 2: Wed. Feb. 7, 2024 38
4.1 The Isomorphism Theorems (II): Isaacs 3A . . . 38
4.2 Correspondence Theorem . . . 38
4.2.1 Generalized Correspondence Theorem . . . 39
4.3 The Isomorphism Theorems (III) . . . 39
4.4 Applications of Isomorphism Theorems . . . 39
4.5 The Decomposition of a Finite Group . . . 39
4.5.1 Maximal Subgroup, Maximal Normal Subgroup . . . 39
4.5.2 Decomposition of a Finite Group . . . 39

5 Lecture 3: Mon. Feb. 12. 2024 39
5.1 Automorphism . . . 39
5.2 Subgroup of Automorphism Group . . . 40
5.3 Characteristic Subgroups . . . 41
5.4 Applications of Characteristic Subgroups . . . 41

6 Lecture 4: Wed. Feb. 14, 2024 41
6.1 Permutations and Cycle Notation . . . 41
6.2 Properties of Cycles . . . 42
6.3 Disjoint Cycle Decomposition . . . 42
6.4 Cycle Structure . . . 42
6.5 Sign or Parity of a Permutation . . . 43

7 Lecture 5: Mon. Feb. 19 43
7.1 Cayley's Theorem . . . 43
7.2 Normal Subgroups of the Symmetric Group . . . 44

8 Lecture 6: Web. Feb. 21 **45**
8.1 Center of Symmetric Groups . . . 45
8.2 Conjugacy Classes . . . 45
8.3 Class Equation . . . 45
8.4 Cauchy's Theorem . . . 46

9 Lecture 7: Mon. Feb. 26 **46**
9.1 p-groups . . . 46
9.1.1 Maximal Normal Subgroups of p-groups . . . 47
9.1.2 Normalizers of p-groups . . . 47

10 Lecture 8: Wed. Feb. 28 **47**
10.1 Direct Product . . . 48

11 Lecture 9: Mon. Mar. 4 **49**
11.1 Fundamental Theorem of Finite Abelian Groups . . . 49
11.1.1 Dummit and Foote's Form . . . 49
11.1.2 Abelian Group Decomposition Lemma . . . 49

12 Lecture 10: Wed. Mar. 6 **50**

13 Lecture 11: Mon. Mar. 11 **50**
13.1 Characteristic . . . 50

14 Lecture 12: Mon. Mar. 18 **52**
14.1 Examples of Rings . . . 52
14.2 Ideals . . . 52
14.2.1 Properties of Ideals . . . 53

15 Lecture 13: Wed. Mar. 20 **53**
15.1 Ring Homomorphism . . . 54

16 Lecture 14: Mon. Apr. 1 **55**
16.1 Commutative Ring Ideals . . . 55

17 Lecture 15: Wed. Apr. 3 **56**
17.1 Maximal and Prime Ideals . . . 57
17.2 Rings of Fractions . . . 57

18 Lecture 16: Mon. Apr. 8 **58**
18.1 Divisibility . . . 58
18.2 Irreducibility, Primes . . . 58

19 Lecture 17: Wed. Apr. 10 **59**
19.1 Principal Ideal Domains . . . 59
19.2 Unique Factorization Domains . . . 60

20 Lecture 18: Mon. Apr. 15 **61**
20.1 More on UFDs, PIDs . . . 61

21 Lecture 19: Wed. Apr. 17 **61**
21.1 Euclidean Domains . . . 61
21.2 Multiplicative Norms . . . 63

22 Lecture 20: Mon. Apr. 22 **63**
22.1 Polynomial Rings . . . 63

23 Lecture 21: Wed. Apr. 24 **64**
23.1 Roots of Polynomials . . . 64
23.2 Polynomial Rings as Euclidean Domains and PIDs . . . 64

24 Lecture 22: Sick again **65**
24.1 Primitive Polynomials . . . 65

25 Lecture 23: Wed. May 1 **66**
25.1 Irreducibility Criterion . . . 66

26 Lecture 24: Mon. May 6 **68**
26.1 Field Theory . . . 68
26.2 Algebraic Extensions . . . 69
26.3 Vector Spaces . . . 69

27 Lecture 25: Wed. May 8 **69**
27.1 Minimal Polynomials . . . 69
27.2 Simple Extensions . . . 70
27.3 Intro to Finite Fields . . . 70

28 Lecture 26: Mon. May 13 **70**
28.1 Splitting Fields . . . 70
28.2 Finite Fields . . . 71

29 Lecture 27: Wed. May 15 **71**

1 Preface

Notes are taken to supplement the Spring 2024 version of 650 at the University of Delaware. The instructor is Professor Shuxing Li. Textbooks:

- Isaacs, *Finite Group Theory*,
- Isaacs, *Algebra: A Graduate Course*,
- Dummit and Foote, *Abstract Algebra*.

Most of the course is taught using Isaacs, *Algebra: A Graduate Course.* Another good resource to consult is the YouTube channel of Prof. Rudenko, UChicago. Group actions, Sylow theorems are covered more in depth in 845.

2 Isaacs, Algebra: A Graduate Course

2.1 Group Preliminaries

The following is a useful lemma of mappings.

Lemma 2.1. *Let $f\colon A \mapsto B$.*

(a). f is injective iff there exists $h\colon B \mapsto A$ such that $fh = i_A$.

(b). f is surjective iff there exists $g\colon B \mapsto A$ such that $gf = i_B$.

(c). If f is a bijection, then the maps g and h above are uniquely determined and equal.

Proof. Suppose f is injective. Fix an element $a \in A$, and define $h\colon B \mapsto A$ by

$$(b)h = \begin{cases} a & \text{if } b \notin (A)f \\ x & \text{if } (x)f = b \text{ for some } x \in A. \end{cases}$$

Note that by injectivity of f, there is at most one element $x \in A$ such that $(x)f = b$. Also, the mapping h is unambiguously defined, since the two cases are mutually exclusive and exhaust the possibilities. Conversely, if $h\colon B \mapsto A$ and $fh = i_A$, we wish to show that f is injective. Suppose $(x)f = (y)f$. Then $x = (x)fh = (y)fh = y$, as required.

Now suppose f is surjective. For each $b \in B$, choose $a \in A$ with $(a)f = b$, and once this choice is made, define $g\colon B \mapsto A$ by $(b)g = a$. Clearly, $gf = i_B$. Conversely, suppose $gf = i_B$. Then

$$B = (B)i_B = (B)gf \subseteq (A)f,$$

since $(B)h \subseteq A$. It follows that $(A)f = B$, as required.

Finally, assume f is a bijection so that maps h and g as in parts (a) and (b) exist. Then $g = gi_A = g(fh) = (gf)h = i_Bh = h$. In particular, g is uniquely determined, since it must equal any valid choice h. Similarly h is uniquely determined. □

The following corollary gives properties of the symmetric group.

Corollary 2.1.1. *Let $G = \mathrm{Sym}(X)$.*

(a). $i_X \in G$.

(b). g^{-1} exists and lies in G for each $g \in G$.

(c). $gh \in G$ for each $g, h \in G$.

Proof. Part (a) follows from definition of the symmetric group, and (b) follows from Lemma 2.1. For part (c), given $g, h \in G$, we see that

$$(gh)(h^{-1}g^{-1}) = i = (h^{-1}g^{-1})gh,$$

and thus gh has a left and right inverse. It follows by Lemma 2.1 that $gh \in \mathrm{Sym}(X)$. □

Definition 2.2. Let X be any set. A *permutation group* on X is any nonempty subset $G \subseteq \mathrm{Sym}(X)$ such that

i. $g^{-1} \in G$ for each $g \in G$, and

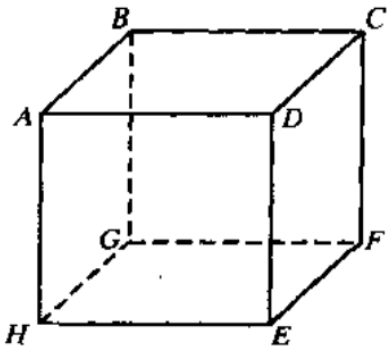

Figure 2.1: A cube.

ii. G is closed under function composition.

Note that for $g \in G$, there is no question that the mapping g^{-1} exists and lies in $\mathrm{Sym}(X)$. The point of condition (i) is that g^{-1} actually lies in the subset G. Conditions (i), (ii), together with the assumption that $G \neq \emptyset$ imply that $i_X \in G$, and so this need not be assumed.

Given a nonempty set G of mappings on some set X¡ perhaps the best strategy for showing that G is a permutation group is first to verify that each element $g \in G$ has both a left and a right inverse in G. From this, it follows that $G \subseteq \mathrm{Sym}(X)$, and this condition need not be verified separately. All that remains is to check the closure condition.

2.2 Examples of Groups

Some obvious examples of permutation groups are $\mathrm{Sym}(X)$ and the singleton set $\{i_X\}$ for arbitrary nonempty X. Isaacs goes on to discuss the *dihedral group* in length, which we cover in lecture.

2.2.1 Dihedral Groups, Rotation Groups, Symmetries

If instead of a square, we study the regular n-gon ($n \geq 3$), the resulting dihedral group would be D_{2n}, of order $2n$. As with D_8, half the elements of D_{2n} should correspond to flips, and half (counting the identity) correspond to plane rotations. Many *users* of group theory write D_n to refer to dihedral group of order $2n$. Most group theorists use the notation we have presented here.

Moving to three dimensions, consider the vertex set X of a regular polyhedron. The permutations of X induced by physical rotations of the object form a group called the *rotation group* of the object. A usually larger group is the *full group of symmetries*, which consists of all permutations of X realizable by geometric congruences of the polyhedron.

2.2.2 The Cube

Consider the case of a cube. The full group of the symmetries includes the "antipodal map" τ, which reflects each vertex through the center of the cube. (Thus $(A)\tau = F$, and $(C)\tau = H$, in Fig. 2.1, for instance.) The reader should check that τ does not correspond to any rotation. Note that there is no antipodal map for the regular tetrahedron, although it is true for Fig. 2.1 that there are symmetries that are not rotations. In fact, in this case, the full group of symmetries is the full symmetric group on the vertex set, of order $4! = 24$.

Let us compute the order of the rotation group R of a cube. After a rotation, face $ABCD$ can coincide with any of the six faces of the original cube, and in each location, it can have any

of the four rotational orientations. It follows that $|R| = 6 * 4 = 24$. The full group of symmetries S, on the other hand, has order 48 (left as exercise). What are the 24 symmetries that are not rotations? Among these are the reflections in the nine planes of symmetry of the cube. These planes of symmetry are of two types: six that contain four vertices (for instance, the planes determined by B, D, G, E, or by A, E, B, F) and three that are parallel to faces of the cube. A tenth nonrotational symmetry is the antipodal map τ. The remaining 14 nonrotational symmetries are rather hard to visualize, and we shall not discuss them further now. The product (composition) of each of the nine reflections with τ yields a rotation of order 2. A good exercise is to count how many elements of each order there are in the rotation group of a cube.

Note. Elements of a group having order 2 are usually called *involutions*

2.2.3 General Linear Group

The "general linear" group $GL(V)$, where V is a vector space, is the group of all nonsingular (invertible) linear transformations of V. It should be obvious that $GL(V) \subseteq \mathrm{Sym}(V)$ is, in fact, a group.

2.2.4 Affine Group of the Line

The "affine group" of the line is the set of all mappings on the real numbers $\mathbb{R}$ that are of the form $x \mapsto ax + b$, where $a, b \in \mathbb{R}$, and $a \neq 0$. The reader should check that this is really a group.

2.2.5 Rubik Cube

Of the 54 colored squares on the surface of the cube, six may be viewed as never moving from their initial position (although the do rotate). In other words, if we start with the red face on top, and the green face in front, then all interesting cube moves can be made while keeping the red center square on top, and the green center square in front. (Of course, this prohobits rotations of the entire cube, but such rotations are not strictly necessary for solving the puzzle.) Now let G be the group of those permutations on the $54 - 6 = 48$ colored squares that can be realized by some sequence of cube twists. Let us compute $|G|$. As a first approximation, consider disassembling the cube. When this is done, one obtains eight small "corner" cubers having three colored faces each, and 12 small "edge" cubes having two colored faces each. The six face-centers remain attached to one another, and we view them as being fixed in space. To reassemble the cube, we can permute the corner cubes in 8! ways, and the edge cubes in 12!. In addition, each corner cube can occur in three different orientations and each edge cube in two different orientations. This yields a total of $8! \cdot 12! \cdot 3^8 \cdot 2^{12}$ ways to reassemble the cube. It turns out (although this is not trivial to prove) that only one-twelfth of these are attainable via legal moves without doing violence to the puzzle. The order of the Rubik cube group is then given by

$$|G| = \left(\frac{1}{12}\right) 8! \cdot 12! \cdot 3^8 \cdot 2^{12} = 43,252,003,274,489,856,000.$$

2.3 Groups

Throughout most of the nineteenth century, the word "group" meant "permutation group". The modern definition is attributed to English mathematician Arthur Cayley. Recall that a *binary operation* on a set G is a rule that assigns to each ordered pair of elements $x, y \in G$ another element of G. If $\circ$ is a binary operation, we write $x \circ y$ to denote the result of applying this rule to x, y. We say $\circ$ is associative if $x \circ (y \circ z) = (x \circ y) \circ z$, for all $x, y, z \in G$.

Definition 2.3. A *group* is a set G together with an associative binary operation $\circ$ defined on G such that there exists $e \in G$ with the following properties.

i. For each $x \in G, x \circ e = x = e \circ x$.

ii. For each $x \in G$, there exists $y \in G$ such that $x \circ y = e = y \circ x$.

Note that the "closure" condition that $x \circ y \in G$ whenever $x, y \in G$ need not be stated explicitly, since it is subsumed in the assumption that $\circ$ is a binary operation on G. Any permutation group is a group with respect to the operation of function composition. In addition to permutation groups, our modern definition allows such objects as the additive group of the integers, the multiplicative group of the positive rationals, and the group of $n \times n$ nonsingular matrices over fields (with respect to matrix multiplication).

Lemma 2.4. *Let G be a group. Then, for $a, b \in G$, there exists unique elements $x, y \in G$ such that $ax = b$, and $ya = b$. In particular, the element e is unique, and for each $x \in G$, the element y of Definition 2.3(ii) is unique.*

Proof. Choose z such that $az = e = za$. Now $a(zb) = eb = b$, and so we can take $x = zb$. For uniqueness, if $ax = ax'$, we have

$$x = ex = zax = zax' = ex' = x'.$$

The existence and uniqueness of y are proved similarly. □

In a permutation group, the unique element satisfying condition (ii) of Definition 2.3 is called the *identity element* of the group and it is customarily denoted 1. The reader should note that the identity of a permutation group is defined by what it is (a particular mapping), whereas the identity of an abstract group is defined by how it *behaves* with respect to the group operation. Similarly, the element y of a permutation group that satisfies condition (ii) with respect to x it the inverse map, x^{-1}, and by analogy, in an abstract group, y is said to be the *inverse element* of x, and the notation x^{-1} is used in this case too.

The conditions of Definition 2.3 are more stringent than they really need to be.

Theorem 2.5. *Let G be a set with an associative multiplication and suppose there exists $e \in G$ with the following properties:*

i. $xe = x$ for all $x \in G$ and

ii. for each $x \in G$, there exists $y \in G$ with $xy = e$.

Then G is a group.

Proof. Let $x \in G$ and choose y according to property $(ii.)$. It suffices to show that $ex = x$ and $yx = e$. By property $(ii.)$, we find $z \in G$ with $yz = e$. Therefore,

$$x = xe = x(yz) = (xy)z = ez,$$

and

$$yx = y(ez) = yz = e.$$

Now,

$$ex = (xy)x = x(yx) = xe = x.$$

□

Isaacs notes that "elementwise" calculations in the preceding proof are not typical of most algebra. The proof of Theorem 2.5 could almost serve as a model of what algebra is not, in the opinion of Isaacs.

One way to describe the operation in an abstract group G is via a *multiplication table*. This is a square array, with rows and columns labeled by the elements of G, where the position in row x, column y is occupied by the element xy. Generally it is neither useful nor practical to actually write down a multiplication table for G, but we can think of G being defined by such a table.

2.4 Isomorphism

One of the advantages of thinking about groups abstractly, as in Definition 2.3 is that is allows us to see that certain groups are essentially the same. Suppose we rename the rows and columns of the multiplication table of G and also the replace the entries in the table. The result will be the multiplication table of a group that is not in any essential respect, different from G.

Definition 2.6. Let G and G be two groups, and suppose $\theta\colon G \mapsto H$ is a bijection We say that θ is an *isomorphism* if

$$\theta(xy) = \theta(x)\theta(y),$$

for all $x, y \in G$. We say that G and G are *isomorphic*, and we write $G \cong H$ if an isomorphism between them exists.

If θ is an isomorphism, G to H, then θ induces a match-up of the elements of G with the elements of H that causes their multiplication tables to coincide. To the extent that we view groups as being defined by their multiplication tables, we see that isomorphic groups are essentially "the same." All "group theoretic" questions will have the same answers in G and H. For example. each of G and H will have equal number of elements of any given order, and G will be abelian iff H is abelian.

2.5 Examples of Group Isomorphisms

Example 2.7. As a concrete example, consider the group R or rotations of a cube and $S = \mathrm{Sym}(4)$. (We write $\mathrm{Sym}(n)$ as a shorthand for $\mathrm{Sym}(\{1, 2, \ldots, n\})$.) We have seen that $|R| = 24$, and, of course, $|S| = 4! = 24$. In fact, we will see that $R \cong S$, and so these differently constructed objects are group theoretically identical. (Note that R permutes eight objects, the vertices of a cube, and S permutes $\{1, 2, 3, 4\}$. As permutation groups, therefore, R and S are quite different.)

In the cube of Fig. 2.1, there are four "major diagonals." AF, BE, CH, and DG. Each element of R corresponds to a rotation of the cube and each such rotation induces a permutation of these four diagonals. If we fix an assignment of the numbers $1, 2, 3$ and 4 to the four diagonals, then each element of R determines a particular element of S. To see that the corresponding mapping $\theta\colon R \mapsto S$ is an isomorphism, we need to establish that θ is a bijection. We will not write a formal proof of this, but it is easy to see that θ is injective. In other words, two different rotations cannot induce the same permutation of the diagonals. Since $|R| = 24 = |S|$, it follows that θ maps onto S. Because the multiplications in both R and S come about by simply following one operation by another, it should now be fairly clear that θ is an isomorphism.

Note that if $\theta\colon G \mapsto H$ is an isomorphism, then $\theta^{-1}\colon H \mapsto G$ is an isomorphism also. Furthermore, if $\varphi\colon H \mapsto K$ is another isomorphism, it is routine to check that $\theta\varphi\colon G \mapsto K$ is an isomorphism. It follows from all of this that isomorphism of groups is an equivalence relation.

2.6 Subgroups and Cosets

We can get considerable insight into the "structure" of a group G by investigating its subgroups.

Definition 2.8. Let G be a group. A subset $H \subseteq G$ is a *subgroup* if H is closed under multiplication in G, and forms a group with respect to this multiplication.

Example 2.9. For instance, the permutation groups $G \subseteq \mathrm{Sym}(X)$ are precisely the subgroups of the full symmetric group $\mathrm{Sym}(X)$.

Example 2.10. For another example, view the integers $\mathbb{Z}$ as a group with respect to addition. Then for each $n \in \mathbb{Z}$, the set $n\mathbb{Z}$ of all multiples of n is a subgroup of $\mathbb{Z}$. (In fact, these are all of the subgroups of $\mathbb{Z}$.)

Example 2.11. Obvious examples of subgroups for any group G are G itself, and the singleton subgroup $\{1\}$. We shall sometimes write 1 in place of $\{1\}$ to denote the trivial subgroup of any group.

2.6.1 Properties of Subgroups

If $H \subseteq G$ is a subgroup, then H must contain some element e that acts as an identity element for H. In particular, $ee = e$. Since $e1 = e$ also, where 1 is the identity of G, we conclude that $1 = e$, by Lemma 2.4, and thus $1 \in H$. Now, if $h \in H$, then there must exist $h' \in H$ with $hh' = 1$, and it follows that $h' = h^{-1}$. We have shown that subgroups of a group G are closed under taking inverses (in G) as well as under multiplication. Conversely, we have the following lemma.

Lemma 2.12. *Let G be a group, and let $H \subseteq G$ be a nonempty subset. Suppose $xy' \in H$ for all $x, y \in H$. Then H is a subgroup of G. In particular, any nonempty subset of G closed under multiplication and taking inverses in G is a subgroup.*

Proof. Choose $h \in H$. Then $1 = hh^{-1} \in H$ by hypothesis. For $y \in H$, we have $y^{-1} = 1y^{-1} \in H$, and if also $x \in H$, then $xy = x(y^{-1})^{-1} \in H$. Therefore, the G-multiplication does define an operation on H and the associative property is inherited from G. Since $1 \in H$, and $y^{-1} \in H$, for all $y \in H$, we see that H has an identity, and inverses, and so is a group. □

Corollary 2.12.1. *Suppose that $\mathcal{H}$ is a collection of subgroups of some group G and let*

$$D = \bigcap_{h \in \mathcal{H}} H.$$

Then D is a subgroup of G.

Proof. Since each $H \in \mathcal{H}$ contains 1, we have $1 \in D$, and in particular, $D \neq \emptyset$. Now if $x, y \in D$, then $x, y \in H$, for all $H \in \mathcal{H}$, and so $xy^{-1} \in H$ for all such H. Thus, $xy^{-1} \in D$, and D is a subgroup. □

2.6.2 Construction of Subgroups

Much of group theory is concerned with variations of the question "how can we construct subgroups for a group?" We will discuss a few such constructions now. Given any subset $X \subseteq G$, we can consider the family $\mathcal{H}$ of all subgroups $H \subseteq G$ such that $X \subseteq H$. (Note that $G \in \mathcal{H}$.) The subgroup $\bigcap \mathcal{H}$ is called the subgroup generated by X, and is denoted $\langle X \rangle$. This subgroup is characterized by two properties:

1. $X \subseteq \langle X \rangle$.

2. If $X \subseteq H$ and H is a subgroup of G, then $\langle X \rangle \subseteq H$.

In other words, the group generated by X is the smallest subgroup of G that contains X (where the word "smallest" should be understood in the sense of containment). Note that if $X \subseteq G$ is itself a subgroup, then $\langle X \rangle = X$. There is a more explicit (though somewhat less "clean") alternative construction of $\langle X \rangle$.

Lemma 2.13. *Let G be a group and suppose that $X \subseteq G$ is an arbitrary subset. Then $\langle X \rangle$ is the set of all finite products*

$$u_1 u_2 u_3 \cdots u_n$$

of elements $u_i \in G$ such that u_i or $u_i^{-1} \in X$. (The "empty product" with $n = 0$ is understood to equal 1.)

Proof. Let S be the set of all finite products as in the statement of the lemma. Note that $1 \in S$, and so $S \neq \emptyset$ (even if $X = \emptyset$). Now S is clearly closed under multiplication, and since

$$(u_1 u_2 u_3 \cdots u_n)^{-1} = u_n^{-1} u_{n-1}^{-1} \cdots u_1^{-1} \in S,$$

it follows that S is a subgroup. Since $X \subseteq S$, we have $\langle X \rangle \subseteq S$. On other hand since $X \subseteq \langle X \rangle$ and $\langle X \rangle$ is closed under multiplication and inverses, it follows from the definition of S that $S \subseteq \langle X \rangle$. □

2.7 Cyclic Groups

If X is given as an explicitly listed set, for instance, $X = \{a, b, c\}$, then it is customary to omit the braces and write $\langle a, b, c \rangle$ instead of $\langle \{a, b, c\} \rangle$. An important case of this is when $|X| = 1$. A group G is said to be *cyclic* if there exists some $g \in G$ with $\langle g \rangle = G$. In general, for any element g of any group, the subgroup $\langle g \rangle$ is cyclic. The following result is immediate from Lemma 2.13. (Note that for negative integers n, the power g^n is defined as $(g^{-1})^{-1}$.)

Corollary 2.13.1. *Let $g \in G$. Then $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.*

Lemma 2.14. *Let $G = \langle g \rangle$, so that G is cyclic. Let $H \subseteq G$ be a subgroup and suppose that $g^n \in H$, where n is the smallest positive integer that makes this true. Then*

a. for $m \in \mathbb{Z}$, we have that $g^m \in H$ iff n divides m and

b. $H = \langle g^n \rangle$.

Note that if g has infinite order and $H = 1$, then there is no positive integer n such that $g^n \in H$. (Recall that $o(g) = \infty$ means that no positive power of g is 1.) In all other cases, if either $H > 1$, or $o(g) < \infty$, then there does exist a positive integer m with $g^m \in H$, and so the integer n of the lemma does exist. To see this, observe that if $o(g) < \infty$, we can take $m = o(g)$, and if $H > 1$, then if $1 \neq h \in H$, it follows that either h or h^{-1} will be of the form g^m for $m > 0$.

Proof of Lemma 2.14. If $n \mid m$, we write $m = nq$, with $q \in \mathbb{Z}$. Then $g^m = (g^n)^q \in H$. Conversely, suppose $g^m \in H$. By the division algorithm, we may write $m = qn + r$, with $0 \leq r < n$. Then

$$g^r = g^m (g^n)^{-q} \in H,$$

and by the minimality of n, it follows that $r = 0$, and n divides m, as required. Statement (b) follows, since certainly $\langle g^n \rangle \subseteq H$, and if h is any element of H, then $h = g^m$, for some m, and so, by part (a), $m = qn$, and $h = (g^n)^q \in \langle g^n \rangle$. □

Corollary 2.14.1. *Every subgroup of a cyclic group is cyclic.*

Lemma 2.15. *Let $g \in G$ with $o(g) = n < \infty$. Then*

a. $g^m = 1$ *iff* $n \mid m$,

b. $g^m = g^\ell$ *iff* $m \equiv \ell \bmod n$ *and*

c. $|\langle g \rangle| = n$.

Proof. Apply Lemma 2.14(a) to the group $\langle G \rangle$ with $H = 1$. This yields part (a). Part (b) follows from (a) since $g^m = g^\ell$ iff $g^{m-\ell} = 1$. Finally, by part (b), the elements of $\langle g \rangle$ are in one-to-one correspondence with the residue classes of integers mod n, and there are exactly n of these. □

Note that if $g \in G$ and $o(g) = \infty$, then all powers of g are distinct, since if $g^m = g^\ell$, with $m > \ell$, then $g^{m-\ell} = 1$, and g has finite order. We can thus write $|\langle g \rangle| = o(g)$ in all cases.

Theorem 2.16. *Let G be a finite cyclic group of order n. Then G has exactly one subgroup of order d for each divisor d of n, and G has no other subgroups.*

Proof. Write $G = \langle g \rangle$ so that $o(g) = n$ by Lemma 2.15(c). For each divisor d of n, we write $e = n/d$, and put $H_d = \langle g^e \rangle$. It is easy to see that $o(g^e) = d$, and thus $|H_d| = d$ by Lemma 2.15(c). What remains is to show that every subgroup $H \subseteq G$ is one of the H_d.

If $H \subseteq G$, then by Lemma 2.14, $H = \langle g^e \rangle$ for some integer e that divides every integer m such that $g^m \in H$. Since $g^n = 1 \in H$, we conclude that e divides n, and thus, $H = H_d$, where $d = n/e$. □

We mention that the additive group of the integers, and of the integers mod n are examples of cyclic groups. In fact, it is easy to prove (and we shall do so later) that every cyclic group is isomorphic to one of these.

To state our final results about cyclic groups in this chapter, recall that if a, b are integers that are both not zero, their *greatest common divisor*, denoted $\gcd(a, b)$ is the largest integer that divides both a and b. Also recall Euler's totient function is defined for positive integers n by $\varphi(n) = |U_n|$, where

$$U_n = \{r \in \mathbb{Z} \mid 0 \leq r < n \text{ and } \gcd(r, n) = 1\}.$$

Theorem 2.17. *Let G by cyclic of finite order n. Then G contains precisely $\varphi(n)$ elements of order n, and these are the elements g^r for $r \in U_n$, where g is any element of order n in G.*

Proof. By Lemma 2.15(c), the elements $x \in G$ of order n are just those elements for which $\langle x \rangle = G$. Let g be any such element so that the powers g^r for $0 \leq r < n$ are the n distinct elements of G. We need to show that $o(g^r) = n$ iff $\gcd(r, n) = 1$.

Suppose that $\gcd(r, n) > 1$, then $d = n/\gcd(r, n) < n$, and n divides rd. It follows that $1 = (g^r)^d$ and so $o(g^r) \leq d < n$ as required. Now suppose $\gcd(r, n) = 1$, and let e be the least positive integer such that $g^e \in \langle g^r \rangle$. By Lemma 2.14($a$) we see that e divides r, and also, (since $g^n = 1 \in \langle g^r \rangle$) e divides n. Thus, $e = 1$, and $g \in \langle g^r \rangle$. Therefore, $\langle g^r \rangle = G$, and $o(g^r) = n$. □

2.7.1 Cyclic Group Isomorphisms

Theorem 2.18. *Let B and C be cyclic of order $n < \infty$. Then $B \cong C$ and there are exactly $\varphi(n)$ different isomorphisms that map B to C.*

Proof. Fix $b \in B$ such that $B = \langle b \rangle$. If $\theta\colon B \mapsto C$ is any isomorphism, write $\theta(b) = c$. Then $\theta(b^m) = c^m$ for all $m \in \mathbb{Z}$, and thus θ is completely determined on all of B once we are given $c = \theta(b)$. Also, since θ is surjective, every element of C must have the form c^m for some $m \in \mathbb{Z}$, and thus, c is a generating element of C.

We have now constructed an injective map from the set of all isomorphisms $\theta\colon B \mapsto C$ into the set of all generating elements c of C; this map carries θ to the generator $c = \theta(b)$ of C. Since the total number of generating elements of C is $\varphi(n)$ by Theorem 2.17, it suffices to show that for every choice of generator c, there exists an isomorphism $\theta\colon B \mapsto C$ such that $\theta(b) = c$.

The isomorphism we seek will necessarily map b^m to c^m, and so we will define θ by $\theta(b^m) = c^m$ for $m \in \mathbb{Z}$. The problem with this is that the element b^m of B might also be called b^ℓ for some other integer ℓ. We need to show that the value of θ at this element is unambiguously defined. We need, in other words, to show that $c^m = c^\ell$. Since $o(b) = |B| = n$, by Lemma 2.15(c) the equation $b^m = b^\ell$ yields that $m \equiv \ell \pmod{n}$ by Lemma 2.15(b). Thus $c^m = c^\ell$ by Lemma 2.15(b) and (c). We now know that θ is well defined, and what remains is to show that θ is an isomorphism. Since every element of C has the form $c^m = \theta(b^m)$, we see that θ is surjective. It is thus necessarily injective, since $|B| = |C| < \infty$. Finally,

$$\theta(b^m b^\ell) = \theta(b^{m+\ell}) = c^{m+\ell} = c^m c^\ell = \theta(b^m)\theta(c^m),$$

and so θ is an isomorphism. □

2.8 Centralizers

Recall that a group G is abelian if $xy = yx$, for all $x, y \in G$. Note that cyclic groups are automatically abelian. If G is nonabelian, we might wish to consider for some $g \in G$, the set

$$\mathbf{C}_G(g) = \{x \in G \mid xg = gx\}$$

of all elements that commute with g. This set is the *centralizer* of g in G, and what makes it especially useful is that it is a subgroup of G.

Lemma 2.19. *Let $g \in G$. Then $\mathbf{C}_G(g)$ is a subgroup of G.*

Proof. Since $1 \in \mathbf{C}_G(g)$, the centralizer is nonempty and it is easy to see that it is closed under multiplication. If $x \in \mathbf{C}_G(g)$, then $xg = gx$, and multiplying by x^{-1} from both the left and the right yields $x^{-1}(xg)x^{-1} = x^{-1}(gx)x^{-1}$. Thus, $gx^{-1} = x^{-1}g$, and $x^{-1} \in \mathbf{C}_G(g)$, as required. □

We can define the centralizer of an arbitrary subset $X \subseteq G$ by

$$\mathbf{C}_G(X) = \{y \in G \mid xy = yx \text{ for all } x \in X\}.$$

Thus,

$$\mathbf{C}_G(X) = \bigcap_{x \in X} \mathbf{C}_G(x),$$

and so the centralizer of any subset of a group is a subgroup, by Corollary 2.12.1. In particular, taking $X = G$, we get the *center* of G, denoted $\mathbf{Z}(G)$. Thus,

$$\mathbf{Z}(G) = \mathbf{C}_G(G) = \{y \in G \mid xy = yx \text{ for all } x \in G\}$$

is a subgroup. Note that $\mathbf{Z}(G)$ is an abelian group and that G is abelian iff $G = \mathbf{Z}(G)$. Of course, it can happen (and often does) that the center of a group is trivial. For instance, for the dihedral groups,

$$|\mathbf{Z}(D_{2n})| = \begin{cases} 1 & n \equiv 1 \pmod 2 \\ 2 & n \equiv 0 \pmod 2. \end{cases}$$

The rotation groups of the five regular polyhedra all have trivial centers, but the full group of symmetries of four of these objects have centers of order 2. (Which one is the exception, and why?) The following is an example that shows how one can use the fact that centralizers are not merely sets of elements but are subgroups.

Lemma 2.20. *Let $X \subseteq G$ be a subset such that $xy = yx$ for all $x, y \in X$. Then $\langle X \rangle$ is abelian.*

Proof. This follows fairly easily from Lemma 2.13, but we prefer this argument. By hypothesis, $X \subseteq \mathbf{C}_G(X)$. Since $\mathbf{C}_G(X)$ is a subgroup, we conclude $\langle X \rangle \subseteq \mathbf{C}_G(X)$ and so $X \subseteq \mathbf{C}_G(\langle X \rangle)$. As above, this yields $\langle X \rangle \subset \mathbf{C}_G(\langle X \rangle)$ and so $\langle X \rangle$ is abelian. □

If $\theta\colon G_1 \mapsto G_2$ is an isomorphism, it should be clear that $\theta(\mathbf{Z}(G_1)) = \mathbf{Z}(G_2)$. Although this can be proved by a routine computation, we hope the reader will see that this has to be true because the center is a "group theoretic" object, and isomorphisms capture all group theoretic information.

2.9 Automorphism

An isomorphism from a group G to itself is called an automorphism of G. (Note that the identity map on G is an automorphism, but most groups have many other automorphisms too.) Since isomorphisms carry centers to centers, it follows that every automorphism of G maps $\mathbf{Z}(G)$ to itself.

2.9.1 Characteristic Subgroups

A subgroup $H \subseteq G$ with the property that $\theta(H) = H$ for every automorphism θ of G is said to be *characteristic* in G, and we write $H \operatorname{char} G$. Not only is the center of a group characteristic, but generally any subgroup uniquely defined by group theoretic properties and not dependent on arbitrary choices or on the names of elements is also characteristic. A good rule of thumb is that any subgroup described by the definite article "the" is characteristic. For example, the Frattini subgroup of any group should be understood by the reader to be characteristic.

2.9.2 Inner Automorphism

An important example of an automorphism of G is the *inner automorphism* θ_g induced by an element $g \in G$. This is the map

$$\theta_g(x) = g^{-1}xg.$$

The reader should check that θ_g really is an automorphism. A fairly standard notation we will adopt is

$$x^g = g^{-1}xg$$

for $x, g \in G$. The element x^g is said to be the *conjugate* of x with respect to g. In this language, the inner automorphism induced by g is the corresponding conjugation map. Observe that if x, g commute, then $x^g = x$, and thus, in an abelian group, inner automorphisms are trivial. (As if to

compensate for this, another type of automorphism exists only in abelian groups: this is the map $\theta(x) = x^{-1}$ for $x \in G$.)

The set $\mathrm{Aut}(G)$ of all automorphisms of G is a subgroup of $\mathrm{Sym}(G)$, and the set $\mathrm{Inn}(G)$ of inner automorphisms is a subgroup of $\mathrm{Aut}(G)$. (The reader should check these assertions.)

2.10 Normal Subgroups

Let us go back to the situation of an isomorphism $\theta\colon G_1 \mapsto G_2$. It should be clear that if $H \subseteq G_1$ is a subgroup, then $\theta(H)$ is a subgroup of G_2. In particular, automorphisms map subgroups to subgroups. The subgroup

$$H^g = \{h^g \mid h \in H\}$$

is a subgroup conjugate to H. It is, of course, the image of H under the inner automorphism induced by g.

Since characteristic subgroups are fixed by all automorphisms, they are surely fixed by inner automorphisms, and so, if $C \operatorname{char} G$, then $C = C^g$ for all $g \in G$. (Note that this is completely obvious in the case $C = \mathbf{Z}(G)$, and since $x^g = x$ for all $x \in X$. In general, the equation $C^g = C$ does not imply that $x^g = x$ for all $x \in C$.) We are now ready to introduce one of the most important concepts in group theory.

Definition 2.21. A subgroup $N \subseteq G$ is *normal* if $N^g = N$ for all $g \in G$. We write $N \lhd G$ in this situation.

In other words, the normal subgroups of a group are precisely those subgroups fixed by all inner automorphisms. All characteristic subgroups are normal, and all subgroups of abelian groups are normal. Of course, the subgroups 1 and G are always normal in any group G.

Lemma 2.22. *Let $H \subseteq G$ be a subgroup. Then $H \lhd G$ if $H^g \subseteq H$ for all $g \in G$.*

The reader should be warned that this lemma does not state that $H^g = H$ whenever $H^g \subseteq H$. Since the inner automorphism induced by the element g is a bijection, it is certainly true that $|H^g| = |H|$, and if H is finite, this equality of orders together with the containment $H^g \subseteq H$ certainly does imply that $H^g = H$. For infinite subgroups, however, this does not generally follow, and is not generally true. (There is an example given in the exercises.)

Proof of Lemma 2.22. We must show that $H^g = H$ for all $g \in G$. Since $H^g \subseteq H$ for all elements g, it follows that

$$H = (H^g)^{g^{-1}} \subseteq H^{g^{-1}}$$

for all $g \in G$. Applying this result with the element g^{-1} in place of g yields

$$H \subseteq H^{(g^{-1})^{-1}} = H^g$$

and thus $H = H^g$. □

For example, consider the case $G = D_{2n}$, the dihedral group, and let H be the set of plane rotations in G. Since H is closed under multiplication, we have $H^g \subseteq H$, if $g \in H$. On the other hand, if $g \notin H$, then g is a "flip" that interchanges the front and back of the n-gon. In this case, $g^{-1} = g$, and for $h \in H$, we have $h^g = ghg$, which does not interchange front and back. Thus, $h^g \in H$, for all $h \in H$, and it follows that $H \lhd G$.

Now H is cyclic of order n, and it follows that each subgroup C of H is characteristic in H. This is so since if $\theta \in \mathrm{Aut}(H)$, then $\theta(C)$ is a subgroup of H such that $|C| = |\theta(C)|$. It follows by Theorem 2.16 that $C = \theta(C)$, as required. Thus, $C \operatorname{char} H$, and $H \lhd G$. The next result shows that $C \lhd G$.

Lemma 2.23. *Let $N \triangleleft G$, and suppose that C char N. Then $C \triangleleft G$.*

Proof. Let $g \in G$. Since $N \triangleleft G$, the inner automorphism induced by g maps N to itself, and, in fact, defines an automorphism of N. (It may not be an inner automorphism of N.) Since C is characteristic in N, this automorphism of N maps C to itself, and so, $C^g = C$, as required. □

Note. It does not follow that $C \triangleleft G$ if all that is known is that $C \triangleleft N$ and $N \triangleleft G$, or even that N char G.

We give one more example of a normal subgroup now.

Theorem 2.24. *Let G be any group. Then* $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

Proof. Let $\theta \in \mathrm{Inn}(G)$, and $\sigma \in \mathrm{Aut}(G)$. By Lemma 2.22, it suffices to show that $\theta^\sigma \in \mathrm{Inn}(G)$ for any choice of θ and σ. We can write $\theta = \theta_g$ (the conjugation map induced by $g \in G$). To compute θ^σ, we can apply it to $x \in G$ as such:

$$(x)\theta^\sigma = (x)\sigma^{-1}\theta_g\sigma = (g^{-1}(x\sigma^{-1})g)\sigma = (g^{-1})\sigma \cdot x \cdot (g)\sigma$$

where the last equality holds because σ is an automorphism. We have

$$(x)\theta^\sigma = (g\sigma)^{-1}x(g\sigma),$$

and so $\theta^\sigma = \theta_{(g)\sigma}$, the inner automorphism induced by $(g)\sigma \in G$. □

2.11 Subgroup Composition

Let $X, Y \subseteq G$ be any two subsets. We write

$$XY = \{xy \mid x \in X, y \in Y\}.$$

Lemma 2.25. *Let $H, K \subseteq G$ be subgroups. Then HK is a subgroup iff $HK = KH$.*

2.12 Cosets

In the case where $X = \{x\}$, we write xY or Yx instead of $\{x\}Y$ or $Y\{x\}$.

Definition 2.26. Let $H \subseteq G$ be a subgroup. If $g \in G$, then the sets

$$Hg = \{hg \mid h \in H\}$$

and

$$gH = \{gh \mid h \in H\}$$

are, respectively, the right coset and the left coset of H determined by g.

Note that if $g \notin H$, then also $g^{-1} \notin H$, and it follows that $1 \notin Hg$, and $1 \notin gH$. In particular, cosets Hg, gH are not subgroups in this case. If $g \in H$, on the other hand, then $Hg = H = gH$, and thus, the subgroup H is one of its own right and left cosets. Also note that for any element $g \in G$, we have $g \in gH$ and $g \in Hg$. This shows that G is the union of all the right and left cosets of any subgroup.

Lemma 2.27. *Let $H \subseteq G$ be a subgroup.*

a. If $Hx \cap Hy \neq \emptyset$, then $Hx = Hy$.

b. If $xH \cap yH \neq \emptyset$, then $xH = yH$.

Proof. First note that $Hh = H$ for $h \in H$. (This is really part of Lemma 2.4 applied to H.) Thus

$$H(hx) = (Hh)x = Hx,$$

and so if $g \in Hx \cap Hy$, we have $Hg = Hx$ and $Hg = Hy$, so that $Hx = Hy$ as desired. Part (b) is proven similarly. □

Corollary 2.27.1. *Let $H \subseteq G$ be a subgroup. Then G is the disjoint union of the distinct right cosets of H. The analogous result holds for left cosets.*

Lemma 2.28. *Let $H \subseteq G$ be a subgroup. For every $g \in G$, we have*

$$|gH| = |H| = |Hg|.$$

Proof. The map $\theta\colon H \mapsto Hg$ defined by $(h)\theta = hg$ certainly maps onto Hg, and is injective by Lemma 2.4. It follows that $|H| = |Hg|$, and the other equality is proved similarly. □

If $H \subseteq G$ is a subgroup, then the *index* of H in G, denoted $|G\colon H|$ is the number of distinct right cosets of H in G. As we shall see, the cardinality of the set of left cosets of H in G is equal to that of the right cosets, and so the index of a subgroup is, in fact, left-right symmetric.

2.12.1 Lagrange Theorem

In Theorem 2.16, we proved that if G is a finite cyclic group and $H \subseteq G$, is a subgroup, then $|H|$ divides $|G|$. We are now ready to prove this much more generally.

Theorem 2.29 (Lagrange)**.** *Suppose $H \subseteq G$ is a subgroup. Then $|G| = |H||G : H|$. In particular, if G is finite, then $|H|$ divides $|G|$, and $|G|/|H| = |G : H|$.*

Proof. The group G is the disjoint union of $|G : H|$ right cosets, each of cardinality equal to $|H|$. □

Note that we could as well have worked with left cosets, and concluded that if G is finite, then the "left index" equals $|G|/|H|$ and therefore the left and right indices are equal for subgroups of finite groups. An important consequence of Lagrange's theorem is the following corollary.

Corollary 2.29.1. *Let G be finite, and let $g \in G$. Then $o(g)$ divides $|G|$, and $g^{|G|} = 1$.*

Proof. We have $o(g) = |\langle g \rangle|$ by Lemma 2.15(c), and this divides $|G|$ by Theorem 2.29. The last assertion is immediate from Lemma 2.15(a). □

As an application of Corollary 2.29.1, we mention the number theoretic result of Euler that $a^{\varphi(n)} \equiv 1 \bmod n$ for positive integers a and n such that $\gcd(a, n) = 1$. The trick here is to observe that

$$U_n = \{r \in \mathbb{Z} \mid 0 \leq r < n \text{ and } \gcd(r, n) = 1\}$$

becomes a group under multiplication if we identify each element r with its residue class mod n. (A few things need to be checked, but we will not do so here.) Euler's theorem is immediate by applying Corollary 2.29.1 to the group U_n.

2.13 Properties of Normality of a Subgroup

There is an important connection between normality of a subgroup and the properties of its cosets.

Theorem 2.30. *Let $H \subseteq G$ be a subgroup. Then the following are equivalent:*

i. $H \triangleleft G$,

ii. $Hg = gH$ *for all* $g \in G$.

iii. Every left coset of H *in* G *is a right coset.*

iv. The set of right cosets of H *in* G *is closed under set multiplication.*

Proof. Let us first assume (i). Then $g^{-1}Hg = H$ for all $g \in G$, and multiplication by g on the left hields $Hg = gH$, proving (ii). That (ii) implies (iii) is obvious, so we assume (iii) and prove (iv). If $x, y \in G$, we must show that $HxHy$ is a right coset. By (iii), however, $xH = Hg$ for some $g \in G$, and we have

$$HxHy = H(Hg)y = Hgy,$$

which is a right coset as required. Finally, assume (iv), then $Hg^{-1}Hg$ is a right coset containing $g^{-1}g = 1$. Thus,

$$g^{-1}Hg \subseteq Hg^{-1}Hg = H1 = H,$$

and H is normal by Lemma 2.22. □

Note that item (ii) of Theorem 2.29 is left-right symmetric. It follows that we can get two additional conditions equivalent to H being normal by exchanging the words "left" and "right" in (iii) and (iv).

2.14 Quotient Groups

If $H \triangleleft G$, we use the notation G/H (read "G mod H") to denote $\{Hg \mid g \in G\}$. By Theorem 2.30, we know that G/H is closed under set multiplication.

Theorem 2.31. *If $H \triangleleft G$, then G/H is a group. The identity element of G/H is the coset H, and the inverse of the coset (Hx) in G/H is Hx^{-1}. Also,*

$$(Hx)(Hy) = H(xy)$$

for all $x, y \in G$.

Proof. We have $(H)(Hx) = Hx$, and $(Hx)H = HxH = HHx = Hx$, since $xH = Hx$. Also, $xy \in (Hx)(Hy)$ and thus $(Hx)(Hy) = H(xy)$ by Lemma 2.27. In particular, $(Hx)(Hx^{-1}) = H = (Hx^{-1})(Hx)$. □

The group G/H is called the *quotient group* or *factor group* of G by H. For example, if $G = \mathbb{Z}$ (w.r.t. addition) and $H = n\mathbb{Z}$ (the multiples of N), then the (additive) coset $H + m$ is the residue class of m mod n, and the factor group G/H is the additive group of residues mod n.

Corollary 2.31.1. *Let $N \triangleleft G$ and let $H \subseteq G$ be any subgroup. Then $HN = NH$ is a subgroup and it is normal if $H \triangleleft G$.*

Proof. We have

$$\bigcup_{h\in H} hN = \bigcup_{h\in H} Nh = NH$$

by Theorem 2.30, It follows that HN is a subgroup by Lemma 2.25. If $g \in G$, then since conjugation by g defines an automorphism of G, we have $(HN)^g = H^g N$. If $H \triangleleft G$, then $H^g = H$, and the proof is complete. □

2.15 Normalizers

Even if the subgroup $H \subseteq G$ is not normal, we may still be able to use some of our results about normality. The idea is to find some subgroup $K \subseteq G$ such that $H \triangleleft K$. In fact, we shall see that for any subgroup $H \subseteq G$, there is a unique subgroup $K \supseteq H$ maximal with the property that $H \triangleleft K$.

It is convenient to work more generally and consider subsets that may not be subgroups. If $X \subseteq G$ is any subset, the we define the *normalizer* of X in G to be the set $\mathbf{N}_G(X) = \{g \in G \mid X^g = X\}$.

Lemma 2.32. *The normalizer $\mathbf{N}_G(X)$ is a subgroup of G for every subset $X \subseteq G$. If X is a subgroup, then $X \subseteq \mathbf{N}_G(X)$.*

Proof. First note that $X^1 = X$, and $(X^g)^h = X^{gh}$ for elements $g, h \in G$. It follows that $\mathbf{N}_G(X)$ is nonempty, and that it is closed under multiplication. To see that it contains the inverse of each of its elements, suppose that $g \in \mathbf{N}_G(X)$. Then

$$X^{g^{-1}} = (X^g)^{g^{-1}} = X^{gg^{-1}} = X^1 = X,$$

and thus, $g^{-1} \in \mathbf{N}_G(X)$, as desired. If X is a subgroup, then conjugation by any element $x \in X$ defines an automorphism of X and in particular, the conjugation map is surjective. Thus, $X^x = X$, for $x \in X$, and it follows that $X \subseteq \mathbf{N}_G(X)$ as required. □

Corollary 2.32.1. *Suppose $H \subseteq G$ is a subgroup and write $N = \mathbf{N}_G(H)$. Then $H \triangleleft N$ and if $K \subseteq G$ is any subgroup containing H, then $H \triangleleft K$ iff $K \subseteq N$.*

We saw in Corollary 2.31.1 that if $N \triangleleft G$, then $HN = NH$, and so NH is a subgroup of G. This can be generalized as follows.

Corollary 2.32.2. *Let $H, K \subseteq G$ be subgroups. If $K \subseteq \mathbf{N}_G(H)$, then $HK = KH$, and HK is a subgroup of G.*

Proof. Since $H \triangleleft \mathbf{N}_G(H)$, we can apply Corollary 2.31.1 in the group $\mathbf{N}_G(H)$. □

The reader should note that although the condition $xH = Hx$ implies that $x \in \mathbf{N}_G(H)$, it does not follow from the equation $HK = KH$ that $K \subseteq \mathbf{N}_G(H)$.

2.16 Homomorphism

When considering mappings from one mathematical object to another of the same type, we usually give special attention to those maps which respect the structure of the objects.

Definition 2.33. A map $\varphi\colon G \mapsto H$, for G, H groups, is called a *homomorphism* if $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$.

Group isomorphisms are those homomorphisms that happen to be bijections.

Example 2.34. The trivial homomorphism is defined as $\varphi\colon G \mapsto H$ for groups G, H, where $\varphi(g) = 1$ for all $g \in G$.

Example 2.35. Consider the group $GL(V)$ of nonsingular linear transformations on the finite-dimensional vector We can of course identify $GL(V)$ with the group of nonsingular $n \times n$ matrices over $\mathbb{F}$ where $n = \dim_F V$. For each $t \in G$, its determinant $\det t \in \mathbb{F} - \{0\}$. The set $\mathbb{F}^x$ of nonzero elements of $\mathbb{F}$ form a group with respect to multiplication, and the fact that $\det st = \det s \det t$ tells us that $\det\colon GL(V) \mapsto \mathbb{F}^x$ is a homomorphism. space V over a field $\mathbb{F}$.

Example 2.36. We can map the additive group of the integers onto that of the integers mod n by sending each integer to its residue class. It should be clear that this defines a homomorphism. In fact, since residue classes are cosets, this is a special case of something more general, and we come to what is perhaps the most important example of a homomorphism.

2.16.1 Canonical Homomorphism

Definition 2.37 (Canonical Homomorphism)**.** Let $N \triangleleft G$, and consider the factor group G/N. Define $\pi\colon G \mapsto G/N$ by $\pi(g) = Ng$. Since $NxNy = Nxy$ for all $x, y \in G$, we see that π is a homomorphism. This map is called the *canonical* homomorphism of G onto G/N, and we note that it does map *onto* G/N.

2.17 Properties of Homomorphism

Lemma 2.38. *Let $\varphi\colon G \mapsto H$ be a homomorphism. Then:*

(*a*). $\varphi(1) = 1$, *and* $\varphi(x^{-1}) = \varphi(x)^{-1}$ *for all* $x \in G$,

(*b*). $N = \{g \in G \mid \varphi(g) = 1\}$ *is a normal subgroup of* G,

(*c*). $\varphi(x) = \varphi(y)$ *iff* $Nx = Ny$,

(*d*). φ *is injective iff* $N = 1$.

Proof. We have $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$, and canceling $\varphi(1)$ yields $1 = \varphi(1)$. Now, $1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, therefore, $\varphi(x^{-1}) = \varphi(x)^{-1}$. Part (*a*) is proved.

Since $1 \in N$ by part (*a*), we see that $N \neq \emptyset$. If $x \in N$, then $\varphi(x^{-1}) = \varphi(x)^{-1} = 1^{-1} = 1$, and $x^{-1} \in N$. Also, if $x, y \in N$, then $\varphi(xy) = \varphi(x)\varphi(y) = 1 \cdot 1 = 1$, and $xy \in N$. This proves that N is a subgroup. For normality, we compute that $\varphi(x^{-1}nx) = \varphi(x^{-1})\varphi(n)\varphi(x) = \varphi(x)^{-1}\varphi(x) = 1$ for $n \in N$, and $x \in G$. Thus, $N^x \subseteq N$ for all $x \in G$, so $N \triangleleft G$.

For part (*c*), observe that if $\varphi(x) = \varphi(y)$, then $1 = \varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1})$, so $xy^{-1} \in N$, and $x \in Ny$. Therefore, $Nx = Ny$. Conversely, if $Nx = Ny$, then $x = ny$ for some $n \in N$, and we have $\varphi(x) = \varphi(ny) = \varphi(n)\varphi(y) = \varphi(y)$, since $\varphi(n) = 1$.

Finally, if φ is injective, then for $n \in N$, we have $\varphi(n) = 1 = \varphi(1)$, and so $n = 1$, and thus $N = 1$. Conversely, if $N = 1$, and $\varphi(x) = \varphi(y)$, we must have $x = y$, by part (*c*).

□

The normal subgroup $N = \{g \in G \mid \varphi(g) = 1\}$ is called the *kernel* of the homomorphism φ, denoted $\ker(\varphi)$.

Example 2.39. For the determinant map $\det\colon GL(V) \mapsto \mathbb{F}^x$, we see that $\ker(\det)$ is the group of all linear transformations of V with determinant 1. This subgroup is called the *special linear* group, and is denoted $SL(V)$.

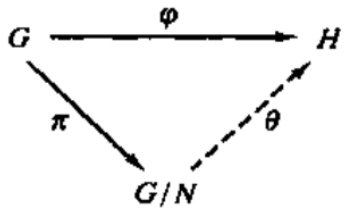

Figure 2.2: Commutative diagram of Isomorphism theorem.

If $\pi\colon G \mapsto G/N$ is the canonical homomorphism, where G is arbitrary, and $N \triangleleft G$, then $\ker(\pi) = N$. To see this, observe that $\pi(g) = 1$ iff $Ng = N$, and this happens iff $g \in N$. (Recall that N is the "1" element of G/N.) This gives an interesting characterization of the set of all normal subgroups of a group.

Corollary 2.39.1. *Let G be an arbitrary group. Then the normal subgroups of G are precisely the kernels of all homomorphisms defined on G.*

Proof. This is immediate from Lemma 2.38(b) and the fact that every $N \triangleleft G$ is the kernel of the associated canonical homomorphism $G \mapsto G/N$. □

2.17.1 Isomorphism Theorem

In some sense, the canonical homomorphisms $\pi\colon G \mapsto G/N$ for normal subgroups $N \triangleleft G$ are the only surjective homomorphisms. More precisely, we have the following Isomorphism theorem.

Theorem 2.40 (Isomorphism Theorem)**.** *Let $\varphi\colon G \mapsto H$ be a surjective homomorphism and let $N = \ker(\varphi)$ Then $H \cong G/N$. In fact, there exists a unique isomorphism $\theta\colon G/N \mapsto H$ such that $\pi\theta = \varphi$, where π is the canonical homomorphism $G \mapsto G/N$.*

Before giving the proof, some discussion is appropriate. Fig. 2.2 is a diagram showing the relevant groups and maps. The arrow representing θ is dashed rather than solid, since it is the existence of this map that is the assertion of the theorem. The equation $\pi\theta = \varphi$ states that starting with an element of G and following either of the two routes to H, either direct, or via G/N, we reach the same element of H. In general, one says that a diagram of groups and homomorphisms is a *commutative diagram* if, whenever there are alternative routes between groups, the composite map along the two routes are equal.

Note that what the commutativity of the diagram in Fig. 2.2 really says is that if we were to identify G/N with H, using the map θ to make this identification, then φ and π would turn out to be the same map. In other words, every surjective homomorphism is "essentially" just a canonical homomorphism.

Proof of Theorem 2.40. Since we require $\pi\theta = \varphi$, we are forced to define $(Ng)\theta = g\varphi$, and hence θ is certainly unique. We need to check, however, that θ is well defined. Specifically, if $Nx = Ny$, we require that $x\varphi = y\varphi$. (If this were not the case, the definition of the image of this coset under θ would be ambigious.) We have the desired equality by Lemma 2.38(c). Since

$$(NxNy)\theta = (Nxy)\theta = (xy)\varphi = (x\varphi)(y\varphi) = (Nx)\theta(Ny)\theta,$$

we see that θ is a homomorphism. We certainly have $\pi\theta = \varphi$, and since φ, it follows that θ must be surjective too.

Finally, we check that θ is injective by showing that $\ker(\theta)$ is trivial (and using Lemma 2.38(d)). If $Ng \in \ker(\theta)$, then $1 = (Ng)\theta = g\varphi$, and so $g \in \ker(\varphi) = N$. Thus, $Ng = N$ (the identity of G/N) and $\ker(\theta)$ is trivial, as required. □

The following application of the Isomorphism theorem (Theorem 2.40) is a slight variation on Theorem 2.18.

Corollary 2.40.1. *Up to isomorphism, the only cyclic groups are the groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ for positive integers n.*

Proof. Let C be cyclic and write $C = \langle c \rangle$. Map $\varphi\colon \mathbb{Z} \mapsto C$ by $\varphi(k) = c^k$. Observe that $\varphi(k+\ell) = c^{k+\ell} = c^k c^\ell$, and so φ is a homomorphism from the group $\mathbb{Z}$ (with respect to addition) to C. Clearly, φ maps onto C, and so by Theorem 2.40 we have $C \cong \mathbb{Z}/K$, where $K = \ker(\varphi)$. The proof is completed by observing that the subgroup $K \subseteq \mathbb{Z}$ is cyclic (by Corollary 2.14.1) and thus $K = \langle n \rangle$ for some integer n. Since $\langle n \rangle = \langle -n \rangle$, we can take $n > 0$ if K is nontrivial. □

2.18 Correspondence

Next, we explore the connections between homomorphisms and the subgroup structures of the domain and target. Suppose $\varphi\colon G \mapsto H$ is a homomorphism. If $U \subseteq G$, we write

$$\varphi(U) = \{\varphi(u) \mid u \in U\}.$$

We say that $\varphi(U)$ is the *image* of U under φ. Similarly, if $V \subseteq H$ we define the *inverse image* of V under φ by the formula

$$\varphi^{-1}(V) = \{u \in G \mid \varphi(u) \in V\}.$$

The inverse image is always defined, even though there may not be a map φ^{-1}. If φ is an isomorphism, so that φ^{-1} does exist, then the notation $\varphi^{-1}(V)$ may seem ambiguous since it might also mean the image of V under φ^{-1}. Because this is equal to the inverse image of V under φ in this case, no confusion should arise.

Lemma 2.41. *Let $\varphi\colon G \mapsto H$ be a homomorphism.*

(a). If $U \subseteq G$ is a subgroup, then $\varphi(U) \subseteq H$ is a subgroup.

(b). If $V \subseteq H$ is a subgroup, then $\varphi^{-1}(V) \subseteq G$ is a subgroup that contains $\ker(\varphi)$.

Proof. Proof is routine using Lemma 2.38. □

An important example of Lemma 2.41 is where $N \triangleleft G$ and $\pi\colon G \mapsto G/N$ is the canonical homomorphism. If $H \subseteq G$, then NH is a group and $N \triangleleft NH$. The quotient group NH/N is a subgroup of G/N, and in fact, NH/N is the image of H under π. To see this, note that

$$NH/N = \{Nnh \mid n \in N, h \in H\} = \{Nh \mid h \in H\} = \pi(H).$$

Theorem 2.42 (Diamond)**.** *Let $N \triangleleft G$ and $H \subseteq G$. Then $H \cap N \triangleleft H$, and $H/(H \cap N) \cong NH/N$.*

Proof. Let $\pi\colon G \mapsto G/N$ be the canonical homomorphism and let φ be the restriction of π to the subgroup H. Thus, φ is a homomorphism of H onto $\pi(H) = NH/N$, and since φ is equal to π on the elements of H, we have

$$\ker(\varphi) = H \cap \ker(\pi) = H \cap N.$$

Thus, $H \cap N \triangleleft H$ and

$$H/(H \cap N) = H/\ker(\varphi) \cong NH/N$$

by Theorem 2.40, the Isomorphism theorem. □

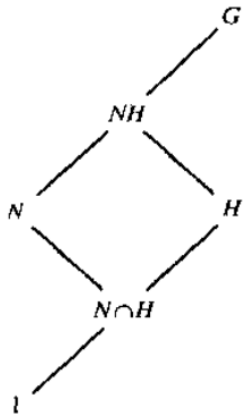

Figure 2.3: Lattice diagram of Theorem 2.42.

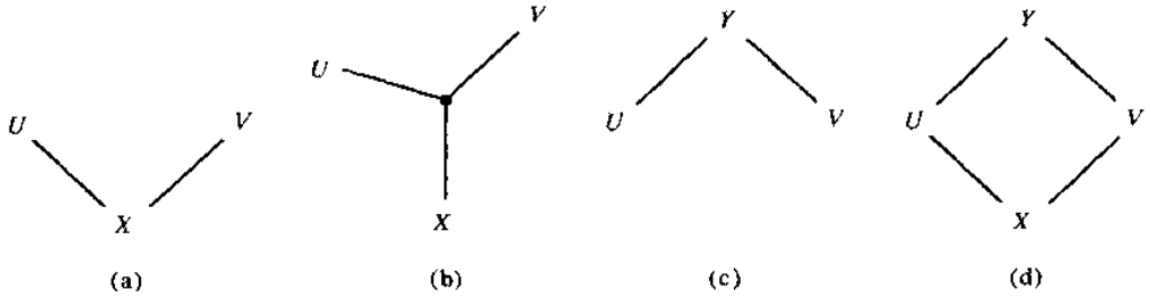

Figure 2.4: Bunch of lattice diagrams.

The diagram in Fig. 2.3 is known as a "lattice diagram" and is entirely different from the mapping diagram in Fig. 2.2. These lattice diagrams can be extremely useful, since with them it is possible to represent graphically some quite complicated interrelationships among subgroups. Indeed, it is occasionally possible to read an entire proof directly from a carefully drawn diagram.

2.18.1 Lattice Diagram Digression

In a lattice diagram, the nodes represent a few of the subgroups of some group, and the line segments indicate containment: the lower node is a subgroup of the upper.

According to the standard conventions, Fig. 2.4(a) indicates not only that $X \subseteq U$ and $X \subseteq V$ (allowing the possibility of equality) but also that $X = U \cap V$. We would draw diagram Fig. 2.4(b) if we did not know that X was the intersection, and the unlabeled node in Fig. 2.4(b) represents $U \cap V$. We do not intend Fig. 2.4(b) to preclude the possibility that $U \cap V = X$, however.

In Fig. 2.4(c), the assertion is that Y is generated by U and V, and not merely that $U \subseteq Y$ and $V \subseteq Y$. An important special case is where $Y = UV$ is the product, and not just the group generated. In that case, we say that the four nodes $U, V, Y = UV$, and $X = U \cap V$ form a *diamond*, and it is customary to draw the figure as a parallelogram, as in Fig. 2.4(d). The conclusion of Theorem 2.42, the Diamond theorem, can be paraphrased as "opposite sides of a parallelogram are isomorphic." This requires some normality, of course.

In the case that we have a diamond as in Fig. 2.4(d), there is further information available. By Problem 2.8(c) (Isaacs), we have $|Y\colon V| = |U\colon X|$, and $|Y\colon U| = |V\colon X|$, and so if we imagine that the lengths of the line segments in a lattice diagram represent indices of subgroups, this is consistent with the fact that opposite sides of a parallelogram are equal.

2.18.2 Correspondence Theorem

The point of the next theorem is that the subgroup structure of the image of a homomorphism from G is captured by that part of G containing the kernel.

Theorem 2.43 (Correspondence)**.** *Let $\varphi\colon G \mapsto H$ be a surjective homomorphism, and let $N = \ker(\varphi)$. Define the following sets of subgroups:*

$$S = \{U \mid N \subseteq U \subseteq G\},$$

and

$$T = \{V \mid V \subseteq H\}.$$

Then φ and φ^{-1} are inverse injections between S and T. Furthermore, these maps respect containment, indices, normality and factor groups.

The meaning of the last sentence is as follows. Suppose $U_1, U_2 \in S$, and V_1, V_2 are the corresponding elements of T. (Thus, $V_i = \varphi(U_i)$ and $U_i = \varphi^{-1}(V_i)$.) Then $U_1 \subseteq U_2$ iff $V_1 \subseteq V_2$, and in this case, $|U_2\colon U_1| = |V_2\colon V_1|$. Also, $U_1 \lhd U_2$ iff $V_1 \lhd V_2$, and in this case, $U_2/U_1 \cong V_2/V_1$.

Proof of Theorem 2.43. By Lemma 2.41, φ, φ^{-1} do define maps between S and T and we need to show that they are inverses of each other. For $U \in S$, it is immediate from the definitions that $U \subseteq \varphi^{-1}(\varphi(U))$. If $g \in \varphi^{-1}(\varphi(U))$, then $\varphi(g) \in \varphi(U)$ and thus $Ng = Nu$ for some $u \in U$ by Lemma 2.38(c). Thus, $g \in Nu \subseteq U$ since $N \subseteq U$, and we have $\varphi^{-1}(\varphi(U)) = U$.

Now let $V \in T$. Clearly, $\varphi(\varphi^{-1}(V)) \subseteq V$. If $v \in V$, then since φ is surjective, there exists $g \in G$ with $\varphi(g) = v$. Thus, $g \in \varphi^{-1}(V)$ and $v = \varphi(g) \in \varphi(\varphi^{-1}(V))$. We have now established that $\varphi(\varphi^{-1}(V)) = V$, and so φ and φ^{-1} are inverse bijections.

It is clear that these maps respect containment, and nothing further need be said about that. Now suppose $U_1 \lhd U_2$, with $U_i \in S$. Then for all $x \in U_2$, we have $x^{-1}U_1x = U_1$, and applying φ, we get $\varphi(x)^{-1}\varphi(U_1)\varphi(x) = \varphi(U_1)$. This says that $\varphi(U_1) \lhd \varphi(U_2)$, as required.

Next, assume $U_1 \subseteq U_2$ with $U_i \in S$, and suppose $\varphi(U_1) \lhd \varphi(U_2)$. We need to show that $U_1 \lhd U_2$ and so we let $x \in U_2$ and observe that

$$\varphi(x^{-1}U_1x) = \varphi(x)^{-1}\varphi(U_1)\varphi(x) = \varphi(U_1)$$

by the normality assumption. Since $x^{-1}U_1x \in S$, and φ is injective, we conclude that $x^{-1}U_1x = U_1$ and $U_1 \lhd U_2$ as required. The maps, therefore, do respect normality.

Next, we consider factor groups. Let $U_1 \lhd U_2$, with $U_i \in S$ and write $V_i = \varphi(U_i)$. To show $U_2/U_1 \cong V_2/V_1$, we construct a homomorphism θ of U_2 onto V_2/V_1 and show that $\ker(\theta) = U_1$. What we want then will follow from the Isomorphism theorem.

Let $\pi\colon V_2 \mapsto V_2/V_1$ be the canonical homomorphism, and let φ' be the restriction of φ to U_2. Write $\theta = \varphi'\pi$, so that $\theta\colon U_2 \mapsto V_2/V_1$. Then θ is a homomorphism, and since $\theta(U_2) = \pi(\varphi(U_2)) = \pi(V_2) = V_2/V_1$, we see that θ is surjective. Now $\ker(\theta) = \varphi^{-1}(V_1) = U_1$, and it follows that $U_2/U_1 \cong V_2/V_1$ by the Isomorphism theorem.

Suppose $U_1 \subseteq U_2$ with $U_i \in S$, and $V_i = \varphi(U_i)$. We must show that $|U_2\colon U_1| = |V_2\colon V_1|$, and so we construct a bijection from $\{U_1x \mid x \in U_2\}$ onto $\{V_1z \mid z \in V_2\}$. Note that $\varphi(U_1x) = V_2\varphi(x)$

and so φ maps cosets to cosets. To show this map is surjective, let $z \in V_2$. Then $z = \varphi(x)$ for some $x \in U_2$, and we have $\varphi(U_1 x) = V_1 z$, as required. Finally, if $\varphi(U_1 x) = \varphi(U_1 y)$ for $x, y \in U_2$, we have $V_1\varphi(x) = V_1\varphi(y)$, and so $\varphi(x)\varphi(y)^{-1} \in V_1$. Thus $\varphi(xy^{-1}) \in V_1$ and $xy^{-1} \in \varphi^{-1}(V_1) = U_1$. Therefore, $x \in U_1 y$ and $U_1 x = U_1 y$. This shows that our map is injective, and the proof is complete. □

The following corollary is very useful.

Corollary 2.43.1. *Let $N \triangleleft G$. Then every subgroup of G/N has the form H/N for some (unique) subgroup $H \subseteq G$ with $H \supseteq N$.*

Proof. Apply Theorem 2.43 to the situation $\pi\colon G \mapsto G/N$, where π is the canonical homomorphism. Note that if $H \subseteq G$ with $N \subseteq H$, then we have $\pi(H) = \{Nh \mid h \in H\} = H/N$. □

Another consequence of our theorem is the following corollary.

Corollary 2.43.2. *Let $N \subseteq M \triangleleft G$ with $N \triangleleft G$. Then $G/M \cong (G/N)/(M/N)$.*

Proof. Again, apply the Correspondence theorem to the canonical homomorphism $\pi\colon G \mapsto G/N$. Since G corresponds to G/N, and M corresponds to M/N, the desired isomorphism is just the statement that the maps in Theorem 2.43 respect factor groups. □

We comment briefly on the interpretation of the Correspondence theorem in terms of lattice diagrams, at least in the case where φ is the canonical homomorphism $G \mapsto G/N$. If we have a lattice diagram for some of the subgroups of G, including N, then the part of the diagram above N is a valid lattice diagram for G/N. In fact, diamonds go over to diamonds, since if $N \subseteq U$, and $N \subseteq V$, and UV is a group, then in G/N we have $(U/N)(V/N) = (UV)/N$.

The Isomorphism theorem, the Diamond theorem, the correspondence theorem, and Corollary 2.43.2 are often referred to collectively as the "homomorphism theorems." The three results we have named must surely be the most used theorems in algebra (if one includes their module and ring theoretic analogs). They are so basic, however, that they are seldom quoted explicitly in the professional literature. They are simply used without comment.

2.19 Commutators

Definition 2.44. Define the *commutator* $[x, y]$ of $x, y \in G$ by the formula $[x, y] = x^{-1}y^{-1}xy$, and we pointed out that x, y commute iff $[x, y] = 1$. The subgroup generated by all commutators in G is called the commutator subgroup, or the *derived subgroup* of G, and is denoted G'. Since an isomorphism of one group to another clearly maps the commutator subgroup of the first group onto that of the second, it follows that automorphisms of G map G' to itself. In short, G' $\operatorname{char} G$, and in particular, $G' \triangleleft G$. Note that $G' = 1$ iff G is abelian.

Theorem 2.45. *Let $N \triangleleft G$. Then G/N is abelian iff $G' \subseteq N$.*

Proof. Let $\pi\colon G \mapsto G/N$ be the canonical homomorphism. If $x, y \in G$, then $[\pi(x), \pi(y)] = \pi([x, y])$, and so $\pi(x)$ and $\pi(y)$ commute iff $\pi([x, y]) = 1$. Since this happens iff $[x, y] \in N$, it follows that G/N is abelian iff $[x, y] \in N$ for all $x, y \in G$. □

Corollary 2.45.1. *Let $\varphi\colon G \mapsto A$ be a homomorphism, where A is abelian. Then $G' \subseteq \ker(\varphi)$.*

Proof. We have $G/\ker(\varphi) \cong \varphi(G) \subseteq A$ by the Isomorphism theorem (Theorem 2.40). Therefore, $G/\ker(\varphi)$ is abelian, and $G' \subseteq \ker(\varphi)$. □

Corollary 2.45.2. *Let $G' \subseteq H \subseteq G$. Then $H \triangleleft G$.*

Proof. Since G/G' is abelian, we have $H/G' \triangleleft G/G'$. By the Correspondence theorem (Theorem 2.43) applied to the canonical homomorphism $\pi\colon G \mapsto G/G'$, we conclude that $H \triangleleft G$. □

We shall have more to say about derived subgroups later, when we consider "solvable" groups.

2.20 Simple Groups

Definition 2.46. A nonidentity group is *simple* if it has just two normal subgroups, the identity and the group itself

Example 2.47. Groups of prime order are automatically simple since their only subgroups, normal or otherwise, are the identity, and the whole group.

Example 2.48. It is provable that the only abelian simple groups are the cyclic groups of prime order.

Since the normal subgroups of a group are precisely the kernels of homomorphisms, it follows that a group G is simple iff $G > 1$ and every nontrivial homomorphism defined on G is injective.

It turns out that nonabelian simple groups are really quite rare. For instance, there are just five (isomorphism classes of) nonabelian groups of order less than 1000; they have orders 60, 168, 360, 504, and 660. Isaacs encourages the reader to prove this result, and warns that the number 720 is an order of magnitude more difficult to eliminate than any other order.

Various aspects of the problem of finding all finite nonabelian simple groups have been undergoing active research for the better part of a century, and recently, the complete solution of this problem was announced. The so-called Classification theorem gives a list of a number of infinite families of simple groups, and 26 exceptional "sporadic" groups, and it asserts that every nonabelian finite simple group lies on this list.

The complete proof of the Classification theorem runs to many thousands of pages written by dozens of authors. Why have simple groups evoked so much interest and effort? Presumable, it is their comparative rarity among finite groups in general that has inspired most of this, but another reason is that in some sense, simple groups are the "bricks" from which all finite groups are constructed.

To make this precise, let G be any finite group, and assume $G > 1$. Let N be a maximal normal subgroup of G. (In other words, $N \triangleleft G$ is a proper subgroup and there exists no subgroup $M \triangleleft G$ with $N < M < G$.) It follows by the Correspondence theorem that G/N is simple. If $N > 1$, repeat this process by choosing some maximal normal subgroup of N (which of course, may not be normal in G). Continuing in this way, we obtain a series of subgroups

$$S\colon 1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n = G,$$

where each group is maximal normal in the next. Such a series is called a *composition series* for G. The factor groups G_i/G_{i-1} for $1 \leq i \leq n$ are all simple (possibly of prime order), and the group G may be viewed as being built from these simple *composition factors.*

In Chapter 10, Isaacs, the Jordan-Hölder theorem is proven, which asserts that the composition factors of G are uniquely determined (up to isomorphism) and they are independent of the particular series S. Different composition series for G will yield composition factors that are isomorphic to those from S, although perhaps they occur in a different sequence.

We close this discussion of simple groups with the observation that there is a practical consequence of the fact that all finite groups are built from simple groups. Often, a theorem about

general finite groups can be proved by an appeal to the simple group classification. As an example of this technique, let us consider groups of order relatively prime to 15. From the classification, the following is true:

Proposition 2.49. *If S is a finite simple group, and $|S|$ is not divisible by 3 or 5, then $|S|$ is prime.*

Theorem 2.50. *Assume Proposition 2.49. Let $G > 1$ be a finite group with order relatively prime to 15. Then G has a nonidentity abelian normal subgroup.*

Proof. Let M be minimal normal in G. In other words, $1 < M \trianglelefteq G$, and there does not exist $K \trianglelefteq G$ with $1 < K < M$. (Note that the existence of M is assured by the finiteness of G.) Next, let N be maximal normal in M. By Theorem 2.43, the group M/N is simple. Since $|M/N|$ divides $|G|$, it is relatively prime to 15, and so, by Proposition 2.49, M/N has prime order. In particular, M/N is abelian, and hence, $M' \subseteq N$ by Theorem 2.45, and it follows that $M' < M$. Now $M' \operatorname{char} M \trianglelefteq G$, and thus $M' \trianglelefteq G$. It follows from the minimality of M that $M' = 1$, and thus, M is abelian, as desired. □

2.21 Group Actions

Although there are many advantages in moving from the older definitions of groups as permutation groups to the modern abstract axiomatic definition, there is also one significant potential disadvantage. With a permutation group one has the set being permuted, and this provides a tool for the study of the group. For instance, if the set has exactly n elements, then by Lagrange's theorem, we can conclude that the order of the group divides $|\operatorname{Sym}(n)| = n!$.

The idea behind the theory of group actions is to regain the advantages of working with permutation groups while continuing to deal with abstract groups. Actions provide techniques for producing subgroups and (especially important) normal subgroups. They can be used as an efficient counting tool to prove theorems about groups and to solve certain combinatorial problems involving symmetry.

Definition 2.51. Let G be a group, and Ω any nonempty set. Assume that for each $g \in G$, and $\omega \in \Omega$, there is defined a unique element $\omega \cdot g \in \Omega$. Suppose the following conditions hold:

(a.) $\omega \cdot 1 = \omega$ for all $\omega \in \Omega$ and

(b.) $(\omega \cdot g) \cdot h = \omega \cdot (gh)$ for all $\omega \in \Omega$ and $g, h \in G$.

Then we say that G *acts* on Ω or that $\cdot$ is an *action* of G on Ω.

The prototype examples of a group action are permutation groups. Let $\Omega \neq \emptyset$ and suppose $G \subseteq \operatorname{Sym}(\Omega)$. Then for $\alpha \in \Omega$ and $g \in G$, we can simply take $\alpha \cdot g = (\alpha)g$. (In other words, we simply evaluate the function g at α.) Condition (a) of Definition 2.51 is satisfied by the definition of the identity element of $\operatorname{Sym}(\Omega)$, and condition (b) is satisfied by the definition of multiplication in this group.

Example 2.52 (Trivial Action)**.** If G is any group, and $\Omega \neq \emptyset$ is arbitrary, we can define the *trivial action* of G on Ω by $\alpha \cdot g = \alpha$ for all $\alpha \in \Omega$, and $g \in G$. This rather uninteresting example demonstrates that an action need not be "faithful." (An action is *faithful* if the identity is the only element $g \in G$ such that $\alpha \cdot g = \alpha$ for all $\alpha \in \Omega$.) In general, the *kernel* of an action is the set of group elements that act like 1 and "fix" all $\alpha \in \Omega$. (We say g *fixes* α if $\alpha \cdot g = \alpha$.)

The most useful actions of finite groups are usually internal (in some sense) to the group. There are, for instance, two important ways in which a group G can act on itself. (In other words, we take $\Omega = G$.) The first of these is the *regular action* defined by $x \cdot g = xg$ for all $x \in G, g \in G$. (Note that in this case, condition (b) of Definition 2.51 is just the associative law.) The other important action of G on itself is the *conjugation action*, where we define $x \cdot g = x^g = g^{-1}xg$. The reader should verify that this is really an action. Observe that the regular action is faithful, and that $\mathbf{Z}(G)$ is the kernel of the conjugation action of G.

If $X \subseteq G$ is any subset and $g \in G$, then as usual, we define the product $Xg = \{xg \mid x \in X\}$. This can be used to define an action of G on the set of all subsets of G by setting $X \cdot g = Xg$. (Again, this reader should check that this is really an action. Typically, the verification that something is an action is utterly routine, and will be omitted.) If $H \subseteq G$ is a subgroup, take Ω to be the set $\{Hx \mid x \in G\}$ of all right cosets of H in G. If $X \in \Omega$, then also $Xg \in \Omega$, since $(Hx)g = H(xg)$, and thus right multiplication defines an action of G on Ω. (Note that in general neither of the following will define an action of G on the set of left cosets of H in G:

1. $(xH) \cdot g = xHg$
2. $(xH) \cdot g = (xg)H$.

We leave it to the reader to discover what goes wrong in each case.)

Lemma 2.53. *Let G act on Ω. For each $g \in G$, define $\pi_g \colon \Omega \mapsto \Omega$ by $(\alpha)\pi_g = \alpha \cdot g$. Then $\pi_g \in \mathrm{Sym}(\Omega)$ and the map $\theta \colon G \mapsto \mathrm{Sym}(\Omega)$ defined by $\theta(g) = \pi_g$ is a homomorphism whose kernel is equal to the kernel of the action.*

Proof. If $g, h \in G$, and $\alpha \in \Omega$, then

$$(\alpha)\pi_g\pi_h = (\alpha \cdot g)\pi_h = (\alpha \cdot g) \cdot h = \alpha \cdot (gh) = (\alpha)\pi_{gh},$$

and so $\pi_g\pi_h = \pi_{gh}$ for all $g, h \in G$. (Note that we used condition (b) from Definition 2.51.) Also, by condition (a),

$$(\alpha)\pi_1 = \alpha \cdot 1 = \alpha,$$

and so π_1 is the identity function i_Ω on Ω. Now for $g \in G$, we have

$$\pi_g\pi_{g^{-1}} = \pi_1 = \pi_{g^{-1}}\pi_g,$$

and therefore, π_1 is an element of $\mathrm{Sym}(\Omega)$ by Lemma 2.1(a) and (b). Now, we have $\theta(g)\theta(h) = \pi_g\pi_h = \pi_{gh} = \theta(gh)$, so θ is a homomorphism. An element $g \in G$ lies in $\ker(\theta)$ iff $\pi_g = i_\Omega$, and this is equivalent to saying that $\alpha \cdot g = \alpha$ for all $\alpha \in \Omega$; that is, g is in the kernel of the action. □

Corollary 2.53.1. *Let G act on Ω, and let K be the kernel of the action. Then $K \triangleleft G$ and G/K is isomorphic to a subgroup of* $\mathrm{Sym}(\Omega)$.

Proof. Let $\theta \colon G \mapsto \mathrm{Sym}(\Omega)$ be as in Lemma 2.53. Then $K = \ker(\theta) \triangleleft G$, and $G/K \cong \theta(G)$ by the Isomorphism theorem. □

In the search for simple groups, it is convenient to have nonsimplicity criteria in order to eliminate potential candidates and narrow the field. For this reason, we feel that any result that can be used to produce a nonidentity proper normal subgroup where one was not previously known to exist must be considered to be a good theorem. By this standard, the following is surely one of the most accessible good theorems.

Theorem 2.54. *Let $H \subseteq G$ with $|G : H| = n < \infty$. Then there exists $N \triangleleft G$ such that*

(a.) $N \subseteq H$ and

(b.) $|G : N|$ divides $n!$.

In particular, if $n > 1$ and $|G|$ does not divide $n!$, then G is not simple.

Proof. Let G act by right multiplication on the set $\Omega = \{Hx \mid x \in G\}$, and let N be the kernel of this action. By Corollary 2.53.1, $N \triangleleft G$ and G/N is isomorphically embedded in $\mathrm{Sym}(\Omega)$. Since $|\Omega| = n$, we have $|\mathrm{Sym}(\Omega)| = n!$, and by Lagrange, $|G : N| = |G/N|$ divides $n!$.

To see that $N \subseteq H$, observe that if $x \in N$, then since $H \in \Omega$, we have

$$x \in Hx = H \cdot x = H,$$

where the last equality holds by the definition of the kernel of an action. For the last statement, it suffices to show that $1 < N < G$. Since $n > 1$ we have $H < G$ and so $N < G$ by property (a). Finally, if $N = 1$, then $|G| = |G : N|$ divides $n!$, and so this contradiction proves $N > 1$. □

To use Theorem 2.54 as a nonsimplicity criterion, we need some way to find subgroups $H \subseteq G$ with relatively small indices. So far, we have not seen much that can be used for this purpose, but in the next chapter, we shall obtain the Sylow theorems; these provide some very powerful techniques for finding subgroups of finite groups and keeping control over their indices.

Corollary 2.54.1. *Let $H \subseteq G$, where G is finite, and $|G : H| = p$ is the smallest prime divisor of $|G|$. Then $H \triangleleft G$.*

Proof. Let $N \triangleleft G$ be as in Theorem 2.54. We have $N \subseteq H$ and we write $|H : N| = m$. Therefore, $|G : N| = |G : H||H : N| = pm$, and by Theorem 2.54, this must divide $p! = p(p-1)!$. It follows that m divides $(p-1)!$, and so every prime divisor q of m satisfies $q \leq (p-1)$. By Lagrange's theorem, however, q divides $|G|$, and this contradicts the assumption on p. We conclude that q cannot exist, and so $m = 1$. This yields $H = N \triangleleft G$. □

Theorem 2.54 remains valid even if G is infinite, provided that $|G : H| < \infty$.

Corollary 2.54.2. *Let $H \subseteq G$ have finite index. Then there exists a normal subgroup N of finite index with $N \subseteq H$.*

Corollary 2.54.2 can sometimes be used to convert problems about infinite groups into the corresponding finite group problem. If G is finite, for instance, and $U \subseteq V \subseteq G$, then it is immediate by Lagrange that $|G : U| = |G : V||V : U|$. Suppose now that G is infinite but that $|G : U| < \infty$, with $U \subseteq V \subseteq G$ as before. It is still true that $|G : U| = |G : V||V : U|$. To see this, apply Corollary 2.54.2 to obtain $N \triangleleft G$ of finite index with $N \subseteq U$. Write $\overline{G} = G/N$, and let $\overline{U}$ and $\overline{V}$ denote the images of U and V under the canonical homomorphism $G \mapsto \overline{G}$. Since $\overline{G}$ is finite, we have $|\overline{G} : \overline{U}| = |\overline{G} : \overline{V}||\overline{V} : \overline{U}|$. However, $|\overline{G} : \overline{U}| = |G : U|$ by the Correspondence theorem. Our desired equality quickly follows.

2.21.1 Normal Subgroups and Group Action

We present a result that gives some more precise information about the normal subgroup N.

Theorem 2.55. *Let $H \subseteq G$ and let N be the kernel of the action of G on the right cosets of H (by right multiplication). Then*

(a.) $N = \bigcap_{x \in G} H^x$ *and*

(b.) if $M \triangleleft G$ *with* $M \subseteq H$*, then* $M \subseteq N$*.*

Proof. Let $x, g \in G$. Then $(Hx) \cdot g = Hx$ iff $Hxg = Hx$, and this happens iff $xg \in Hx$. Thus, g fixes Hx iff $g \in x^{-1}Hx = H^x$. It follows that the kernel of the action is precisely the set of elements that lie in every one of the conjugates of H, and this proves property (a).

Now let M be as in (b). For $x \in G$, we have $M = M^x \subseteq H^x$, and thus,

$$M \subseteq \bigcap_{x \in G} H^x = n,$$

as claimed. □

In the situation of Theorem 2.55, the normal subgroup N is the largest normal subgroup of G contained in H. It is called the *core* of H in G, and we write $N = \mathrm{core}_G(H)$.

2.22 Stabilizers

Group actions can also be used to produce subgroups that are not necessarily normal. If G acts on Ω, and $\alpha \in \Omega$, we write

$$G_\alpha = \{g \in G \mid \alpha \cdot g = \alpha\}.$$

This is called the *stabilizer* of α in G, and it is routine to check that G_α is always a subgroup of G.

Example 2.56. Let G act via conjugation on the set of all subsets of G. If X is one of these subsets, then $G_X = \mathbf{N}_G(X)$, the normalizer of X. Some authors call G_X the *setwise* stabilizer of X to distinguish it from $\mathbf{C}_G(X)$, which they call the *pointwise* stabilizer of X.

Example 2.57. Let G act by right multiplication on the set of right cosets of $H \subseteq G$ in G. Then as we saw in the proof of Theorem 2.55, the stabilizer of the coset Hx is the conjugate H^x, and in particular, H is its own stabilizer in this action.

2.23 Transitivity and Orbit

We return to the general case of a group G acting on a set Ω. We say that the action is *transitive* if for every two elements $\alpha, \beta \in \Omega$, there exists an element $g \in G$ with $\alpha \cdot g = \beta$. For instance, the regular action of G and the usual action on the right cosets of a subgroup are transitive. In general, the conjugation action G on itself is not transitive, since if $x, y \in G$ have different orders, then there can exist no $g \in G$ with $x^g = y$. (Recall that conjugation by g defines an automorphism, and so it preserves the orders of elements.) In general, if G acts on Ω, then the *orbits* of this action are the sets of the form $\{\alpha \cdot g \mid g \in G\} \subseteq \Omega$.

Lemma 2.58. *Let* G *act on* Ω*. Then the orbits partition* Ω*. This means*

(a.) Ω *is the union of the orbits and*

(b.) any two different orbits are disjoint.

Proof. Write $\mathcal{O}_\alpha = \{\alpha \cdot g \mid g \in G\}$. Since $\alpha \cdot 1 = \alpha$, we have $\alpha \in \mathcal{O}_\alpha$, and thus

$$\Omega = \bigcup_{\alpha \in \Omega} \mathcal{O}_\alpha,$$

proving part (a). We show now that if $\gamma \in \mathcal{O}_\alpha$, then $\mathcal{O}_\gamma = \mathcal{O}_\alpha$. We have $\gamma = \alpha \cdot x$ for some $x \in G$, and thus

$$\gamma \cdot g = (\alpha \cdot x) \cdot g = \alpha \cdot xg \in \mathcal{O}_\alpha.$$

This yields $\mathcal{O}_\gamma \subseteq \mathcal{O}_\alpha$. Also, $\alpha = \gamma \cdot x^{-1}$, and so $\alpha \in \mathcal{O}_\gamma$, and hence the above argument yields $\mathcal{O}_\alpha \subseteq \mathcal{O}_\gamma$. We have shown $\mathcal{O}_\alpha = \mathcal{O}_\gamma$ as claimed. Finally, if $\mathcal{O}_\alpha \cap \mathcal{O}_\beta \neq \emptyset$, choose $\gamma \in \mathcal{O}_\alpha \cap \mathcal{O}_\beta$, then $\mathcal{O}_\alpha = \mathcal{O}_\gamma = \mathcal{O}_\beta$, and part (b) is proved. □

The partition of Ω by the orbits of an action is analogous to the partition of a group by the cosets of a subgroup. This is not entirely accidental, since if $H \subseteq G$, we can let H act on G by right multiplication. In this case, the orbit containing $g \in G$ is exactly the left coset gH. (The reader should try to find an action of H on G whose orbits are the right cosets of H.)

An important example of the partition of a set into orbits with respect to an action occurs in the conjugation action of a group on itself. In that case, the orbits are called *conjugacy classes*. Note that the class (i.e. conjugacy class) of an element $x \in G$ consists of the element x alone iff $x \in \mathbf{X}(G)$.

Example 2.59. The reader should check that the classes of D_8, the group of symmetries of a square, are the following. Each of the identity and the 180° rotation constitutes an entire clas. The ±90° rotations form a class, the two diagonal flips form a class, and the horizontal and vertical flips form a class. This gives a total of five classes for D_8.

The phrase "conjugacy class" is also sometimes applied to an orbit of the conjugacy action of G on its set of subgroups, and so one must examine the context to be certain of the meaning. Usually, if a class of subgroups is intended, this is stated explicitly.

2.23.1 Orbit Stabilizer Theorem

Theorem 2.60. *Let G act on Ω and let $\mathcal{O}$ be an orbit of this action. Let $\alpha \in \mathcal{O}$ and write $H = G_\alpha$, the stabilizer. Then there exists a bijection $\mathcal{O} \leftrightarrow \{Hx \mid x \in G\}$.*

Since we didn't really learn group action in class, I omit this proof for time sake.

2.24 Direct Product

Note. This is Chapter 7, Isaacs. In this chapter, we discuss two techniques for constructing groups. The simpler and more important of these is the direct product, often also called the "direct sum." Although we present direct products in the context of group theory, analogous constructions occur throughout algebra. We also consider the semidirect product, which is relevant only to group theory.

Let H_1, H_2 be arbitrary groups. We can put the structure of a group on the set $H_1 \times H_2$ of ordered pairs of elements (x_1, x_2) with $x_i \in H_1$ by setting

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2).$$

It is trivial to check that $H_1 \times H_2$ is a group, and this is called the *external direct product* of the H_i. If the operations in H_i are written additively rather than multiplicatively, it is common to call G

the *external direct sum* of the H_i, and to write $G = H_1 \oplus H_2$. It should be clear that $\mathbb{C}^+ \cong \mathbb{R}^+ \oplus \mathbb{R}^+$, where $\mathbb{C}^+$ and $\mathbb{R}^+$ are the additive groups of complex and real numbers.

If $G = H \times K$, we can define subgroups $\overline{H}, \overline{K} \subseteq G$ by setting $\overline{H} = \{(h, 1) \mid h \in H\}$ and $\overline{K} = \{(1, k) \mid k \in K\}$. It should be obvious that $H \cong \overline{H}$ and $K \cong K$, and that $\overline{HK} = G$ and $\overline{H} \cap \overline{K} = 1$.

Another observation is that $\overline{H}$ and $\overline{K}$ centralize each other, and therefore, $\overline{H} \triangleleft G$ and $\overline{K} \triangleleft G$. In general, if G is any group having two normal subgroups M and N with $MN = G$, and $M \cap N = 1$, we say G is the *internal direct product* of its subgroups M and N, and in this situation we write

$$G = M \dot{\times} N.$$

The additive version of this notation is

$$A = U \dot{+} V,$$

where A is an abelian group, and $U, V \subseteq A$ with $U + V = A$, and $U \cap V = 0$. In this case, we say A is the *internal direct sum* of the subgroups U and V.

Lemma 2.61. *Let M and N be normal in G with $M \cap N = 1$. Then $mn = nm$ for all $m \in M$ and $n \in N$.*

Proof. We compute the commutator $[m, n] = m^{-1}n^{-1}mn$. Since $m^n \in M$, we have $m^{-1}m^n \in M$, and since $(n^{-1})^m \in N$, we have $(n^{-1})^m n \in N$. Therefore, $[m, n] \in M \cap N = 1$. □

Lemma 2.62. *If $G = H \times K$, then $G = \overline{H} \dot{\times} \overline{K}$. Also, if $\Gamma = M \dot{\times} N$, then $\Gamma \cong M \times N$.*

Proof. We have already observed that $G = \overline{HK}$ and $\overline{H} \cap \overline{K} = 1$, and that $\overline{H} \triangleleft G$, and $\overline{K} \triangleleft G$. This proves the first assertion. To prove the second, note that $mn = nm$ for $m \in M$ and $n \in N$. Map $\theta M \times N \mapsto \Gamma$ by $\theta(m, n) = mn$. We have

$$\theta((m, n)(m', n')) = \theta(mm', nn') = mm'nn' = mnm'n' = \theta(m, n)\theta(m', n'),$$

so θ is a homomorphism. Since $MN = \Gamma$, we see that θ is surjective. Also, if $(m, n) \in \ker \theta$, so that $mn = 1$, we have $m = n^{-1} \in M \cap N = 1$, and hence, $(m, n) = (1, 1) = 1$. The proof is now complete. □

Lemma 2.63. *If $G = M \dot{\times} N$, then $M \cong G/N$ and $N \cong G/M$.*

Proof. We have $G/N = MN/N \cong M/(M \cap N) = M$. The isomorphism $G/M \cong N$ follows similarly. □

Corollary 2.63.1. *If $G = M \dot{\times} N = M \dot{\times} L$, then $N \cong L$.*

In general, there is no such cancellation property that works for isomorphisms of external direct products. It is possible that $M \times N \cong M \times L$, and yet $N \ncong L$. Believe it or not, It follows that if we write 0 to denote the trivial group, we have $\mathbb{R}^+ \oplus 0 \cong \mathbb{R}^+ \cong \mathbb{R}^+ \oplus \mathbb{R}^+$, and so cancellation fails.

To see why $\mathbb{R}^+ \cong \mathbb{R}^+ \oplus \mathbb{R}^+$, we must appeal to a bit of transfinite linear algebra. Each of these objects may be viewed as a vector space over $\mathbb{Q}$, and in both cases, the dimensions are equal to the cardinality of the continuum. Any bijection between bases for these two spaces extends to a linear transformation that is a vector space isomorphism, and hence is an isomorphism of abelian groups.

We can extend the notions of direct product (both internal and external) to situations where there are more than two factors. Let $\{H_\alpha \mid \alpha \in I\}$ be any indexed collection of groups, where the index set I may be finite or infinite. It is convenient to replace the notion of an ordered pair or

ordered n-tuple by a function f from the index set I into the union $\bigcup H_\alpha$ with the condition that $f(\alpha) = H_\alpha$ for all $\alpha \in I$. Let Γ be the collection of all such functions. Then Γ becomes a group under the operation that defines fg to be the function satisfying $(fg)(\alpha) = f(\alpha)g(\alpha)$. (Note that in the case $I = \{1, 2\}$, we see that $\Gamma = H_1 \times H_2$ if we identify the pair (x_1, x_2) with the function $1 \mapsto x_1, 2 \mapsto x_2$.) We write

$$\Gamma = \bigtimes_{\alpha \in I} H_\alpha$$

and call Γ the *unrestricted external direct product* of the H_α. As in the case where $|I| = 2$, we define $\overline{H}_\alpha \subseteq \Gamma$ by

$$\overline{H}_\alpha = \{f \in \Gamma \mid f(\beta) = 1 \text{ whenever } \alpha \neq \beta \in I\}.$$

If $|I| < \infty$, then Γ is the group generated by the subgroups $\overline{H}_\alpha$, but this is not true when I is infinite. In that case, $\langle \overline{H}_\alpha \mid \alpha \in I \rangle$ is the group of those functions $f \in \Gamma$ that have nonidentity values for at most finitely many indices α. (This is so because one can only take finite products of elements in a group.) This subgroup of Γ, where the functions are restricted to having identity values "almost everywhere," is called the *restricted external direct product* of the H_α.

We are primarily concerned with the case where there are just finitely many factors. Then the restricted and unrestricted direct products coincide, and we need not distinguish them. We thus will use the "n-tuple" notation in place of functions. We write $(x_1, x_2, \ldots, x_n)$ to denote the element of $\bigtimes H_i$ corresponding to the function $f\colon i \mapsto x_i$.

It is easy to see that if $M, N \triangleleft G$, then $G = M\dot{\times}N$ iff every element of G is uniquely of the form $g = mn$ with $m \in M$ and $n \in N$. We will prove this soon. The definition of an internal direct product can be extended to the case where there may be more than two factors by means of this alternative characterization. Let $M_i \triangleleft G$ for $1 \leq i \leq n$, and suppose $G = M_1 M_2 \cdot M_n = \prod_{i=1}^n M_i$. We say that this product is *direct* or that G is the *internal direct product* of the subgroups M_i provided that for every $g \in G$, there is a unique choice of element $x_i \in M_i$ such that $g = x_1 x_2 \cdots x_n$. We write

$$G = \dot{\prod_{i=1}^{n}} M_i$$

in this case, using the dot to signify the uniqueness.

Theorem 2.64. *Let $M_i \triangleleft G$ for $1 \leq i \leq n$ and assume $\prod M_i = G$. Then the following are equivalent:*

(a). $\dot{\prod} M_i = G$.

(b). For each i, $M_i \cap \prod_{j \neq i} M_j = 1$.

(c). For $2 \leq i \leq n$, $M_i \cap \prod_{j=1}^{i-1} M_i = 1$.

Note that condition (b) depends only on the set of subgroups M_i, and not on their numbering, and so the order in which the M_i appear is irrelevant to the question of the directness of the product. Condition (c) is usually easier to check than (b), and often is easier with some orderings of M_i than with others. It is important to remember that the condition $M_i \cap M_j = 1$ for $j \neq i$ is not sufficient to prove directness when $n > 2$, but it is a consequence of directness.

Proof of Theorem 2.64. Assume condition (a), and suppose $g \in M_i \cap \prod_{j \neq i} M_j$ for some particular subscript i. Since $g \in \prod_{j \neq i} M_j$, we may write $g = x_1 x_2 \cdots x_n$ for suitable elements $x_j \in M_j$, where $x_i = 1$. Since $g \in M_i$, however, we can also write $g = y_1 y_2 \cdots y_n$, with $y_j \in M_j$, by setting

$y_j = 1$ for $j \neq i$, and $y_i = g$. The uniqueness of $\prod$ implies that $x_j = y_j$ for all j. In particular, $1 = x_i = y_i = g$, and (b) is proved.

If we assume (b), then (c) follows trivially. Hence, we assume (c) and prove (a). Given $g \in G = \prod M_i$, we can certainly write $g = x_1 x_2 \cdots x_n$ with $x_i \in M_i$. Suppose also $g = y_1 y_2 \cdots y_n$ with $y_i \in M_i$. To establish (a) we need to show that $x_i = y_i$ for all i. Suppose this is false, and let i be the largest index such that $x_i \neq y_i$. If $i < n$, cancel $x_{i+1} \cdots x_n = y_{i+1} \cdots y_n$ from the two expressions for g so that in any case we get

$$x_1 x_2 \cdots x_i = y_2 y_2 \cdots y_i.$$

Then

$$1 \neq x_i y_i^{-1} = (x_1 x_2 \cdots x_{i-1})^{-1}(y_1 y_2 \cdots y_{i-1}) \in M_i \cap \prod_{j=1}^{i-1} M_j,$$

and this contradicts (c). □

We extend Lemma 2.62 to the case of more than two subgroups.

Lemma 2.65. *Let $G = \prod_{i=1}^n N_i$. Then $G \cong \bigtimes_{i=1}^n N_i$.*

Proof. Let $E = \bigtimes_{i=1}^N N_i$ and map $\theta \colon E \to G$ by

$$\theta((x_1, x_2, \ldots, x_n)) = x_1 x_2 \cdots x_n.$$

Then θ is surjective since $G = \prod N_i$ and it is injective since the product is direct. Let us show θ is a homomorphism. Let $f = (x_1, \ldots, x_n)$ and $g = (y_1, \ldots, y_n)$ be elements of E, and compute

$$\theta(fg) = x_1 y_1 x_2 y_2 \cdots x_n y_n.$$

Now x_i, y_i commute if $i > j$ since $N_i, N_j \triangleleft G$, and $N_i \cap N_j = 1$. We can therefore move x_i to the left in the above product, passing over y_j with $j < i$. Our desired result follows. □

I won't include the proof of this next lemma. It is not entirely trivial however.

Lemma 2.66. *Suppose that $G = \prod_{i=1}^n N_i$. Then $Z(G) = \prod_{i=1} Z(N_i)$.*

We don't learn minimal normal subgroups in class, so I will only include this statement as well.

Theorem 2.67. *Let N be a finite minimal normal subgroup of G. Then there exist subgroups $S_i \subseteq N$ such that*

(a). $N = \prod S_i$,

(b). each S_i is simple, and

(c). the S_i are all G-conjugate.

(d). If N is nonabelian, then the S_i constitute a full G-conjugacy class of subgroups.

Isaacs now covers nilpotent groups, which is left to MATH845. I will just include the definition of nilpotence.

Definition 2.68. A finite group G is said to be *nilpotent* if for every prime p, a Sylow p-subgroup of G is normal, or equivalently, is unique. Finite abelian groups and finite p-groups are nilpotent.

2.25 Fundamental Theorem of Finite Abelian Groups

Theorem 2.69 (Fundamental, of abelian groups)**.** *Let G be finite and abelian. Then*

$$\prod_{i=1}^{n}\cdot C_i,$$

where C_i are subgroups that are cyclic p-groups for various primes p.

First, we need a general lemma.

Lemma 2.70. *Let $G = \prod_{i=1}^{n} N_i$, and suppose each N_i decomposes as a direct product*

$$N_i = \prod_{j=1}^{m_i}\cdot M_{ij}.$$

Then

$$G = \prod_{i,j}\cdot M_{ij}.$$

Proof. It should be clear that $G = \prod M_{ij}$. Since the different N_i centralize each other, we see that each $M_{ij} \triangleleft G$, and so it suffices to show that if $\prod x_{ij} = \prod y_{ij}$ with $x_{ij}, y_{ij} \in M_{ij}$, then $x_{ij} = y_{ij}$ for all i, j. To see this, write

$$u_i = \prod_j x_{ij}$$

and

$$v_i = \prod_j y_{ij}.$$

Then $\prod u_i = \prod v_i$ and hence $u_i = v_i$ for all i by the directness of $\prod N_i$. For each i, then, $\prod_j x_{ij} = \prod_j y_{ij}$ and so $x_{ij} = y_{ij}$ for all j by the directness of $\prod_j M_{ij}$. □

The following is the key step in the proof of the Fundamental theorem of abelian groups.

Theorem 2.71. *Let G be a finite abelian p-group and let $C \subseteq G$ be a cyclic subgroup with maximum possible order. Then $G = C\dot{\times}B$ for some subgroup $B \subseteq G$.*

Proof. Since we can take $B = 1$ if $C = G$, we can assume $C \subset G$, and we choose $x \in G \setminus C$ of smallest possible order. Since $x \neq 1$, we see that $o(x^p) < o(x)$, hence $x^p \in C$. If x^p generates C, then $|\langle x\rangle| = p|C|$ and this contradicts the choice of C. Therefore, x^p is a nongenerator of the cyclic p-group C and it follows that x^p is a pth power in C, and we can write $x^p = y^p$ for some $y \in C$. Now $xy^{-1} \notin C$, and $(xy^{-1})^p = x^p(y^p)^{-1} = 1$. By the choice of x, we have $o(x) \leq o(xy^{-1}) = p$, and so $o(x) = p$.

Now let $X = \langle x\rangle$, and use overbars to denote the canonical homomorphism $G \to G/X = \overline{G}$. Since $|X| = p$, we have $C \cap X = 1$, and the map - is an isomorphism from C to $\overline{C}$. Thus $\overline{C}$ is cyclic with order equal to $|C|$. If $\overline{G}$ has a cyclic subgroup $\langle\overline{g}\rangle$ with order larger than $|C|$, then

$$|\langle g\rangle| = o(g) \geq o(\overline{g}) = |\langle\overline{g}\rangle| > |\overline{C}| = |C|,$$

and this contradicts the choice of C. It follows that $\overline{C}$ is a cyclic subgroup of maximum possible order in $\overline{G}$. Since $|\overline{G}| < |G|$, we may work by induction on $|G|$ and conclude that $\overline{C}$ is a direct factor of $\overline{G}$. Since every subgroup of $\overline{G}$ has the form $\overline{B}$ for some $B \subseteq G$ and $B \supseteq X$, we can find $B \supseteq X$ such that $\overline{G} = \overline{C}\dot{\times}\overline{B}$ Thus, $\overline{G} = \overline{C}\ \overline{B} = \overline{CB}$ and hence $CB = G$. Also, $\overline{C} \cap \overline{B} = \overline{1}$, and so $C \cap B \subseteq X$. Then $C \cap B \subseteq C \cap X = 1$. This proves $G = C\dot{\times}B$ as required. □

Proof of Theorem 2.69. Work by induction on $|G|$. If we can write $G = A \dot{\times} B$ with $A < G$, and $B < G$, then each of A and B is a direct product of cyclic p-groups by the inductive hypothesis, and the theorem holds by Lemma 2.70.

We may therefore assume that G is directly indecomposable. Since G is nilpotent, G must be a p-group. We conclude that G itself is cyclic. □

Corollary 2.71.1. *Every finite abelian group is isomorphic to an external direct product of cyclic p-groups.*

3 Lecture 1: Mon. Feb 5. 2024

3.1 The Dihedral Group: Isaacs 3A

Example 3.1 (The Dihedral Group)**.** Consider action on the regular 4-gon; label its vertices $1, \ldots, 4$. We want to find all of the transformations which preserve the relative distance and the shape of the square.

It turns out that there are two types of transformations which we may perform on the square: rotation and reflection. Define r to be rotation of the square by $\pi/2$ radians, such that r^2 is a rotation by π, and r^3 is a rotation by $3\pi/2$.

Define s to be vertical reflection. We claim there are exactly 8 transformations of the square. Let D_8 be the set of all transformations of the square such that

$$D_8 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s.\}$$

Claim. D_8 is a group.

Proof. Recall that a group has an associative binary operation, an identity element, and for each element of the group, there exists the inverse of that element. Let us define our binary operation as the composition of transformations. Suppose $x_1, x_2, x_3 \in D_8$, ...

We let e be our identity element, that is, the square with no transformations. For the inverse of rotation, ... □

3.2 Fundamental Relation

It follows that $s^{-1}rs = r^{-1}$. We may rewrite D_8 as

$$D_8 = \langle r, s \mid r^4 = 1, s^2 = 1, s^{-1}rs = r^{-1}.\rangle$$

Note. See Keith Conrad's writeup on the Dihedral Groups.

3.3 Group Homomorphisms

Definition 3.2. Let G, H be two groups. The mapping $\phi\colon G \mapsto H$ is a homomorphism if $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$.

Definition 3.3. The kernel of ϕ, $\ker\phi$, is the subgroup

$$\ker\phi = \{g \in G \mid \phi(g) = e_H\}.$$

Example 3.4 (Trivial Homomorphism)**.** Map all elements of G to the identity in H.

Example 3.5 (Group of Real Symmetric Matrices)**.** Let $(\operatorname{Sym}\operatorname{Mat}_n(\mathbb{R}), +)$ be the group of $n \times n$ real symmetric matrices with matrix addition. Consider the group homomorphism

$$\operatorname{tr}(\operatorname{Sym}\operatorname{Mat}_n(\mathbb{R})) \mapsto \mathbb{R}.$$

Note that $\ker \operatorname{tr}$ is equal to all the $n \times n$ real symmetric matrices whose eigenvalues sum to 0.

Lemma 3.6 (Properties of Group Homomorphism)**.** *Let $\phi\colon G \mapsto H$ be a group homomorphism. TFAE:*

1. $\phi(E_G) = E_H$,
2. $\ker(\phi) \triangleleft G$,
3. $\phi(a) = \phi(b)$ *iff.* $a(\ker \phi) = b(\ker \phi)$,
4. *If $g \in G$ satisfies $\phi(g) = h$, then* $(\ker \phi)g = \{a \in G \mid \phi(a) = h\}$.

3.4 Group Isomorphism and Automorphism

Definition 3.7. A group homomorphism $\phi\colon G \mapsto H$ is called an isomorphism if ϕ is bijective.

Definition 3.8. An isomorphism $\phi\colon G \mapsto H$ is called an automorphism if $G = H$.

Example 3.9 (Isomorphisms of Cyclic Groups)**.** Let $C_n = \langle g \rangle$, and suppose n is odd. Define $\phi\colon C_n \mapsto C_n$, such that $\phi(g) = g^2$. We claim that ϕ is an homomorphism, and that it is bijective, and therefore, an isomorphism. Finally, it follows that it is an automorphism.

Exercise 3.1. Determine all the homomorphisms and isomorphisms of C_n.

3.5 Normal Subgroups

Definition 3.10 (Canonical Projection)**.** For any $N \triangleleft G$, the canonical projection w.r.t. N is the group homomorphism $\phi\colon G \mapsto G/N$, and $\phi(g) = gN$, for $g \in G$. Clearly, $\ker \phi = N$.

Theorem 3.11 (Normal Subgroups and Kernels)**.** *Let G be any group. The normal subgroups of G are precisely the kernels of all homomorphisms defined on G.*

Proof. Suppose we had a normal subgroup $N \triangleleft G$... □

3.6 The Isomorphism Theorems (I)

Theorem 3.12 (First Isomorphism Theorem)**.** *If $\phi\colon G \mapsto H$ is a homomorphism, then we have the following:*

1. $\ker \phi \triangleleft G$,
2. $\operatorname{Im} \phi = \{\phi(g) \mid g \in G\} < H$,
3. $G/\ker \phi \cong \operatorname{Im} \phi$.

4 Lecture 2: Wed. Feb. 7, 2024

4.1 The Isomorphism Theorems (II): Isaacs 3A

Theorem 4.1 (Second Isomophism Theorem)**.** *If $H < G$ and $N \triangleleft G$, then $N \cap H \triangleleft H$, and $H/N \cap H \cong NH/N$.*

Sketch of proof. Find $\phi_N \colon G \mapsto G/N$. Restrict ϕ_N to H. Show $\mathrm{Im}(\phi_N \mid H) = NH/N \leq G/N$. Show $\ker(\phi_N \mid H) = N \cap H$. □

4.2 Correspondence Theorem

Lemma 4.2 (Relations Between Subgroups Under Homomorphism)**.** *Let $\phi \colon G \mapsto H$ be a homomorphism. The following holds:*

1. *if $U \leq G$, then $\phi(U) \leq H$,*
2. *if $V \leq H$, then $\ker \phi \leq \phi^{-1}(V) \leq G$, where $\phi^{-1}(v) = \{g \in G \mid \phi(G) \in V\}$.*

Theorem 4.3 (Correspondence Theorem)**.** *Let $N \triangleleft G$. The canonical projection $\phi \colon G \mapsto G/N$ defines a one-to-one correspondence between two sets S and T, where $S = \{U \mid N \leq U \leq G\}$, and $T = \{V \mid V \leq G/N\}$.*

Part Two, Correspondence Theorem. Furthermore, the correspondence preserves containment, normality, factor groups, and indices. For $U_1, U_2 \leq G$ satisfying $N \leq U_1, N \leq U_2$, set $V_1 = \phi(U_1), V_2 = \phi(U_2)$. For containment, $U_1 \leq U_2$ if and only if $V_1 \leq V_2$. For normality and factor groups, $U_1 \triangleleft U_2$ if and only if $B_1 \triangleleft V_2$. In this case, $U_1/U_2 \cong V_2/V_1$. For indices, if $U_1 \leq U_2$, *i.e.* $V_1 \leq V_2$, then the indices $[U_2 \colon U_1] = [V_2 \colon V_1]$.

Outline of proof. (a): Show there is a bijection between S and T using ϕ, ϕ^{-1}, by showing $\phi^{-1}\phi$ is an identity mapping from S to itself. (b): Show that $\phi\phi^{-1}$ is an identity mapping from T to itself.

We will prove (a). We want to show that for each $N \leq U \leq G$, $\phi^{-1}\phi(U) = U$. By definition, $U \leq \phi^{-1}\phi(U)$ (as $\phi^{-1}\phi = \{g \in G \mid \phi(g) \in \phi(U)\}$). To show $\phi^{-1}\phi(U) \leq U$, take $g \in \phi^{-1}\phi(U)$... □

Proof of Normality and Factor Groups Preservation. We want to prove that $U_1 \triangleleft U_2$ if and only if $V_1 \triangleleft V_2$. We will prove the forward implication, and it suffices to show $(gN)^{-1}V_1(gN) = V_1$ for each $gN \in V_2$. Choose an arbitrary $gN \in V_2$, consider

$$\begin{aligned}(gN)^{-1}V_1gN &= \phi(g)^{-1}\phi(U_1)\phi(g) \\ &= \phi(g^{-1}U_1g)\end{aligned}$$

Because $\phi(g) = gN \in V_2, g \in \phi^{-1}(V_2) = U_2$. We have

$$\begin{aligned}\phi(g^{-1}U_1g) &= \phi(U_1) \\ &= V_1.\end{aligned}$$

□

Corollary 4.3.1 (Subgroup of Quotient Group)**.** *Let $N \triangleleft G$. Every subgroup of G/N must be of the form H/N for some unique subgroup $H \leq G$ such that $N \leq H$.*

4.2.1 Generalized Correspondence Theorem

The correspondence theorem holds true for any homomorphism $\phi\colon G \mapsto H$; replace N with $\ker\phi$.

4.3 The Isomorphism Theorems (III)

Theorem 4.4. *If $N \triangleleft G$ and $N < H \triangleleft G$, then $H/N \triangleleft G/N$,$G/H \cong (G/N)/(H/N)$. If G is finite, $[G\colon H] = [G/N\colon H/N]$.*

4.4 Applications of Isomorphism Theorems

Claim. Any cyclic group is isomorphic to $(\mathbb{Z}_n, +)$ for some $n \in \mathbb{Z}_+$, or to $(\mathbb{Z}, +)$.

Definition 4.5 (Simple Group)**.** A group G is simple if G has no *proper* normal subgroups.

Example 4.6. Consider C_p, for prime p, is simple.

Example 4.7. The alternating group A_n, for $n \geq 5$ is simple.

4.5 The Decomposition of a Finite Group

4.5.1 Maximal Subgroup, Maximal Normal Subgroup

Definition 4.8 (Maximal Subgroup, Maximal Normal Subgroup)**.** The subgroup M is a maximal subgroup of G if for each $M \leq H \leq G$, either $H = M$ or $H = G$. The subgroup M is a maximal normal subgroup of G if for each $M \leq H \trianglelefteq G$, either $H = M$ or $H = G$.

Example 4.9 (Dihedral Groups)**.** Recall $D_8 = \langle r, s \mid r^4 = s^2 = 1, s^{-1}rs = r^{-1}\rangle$. We claim $H = \langle r^2, s\rangle$ is a maximal subgroup of D_8 and a maximal normal subgroup of D_8.

Lemma 4.10 (Maximal Normal Subgroup and Simple Group)**.** *If N is a maximal normal subgroup of G, then G/N is simple.*

Sketch of proof. Use correspondence theorem. □

4.5.2 Decomposition of a Finite Group

Assume K_1 is a maximal normal subgroup of G. We may decompose G into two subgroups, $K_1, G/K_1$. Assume K_2 is a maximal subgroup of K_1, $K_2, K_1/K_2$. This is sometimes known as a composition series;

$$G \triangleleft H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_n = \{1\}.$$

5 Lecture 3: Mon. Feb. 12. 2024

5.1 Automorphism

Recall that if $\phi\colon G \mapsto G$ is a homomorphism, then ϕ is an automorphism.

Definition 5.1 (Automorphism Groups)**.** Let G be a group. The set of all automorphisms of G denote $\mathrm{Aut}(G)$ forms a group.

Sketch of proof. Properly define the operation on $\mathrm{Aut}(G)$. Naturally, this should be the composition of permutations. For $\sigma_1, \sigma_2 \in \mathrm{Aut}(G)$, define $\sigma_1 \circ \sigma_2$ to be a mapping satisfying $(\sigma_1 \circ \sigma_2)(x) = \sigma_2(\sigma_1(x))$, for $x \in G$. Prove the group axioms:

1. closure under composition: $\sigma_1 \circ \sigma_2 \in \mathrm{Aut}(G)$,
2. $id \in \mathrm{Aut}(G)$ (left, right),
3. associativity,
4. closure under inverse.

□

Lemma 5.2 (Automorphism Group of Cyclic Groups)**.** *If $G = C_n$, then $\mathrm{Aut}(G) \cong U_n$, where U_n are the integers modulo n and coprime to n with multiplication being the operation in U_n.*

Proof. Let $G = \langle g \rangle$. For each element $\sigma \in \mathrm{Aut}(G)$, $\sigma(g^j) = \sigma(g)^j$, thus σ is completely determined by $\sigma(g)$. Define $\sigma_i \in \mathrm{Aut}(g)$ such that $\sigma_i(g) = g^i$. We know $\sigma_i \in \mathrm{Aut}(G)$, and $\sigma_i(G) = G = \langle \sigma_i(g) \rangle = \langle g^i \rangle$. Therefore, $o(g^i) = n$, hence, i, n must be coprime. Therefore,

$$\mathrm{Aut}(G) = \{\sigma_i \mid 0 \leq i \leq n-1, \gcd(i,n) = 1\}.$$

To show that $U_n \cong \mathrm{Aut}(G)$, we use the bijection $\phi \colon U_n \mapsto \mathrm{Aut}(g)$, where $\phi(i) = \sigma_i$.

From here, it is not difficult to see that ϕ is a surjective group homomorphism. Then from the first isomorphism theorem, we know $U_n / \ker \phi \cong \mathrm{Aut}(G)$. □

5.2 Subgroup of Automorphism Group

We want to investigate the inner automorphism group.

Definition 5.3 (Inner Automorphism Group)**.** For $g \in G$, define the conjugation mapping $\tau_g \colon G \mapsto G$, such that $\tau_g(x) = g^{-1}xg$ for each $x \in G$. First, τ_g is an automorphism, that is, $\tau_g \in \mathrm{Aut}(G)$, and we call τ_g an inner automorphism. Second, $\mathrm{Inn}(G) = \{\tau_g \mid g \in G\}$ is a group, furthermore, $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Closure of inner automorphism group. For $g, h \in G$, $\tau_g, \tau_h \in \mathrm{Inn}(G)$, we claim that $\tau_g \circ \tau_h \in \mathrm{Inn}(G)$. For each $x \in G$,

$$\begin{aligned}(\tau_g \circ \tau_h)(x) &= \tau_h(\tau_g(x)) \\ &= \tau_h(g^{-1}xg) \\ &= (gh)^{-1}x(gh) \\ &= \tau_{gh}(x).\end{aligned}$$

□

Example 5.4 (Inner Automorphism Group of Abelian Groups)**.** For G a group, G is abelian if and only if $\mathrm{Inn}(G) = \{id\}$.

Converse Implication. Suppose $\mathrm{Inn}(G) = \{id\}$. For each $g, x \in G$, we have

$$\begin{aligned}g^{-1}xg &= \tau_g(x) \\ &= id(x) \\ &= x \\ xg &= gx.\end{aligned}$$

□

We have established that $\text{Inn}(G) \leq \text{Aut}(G)$.

Proposition 5.5. *We claim that* $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$.

Proof. It suffices to show that for each $g \in G$, and $\sigma \in \text{Aut}(G)$, we have $\sigma^{-1} \circ \tau_g \circ \sigma \in \text{Inn(G)}$. For $x \in G$,

$$\begin{aligned}(\sigma^{-1} \circ \tau_g \circ \sigma)(x) &= \sigma(\tau_g(\sigma^{-1}(x))) \\ &= \sigma(g^{-1}\sigma^{-1}(x)g) \\ &= \sigma(g)^{-1}x\sigma(g) \\ &= \tau_{\sigma(g)}(x).\end{aligned}$$

□

Proposition 5.6. *We claim that* $N \trianglelefteq G$ *if and only if* $\tau(N) = N$*, for all* $\tau \in \text{Inn}(G)$.

To tackle this proposition, we need some new definitions.

5.3 Characteristic Subgroups

Definition 5.7 (Characteristic Subgroups)**.** Let $H < G$. Then H is a characteristic subgroup of G if for each $\sigma \in \text{Aut}(G)$, $\sigma(H) = H$.

We use $H \,\text{char}\, G$ to denote H is a characteristic subgroup of G.

Theorem 5.8 (Characteristic Subgroup Implies Normal Subgroup)**.** *If* $H \,\text{char}\, G$*, then* $H \triangleleft G$.

Example 5.9. Every subgroup of a finite cyclic group is characteristic.

Proof. Suppose H is a subgroup of G a cyclic group, and $\phi \in \text{Aut}(G)$. We want to show that $\phi(H) = H$. If G is a cyclic group, then the order of each subgroup of G is unique. Because $\phi \in \text{Aut}(G)$, then $|\phi(H)| = |H|$. Then $\phi(H) = H$. □

5.4 Applications of Characteristic Subgroups

Recall that normality is not transitive, that is $H \trianglelefteq G$, $K \trianglelefteq H$ does not generally imply that $K \trianglelefteq G$.

Theorem 5.10. *If* $K \,\text{char}\, H$*, and* $H \trianglelefteq G$*, then* $K \trianglelefteq G$.

Proof. Since $H \trianglelefteq G$, then $\sigma(H) = H$, for $\sigma \in \text{Inn}(G)$. Since $K \,\text{char}(H)$, we know that each $\phi(K) = K$, for each $\phi \in \text{Aut}(H)$, Consider $\phi = \sigma\big|_H \in \text{Aut}(H)$. Therefore, $\sigma\big|_H(K) = K = \sigma(K)$, since $K \subseteq H$. Therefore, $K \trianglelefteq G$. □

6 Lecture 4: Wed. Feb. 14, 2024

6.1 Permutations and Cycle Notation

A permutation on X (finite or infinite) is a bijection from X to itself. We claim the set of all permutations denoted $\text{Sym}(X)$ is a group under composition. If $|X| = n$, then $\text{Sym}(X)$ is typically denoted by S_n.

Example 6.1 (Representation of Permutations)**.** Consider $g \in S_8$. The standard representation of g is a bijection:

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

We say g fixes $1, 6, 8$, and g moves $2, 3, 4, 5$. A natural extension of this representation is the so-called one line notation: $g = (1, 5, 7, 2, 4, 6, 3, 8)$. An important representation is the cycle notation: $g = (1)(2, 5, 4)(3, 7)(6)(8)$. We may drop the fixed points in g when represented in cycle notation: $g = (2, 5, 4)(3, 7)$. Cycle notation allows for easy computation of the order of g, that is, $o(g) = \text{lcm}(3, 2, 1, 1, 1) = 6$, the least common multiple of all cycles of g.

Example 6.2 (Composition of Permutations)**.** Suppose we had $\phi, \psi \in S_4, \phi = (1, 2)(3, 4), \psi = (1, 2, 3)$. Then $\phi\psi = (1, 3, 4)$.

Definition 6.3 (k-cycle)**.** For $\alpha \in \text{Sym}(X)$, with distinctive elements $\alpha_1, \ldots, \alpha_k$, define $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$. Then α is a k-cycle. A 2-cycle is a transposition. A 1-cycle is a fixed point, or an identity permutation.

6.2 Properties of Cycles

Lemma 6.4 (Properties of Cycles)**.** *Let $\alpha = (\alpha_1, \ldots, \alpha_2) \in \text{Sym}(X)$. Then α satisfies six properties:*

(i) there are k ways to write α,

(ii) if $k > 1$, we can always write $\alpha = (\alpha_1, \alpha_2)(\alpha_1, \alpha_2) \cdots (\alpha_1, \alpha_k)$,

(iii) $\alpha^{-1} = (\alpha_k, \ldots, \alpha_1)$,

(iv) $\alpha^k = e$, and $o(\alpha) = k$, where $e = id_{\text{Sym}(X)}$,

(v) for $h \in \text{Sym}(X)$, $\alpha^h = h^{-1}\alpha h = (h(\alpha_1), \ldots, h(\alpha_k))$,

(vi) if $\alpha = (\alpha_1, \ldots, \alpha_k)$, $\beta = (\beta_1, \ldots, \beta_s)$, with α_i, β_j distinct $(i \in [k], j \in [s])$, then $\alpha\beta = \beta\alpha$.

6.3 Disjoint Cycle Decomposition

Lemma 6.5 (Disjoint Cycle Decomposition)**.** *Every permutation of a finite set can be uniquely expressed as a product of disjoint cycles.*

6.4 Cycle Structure

Definition 6.6 (Cycle Structure)**.** For $g \in \text{Sym}(X)$, the cycle structure of g is a function $\mathcal{S}_g \colon Z_{>0} \mapsto Z_{\geq 0}$, where $\mathcal{S}_g(i)$ is the number of i-cycles in the unique disjoint cycle decomposition of g.

Example 6.7. Let $g = (2, 3, 6)(1, 7)(4, 8) \in S_8$, then $\mathcal{S}(1) = 1$, $\mathcal{S}(2) = 2$, $\mathcal{S}(3) = 1$, and $\mathcal{S}(i) = 0$, for $i \geq 4$.

Theorem 6.8 (Conjugation Relation to Cycle Structure)**.** *Two elements of S_n are conjugates if and only if they have the same cycle structure.*

Before we prove this, let's see an example.

Example 6.9. Let $g, h \in S_8, g = (4)(1, 6)(3, 7)(2, 5, 8), h = (1)(7, 8)(2, 6)(3, 4, 5)$. We want to find $k \in S_8$ such that $k^{-1}gk = h$ (Constructive proof given in lecture).

6.5 Sign or Parity of a Permutation

Theorem 6.10 (Parity of 2-cycle Decomposition)**.** *No element in* $\mathrm{Sym}(X)$ *can be written as a product of an even number of transpositions, and a product of an odd number of transpositions.*

Definition 6.11 (Even and Odd Permutations)**.** An even permutation may be expressed as a product of an even number of transpositions, vice versa for odd. The number of even permutations in S_n is equal to the number of odd permutations.

7 Lecture 5: Mon. Feb. 19

Proposition 7.1. *The product of two even permutations is even, the product of two odd permutations is odd, and the product of one even and one odd permutation is odd.*

Proposition 7.2. *An odd length cycle is even.*

Proposition 7.3. *An even length cycle is odd.*

Lemma 7.4 (Expressing Even Permutations)**.** *Every even permutation is a product of even cycles (i.e. cycles with odd length).*

Sketch of proof. For $g \in S_n$, there exists a unique disjoint cycle decomposition of g. Write

$$g = \Pi_i e_i \cdot \Pi_j o_j,$$

where e_j are even cycles, and o_j are odd cycles, all mutually disjoint. □

7.1 Cayley's Theorem

Theorem 7.5 (Cayley's Representation Theorem for Groups)**.** *Every finite group is isomorphic to a group of permutations. In particular, if* $o(G) = n$*, then* G *is isomorphic to a subgroup of* S_n*.*

Proof. Let $G = \{g_i \mid 1 \leq i \leq n\}$. For each g_k, define a mapping $r_k \colon G \mapsto G$, such that $r_k(x) = xg_k$, for all $x \in G$. Define $S = \{r_k \mid 1 \leq k \leq n\}$. It is easy to verify that S is a subgroup of the symmetric group S_n. To prove that $G \cong S$, define the mapping $\phi \colon G \mapsto S$ such that $\phi(g_k) = r_k$. We need to show that $\phi(g_i g_j) = \phi(g_i)\phi(g_j)$. Suppose $x \in G$, and for convenience, assume that $g_i g_j = g_k$. Therefore, we have

$$\begin{aligned}
\phi(g_i g_j)(x) &= \phi(g_k)(x) \\
&= r_k(x) \\
&= xg_k \\
&= x(g_i g_j) \\
&= (xg_i)g_j \\
&= r_j(xg_i) \\
&= (x)(r_i r_j) \\
&= (x)(\phi(g_i)\phi(g_j)).
\end{aligned}$$

It remains to show that ϕ is bijective, which is left as an exercise. □

Example 7.6 (Dihedral Group)**.** Consider D_8. We know $|D_8| = 8$, and by Cayley's theorem, we know that $D_8 \cong S \subseteq S_8$. But we know that $D_8 \subseteq S_4$.

7.2 Normal Subgroups of the Symmetric Group

Let us find all the normal subgroups of S_n.

Theorem 7.7 (Simplicity of Alternating Groups)**.** *The alternating group A_n is simple unless $n = 4$.*

Proof. One can take $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ to be a normal subgroup of A_4.

Lemma 7.8 (Generators of A_n)**.** *Let $n \geq 3$, and X be the set of all 3-cycles in S_n, that is,*

$$X = \{(a, b, c), (a, c, b) \mid a < b < c\}.$$

We claim $A_n = \langle X \rangle$.

Proof of Lemma 7.8. It suffices to show that every even cycle can be generated by elements in X. Equivalently, every even cycle can be written as a product of 3-cycles. We are given that any even cycle is a cycle of length $(2k + 1)$. Obviously, a cycle of length 3 is a product of 3-cycles. Assume that for any cycle of length $(2k - 1)$ is a product of 3-cycles. For a $(2k + 1)$ length cycle c, we have

$$\begin{aligned} c &= (a_1, a_2, \ldots, a_{2k+1}) \\ &= (a_{2k-1}, a_{2k}, a_{2k+1})(a_1, a_2, \ldots, a_{2k-1}). \end{aligned}$$

□

We proceed with our proof by performing case analysis on A_n for $n \geq 5$. We want to show that if we have some N such that $N \triangleleft A_n$, with $N \neq \{e\}$, then we want to show that $N = A_n$. If we can show that N contains all 3-cycles of S_n, then we know that $N = A_n$. There are 5 cases to consider, but we will only consider the first two.

Case 1. N contains a 3-cycle. Then we want to show that N contains every 3-cycle. Since N is normal, any conjugation on an element $g \in N$ is a part of N. We can generate some more 3-cycles in N using this property. Furthermore, since N is closed under multiplication, we can multiply these generated 3-cycles together to find more 3-cycles.

Case 1a. If $n = 5$, it turns out that we can generate every 3-cycle in S_n in this manner.

Case 1b. If $n > 5$, $(a_1, a_4, a_5)(a_1, a_6, a_4) = (a_4, a_5, a_6) \in N$.

Case 2. N contains an element g whose disjoint cycle decomposition has a k-cycle, $k > 3$. Then suppose $g = (a_1, a_2, \ldots, a_k) \cdot \Pi_i t_i$. (Recall that disjoint cycles commute.) Consider the element $g^{-1}(a_1a_2a_3)g(a_3a_2a_1) \in N$. Note that this element is equal to

$$\begin{aligned} (g(a_1)g(a_2)g(a_3))(a_3a_2a_1) &= (a_2a_3a_4)(a_3a_2a_1) \\ &= (a_1a_3a_4) \in N, \end{aligned}$$

and we have reduced **Case 2** to **Case 1**.

Case 3. N contains an element g whose decomposition has two 3-cycles.

Case 4. N contains an element g whose decomposition has only one 3-cycle.

Case 5. N contains an element g whose decomposition only contains 2-cycles.

□

8 Lecture 6: Web. Feb. 21

Theorem 8.1 (Normal Subgroups of S_n)**.** *For $n \geq 5$, if $N \trianglelefteq S_n$, then $N \in \{1, A_n, S_n\}$.*

8.1 Center of Symmetric Groups

Theorem 8.2 (Center of S_n)**.** *The center of S_n, $\mathbf{Z}(S_n) = 1$ if and only if $n \neq 2$.*

Proof. For $n = 1$, clearly, $\mathbf{Z}(S_n) = 1$. For $n = 2$, $S_2 = \langle (1,2) \rangle$, and $\mathbf{Z}(S_2) = S_2$. For $n \geq 3$, Let $z \in S_n$, $z \neq 1$. Without loss of generality, $z(1) = 2$, $z(3) = x \neq 2$. Consider $g = (1,3) \in S_n$. All we need to check is that $(1)gz \neq (1)zg$. □

8.2 Conjugacy Classes

Definition 8.3 (Conjugacy, Conjugacy Classes)**.** If $a, b \in G$, G a group, then b is a conjugate of a if there exists some $c \in G$ such that $c^{-1}ac = b$. The conjugacy class of $a \in G$ is

$$\mathrm{cl}_G(a) = \{x^{-1}ax \mid x \in G\}.$$

Exercise 8.1. Find all the conjugacy classes of S_4.

Lemma 8.4 (Conjugacy is an Equivalence Relation)**.** *For $a \in G$, and $\sim$ denoting conjugacy,*

i. $a \sim a$,

ii. $a \sim b$ *iff* $b \sim a$,

iii. $a \sim b$, $b \sim c$ *implies* $a \sim c$.

Consequently, G is a disjoint union of conjugacy classes.

Example 8.5. We have $N \triangleleft G$ iff N is a disjoint union of conjugacy classes in G.

8.3 Class Equation

Definition 8.6 (Centralizer of an Element)**.** Let $a \in G$. The centralizer of a in G is the subgroup denoted

$$\mathbf{C}_G(a) = \{x \in G \mid xa = ax\}.$$

It is easily verifiable that $\mathbf{C}_G(a)$ is in fact a subgroup. We also have

$$\mathbf{Z}(G) = \bigcap_{a \in G} \mathbf{C}_G(a).$$

Theorem 8.7 (Size of Conjugacy Classes)**.** *Let G be a finite group. Let $a \in G$. Then $|\mathbf{C}_G(a)| = [G\colon \mathbf{C}_G(a)]$.*

Proof. For $x, y \in G$, $x^{-1}ax = y^{-1}ay$ if and only if $(xy^{-1})^{-1}axy^{-1} = a$, which holds if $xy^{-1} \in \mathbf{C}_G(a)$, and therefore, $x\mathbf{C}_G(a) = y\mathbf{C}_G(a)$. It follows that $|\mathrm{cl}_G(a)|$ is equal to the number of left cosets of $\mathbf{C}_G(a)$ in G. □

Theorem 8.8 (Class Equation)**.** *Let G be finite. Then*

$$o(G) = \sum_{a \in R} \frac{o(G)}{o(\mathbf{C}_G(a))},$$

where R is the set of representatives of conjugacy classes in G. Another way to write the class equation is

$$o(G) = o(\mathbf{Z}(G)) + \sum_{a \in R'} \frac{o(G)}{o(\mathbf{C}_G(A))},$$

where R' is the set of representatives of conjugacy classes in $G \setminus \mathbf{Z}(G)$.

Proof. Note $G = \bigcup_{a \in R} \mathrm{cl}(a)$. Therefore,

$$|G| = \sum_{a \in R} |\mathrm{cl}(a)| = \sum_{a \in R} |G \colon \mathbf{C}_G(a)| = \sum_{a \in G} \frac{o(G)}{o(\mathbf{C}_G)(a)}.$$

For the second equation, note that each element $x \in \mathbf{Z}(G)$, $\mathrm{cl}(x) = \{x\}$. □

8.4 Cauchy's Theorem

Theorem 8.9 (Cauchy's Theorem)**.** *If p is a prime number dividing $o(G)$, then G contains an element of order p.*

Proof. We use induction on $o(G)$. When $o(G) = 1$, the result is trivial. Assume the conclusion holds true for all groups with order less than $o(G)$. If $H \subset G$, such that $p \mid o(H)$, we know that H contains an order p element, and therefore, so does G.

Now we consider G such that each $H \subset G$ satisfies $p \nmid o(H)$. By Theorem 8.8,

$$o(G) = o(\mathbf{Z}(G)) + \sum_{a \in R'} \frac{o(G)}{o(\mathbf{C}_G)(a)}.$$

We claim that $\mathbf{C}_G(a) \subset G$... □

9 Lecture 7: Mon. Feb. 26

9.1 *p*-groups

Definition 9.1 (p-groups)**.** A group is a p-group if every element has finite order equal to a power of p.

Lemma 9.2 (Order of finite p-groups)**.** *A finite p-group is a group of order p^n, $n \geq 1$.*

Proof ($\Rightarrow$). Let G be a finite p-group. Assume r is a prime s.t. $r \neq p$, and $r \mid |G|$. By Cauchy's Theorem, G contains an element of order r. This contradicts the definition of p-group. We conclude $|G| = p^n$. □

Proof ($\Leftarrow$). We assume that $|G| = p^n$. Our desired result follows as a result of Lagrange's theorem. □

Theorem 9.3 (Center of p-groups)**.** *Let G be a p-group. Then $Z(G) \neq 1$.*

Proof. Let $o(G) = p^n$. For any $a \in G$, $o(C_G(a)) = p^{n_a}$. Moreover, $0 \leq n_a \leq n$, and $n_a = n$ if and only if $a \in Z(G)$. By the second formulation of the class equation,

$$o(G) = o(Z(G)) + \sum_{a \in R} \frac{o(G)}{o(C_G(a))},$$

where R is the set of representatives of conjugacy classes in $G \setminus Z(G)$. We know $p \mid o(G)$. Furthermore, for any $a \in R$, $o(G)/o(C_G(a)) = p^{n-n_a}$, where $n_a < n$, because $n \notin Z(G)$. Then $p \mid o(G)/o(C_G(a))$, and hence, $p \mid o(Z(G))$, which implies that $Z(G) \neq 1$. □

Corollary 9.3.1 (Groups of order p^2)**.** *Every group of order p^2 is abelian.*

Proof. Let $g \in G$, $|G| = p^2$. Then $|Z(G)| \in \{p, p^2\}$, by the previous theorem, and by Lagrange. If $|Z(G)| = p^2$, we are done. Otherwise, consider $|Z(G)| = p$. Choose $a \in G, a \notin Z(G)$, and consider $C_G(a)$. Then $Z(G) \subseteq C_G(a) \subseteq G$. Then $|C_G(a)| > p$, since $a \notin Z(G)$, and it follows $|C_G(a)| = p^2$, since p^2 is the only other valid divisor of p^2. Thus, $C_G(a) = G$, namely, $a \in Z(G)$. This is a contradiction, and therefore, $|Z(G)| = p^2$. □

9.1.1 Maximal Normal Subgroups of p-groups

Theorem 9.4 (Subgroups of p-groups)**.** *Let G be a group of order p^n, then G has a subgroup of order p^d, for $0 \leq t \leq n$.*

Proof. It suffices to prove that G has a subgroup of order p^{n-1}. Let N be a maximal normal subgroup of G. We want to show that $|N| = p^{n-1}$. Therefore, we know G/N is a finite simple group. Since G/N is also a p-group, we know $Z(G/N) \neq 1$, and $Z(G/N) \triangleleft G/N$. Therefore, $Z(G/N) = G/N$, and therefore, G/N is abelian. Therefore, $G/N \cong C_p$, and $|N| = p^{n-1}$. □

9.1.2 Normalizers of p-groups

Definition 9.5. Let X be a subset of G. The normalizer of X in G is the set $N_G(X) = \{g \in G \mid g^{-1}xg = x\}$.

Example 9.6. The normalizer of a singleton subset $\{a\} \subseteq G$, is $N_G(a) = C_G(a)$.

Example 9.7. Let X be the set of all 3-cycles in S_n. If $g \in N_{S_n}(X)$, then $g^{-1}(a\ b\ c)g = (a'\ b'\ c')$. This shows that the generator of A_n is invariant under conjugation of g, and therefore, the group A_n is invariant under conjugation of g. Thus, $N_{S_n}(X) \subseteq N_{S_n}(A_n)$. Proving reverse containment reveals that $N_{S_n}(X) = N_{S_n}(A_n)$.

Lemma 9.8 (Properties of normalizers)**.** *The normalizer $N_G(X)$ is a subgroup of G. If X is a subgroup, then $X \subseteq N_G(X)$.*

Theorem 9.9 (Normalizer of p-groups)**.** *Let G be a p-group. Let P be a proper subgroup of G. Then, P is a proper subgroup of $N_G(P)$.*

10 Lecture 8: Wed. Feb. 28

Proof of Theorem 9.9. Let $|G| = p^n$. We will use induction on n. When $n = 1$, $P = 1 \subseteq N_G(P) = G$. Assume the conclusion is true for each p-group with order less than p^n. Note that $Z(G)$ is nontrivial, and $Z(G) \triangleleft G$.

If $Z(G)$ is not a subgroup of P, then there exist $x \in Z(G) \subseteq N_G(P)$ such that $x \notin P$. Then $P \subset N_G(P)$.

Otherwise, $Z(G) \triangleleft P$. Consider $P/Z(G)$, which is a proper subgroup of the p-group $G/Z(G)$. Then by hypothesis, $P/Z(G) \subset N_{G/Z(G)}(P/Z(G)) \subseteq G/Z(G)$. Then there must exist some $Z(G) \subseteq Q \subseteq G$ such that $N_{G/Z(G)}(P/Z(G)) = Q/Z(G)$. Therefore, $P/Z(G) \triangleleft Q/Z(G)$. By the correspondence theorem, we know that $P \triangleleft Q$. □

10.1 Direct Product

Example 10.1. Let H, K be two groups, and let $G = H \times K = \{(h, k) \mid h \in H, k \in K\}$. Define the component-wise operation as

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2).$$

Definition 10.2 (External Direct Product)**.** Let $G_1, G_2, \ldots, G_n$ be groups. The external direct product $G = G_1 \times G_2 \times \ldots \times G_n$ is the group of all order n-tuples $(g_1, g_2, \ldots, g_n), g_i \in G_i$.

Exercise 10.1. Given finite groups $G_i, 1 \leq i \leq n$, find the maximal order of elements in the direct product $G_1 \times \ldots \times G_n$.

Exercise 10.2. Show that $G_1 \times G_2 \cong G_2 \times G_1$.

For groups $G_1, \ldots, G_n$, denote the identity of G_i as 1_i, $1 \leq i \leq n$. Define

$$\overline{G_i} = \{(1_1, \ldots, 1_{i-1}, g_i, 1_{i+1}, \ldots, 1_n) \mid g_i \in G_i\}.$$

Then $\overline{G_i} \triangleleft G, \hat{G_i} = G_i$.

Definition 10.3. Let G be a group. If there exists nontrivial normal subgroups $N_1, \ldots, N_n$ of G such that each element of G can be uniquely represented in the form $g = g_1 g_2 \cdots g_n$ where $g_i \in N_i$. Then G is an internal direct product of $N_1, \ldots, N_n$, or,

$$G = \prod_{i=1}^{n} N_i.$$

Lemma 10.4 (Normal subgroups in the internal direct product)**.** *Let $G = \prod_{i=1}^n N_i$. Then $N_i \cap N_j = 1$, $i \neq j$.*

Proof. Let $g \in N_i \cap N_j$. We know

$$g = \overbrace{1 \cdots g \cdots 1}^{i\text{th position}} \cdots = \overbrace{1 \cdots g \cdots 1}^{j\text{th position}},$$

but this implies $g = 1$. □

Corollary 10.4.1 (Commutativity among normal subgroups in internal direct products)**.** *Let $G = \prod_{i=1}^n N_i$. Then for $i \neq j$, every element in N_i commutes with every element in N_j.*

Proof. Take $a \in N_i$, and $b \in N_j$. We have that $a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) \in N_i$, and $a^{-1}b^{-1}ab = (a^{-1}b^{-1}a)b \in N_j$. Therefore, $a^{-1}b^{-1}ab \in N_i \cap N_j = 1$. Our results follows. □

Theorem 10.5 (Internal d.p. isomorphic to external d.p.)**.** *Let $G = \prod_{i=1}^n N_i$. Then $G \cong \bigtimes_{i=1}^n N_i$.*

Proof. Let

$$\phi\colon \bigtimes_{i=1}^{n} N_i \mapsto \prod_{i=1}^{n} N_i,$$

such that $\phi((g_1,\dots,g_n)) = g_1 g_2 \cdots g_n$, where $g_i \in N_i$. We claim ϕ is a bijection, and this is fairly straightforward. We can also easily show ϕ is a homomorphism using the commutativity properties of the internal direct product. □

11 Lecture 9: Mon. Mar. 4

11.1 Fundamental Theorem of Finite Abelian Groups

Theorem 11.1 (Fundamental Theorem of Finite Abelian Groups)**.** *Let G be finite and abelian. Then*

$$G = \prod_{i=1}^{n} C_i,$$

where C_i are cyclic p-groups for various primes p. The expression is unique, that is if we write

$$G = \prod_{i=1}^{m} D_i,$$

where D_i are cyclic p-groups for various primes p, then $m = n$, and up to relabeling of subscripts, $D_i = C_i$, $1 \le i \le n$.

11.1.1 Dummit and Foote's Form

Theorem 11.2 (Dummit and Foote's Form of Theorem 11.1)**.** *Let G be a finite and abelian group. Then $G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s}$, where $n_i \ge 2$, and $n_{i+1} \mid n_i$ for $1 \le i \le s-1$. The expression is unique, that is, if we write $G \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_t}$, then $s = t$, and $m_i = n_i$ for $1 \le i \le s$. The terms $n_1, n_2, \dots, n_s$ are called the invariant factors of G.*

Example 11.3. Supopse G is a group such that $|G| = 1080 = 2^3 \cdot 3^3 \cdot 5$. Then $G = C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_3 \times C_5$, and $G \cong C_{90} \times C_6 \times C_2$.

11.1.2 Abelian Group Decomposition Lemma

Lemma 11.4 (Decomposition into subgroups with coprime orders)**.** *Let G be an abelian group of order $n \times m$, for $(n,m) = 1$. Let $M = \{g \in G \mid g^m = 1\}$, and $N = \{g \in G \mid g^n = 1\}$. Then M, N are subgroups of G, and $G = M \dot{\times} N \cong M \times N$. Moreover, M, N are nontrivial if $m > 1$ and $n > 1$.*

Sketch of proof. It is easy to check that M, N are normal subgroups of G. The next step is to show $M \cap N = 1$. We finally want to show that $G = MN$. Since M, N are abelian, then $MN \subseteq G$. It remains to show the reverse containment. Moreover, M, N are nontrivial if $m > 1, n > 1$ respectively, which is proven using Cauchy's theorem. □

Corollary 11.4.1 (Decomposition into p-groups)**.** *Let G be an abelian group of order n, where $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, for primes p_i. Then we may write*

$$G = \prod_{i=1}^{s} G_i \cong \bigtimes_{i=1}^{s} G_i,$$

where $|G_i| = p_i^{\alpha_i}$.

Lemma 11.5 (Fundamental Theorem for finite abelian p-groups)**.** *Let G be an abelian group of order p^n. Then*

$$G = \prod_{i=1}^{n} C_i,$$

where C_i are cyclic p-groups, and the expansion is unique.

Proof. We claim that $G = A \times H$, with $A = \langle a \rangle$ and $a \in G$, and $a \in G$ is an element with maximal order. We will prove this using induction on n. Let $n = 1$, then $G = C_p = \langle a \rangle \times 1$, where $|a| = p$. Assume that our conclusion holds for all groups with order less than p^n. We shall consider two cases. In the first case, suppose there is some element $b \in G \setminus A$ such that $|b| = p$, and suppose $B = \langle b \rangle$. Clearly, $A \cap B = 1$. Consider the quotient group $\overline{G} = G/B$, where $|\overline{G}| = p^{n-1}$, by Lagrange. We claim that $|Ba| = |a|$, and hence $Ba \in \overline{G}$ has maximal order in G/B. To prove this, we prove $|Ba| \leq |a|$, and $|a| \mid |Ba|$, which implies $|Ba| = |a|$. It is clear that $|Ba| \leq |a|$. Note that $(Ba)^{|Ba|} = Ba^{|Ba|} = B$, and therefore, $a^{|Ba|} \in B \cap A = 1$, hence $a^{|Ba|} = 1$. Hence, $|a| \mid |Ba|$, and therefore, $|Ba| = |a|$.

Let $\overline{A} = \langle Ba \rangle \subseteq G/B$. By hypothesis, $\overline{G} = \overline{A} \times \overline{H}$, where $\overline{A} = \langle Ba \rangle$. Since $\overline{H} \triangleleft G/B$, there exists $B \subseteq H \subseteq G$, such that $\overline{H} = H/B$. Finally, we can write $\overline{A} = BA/B$. Write

$$\overline{G} = BA/B \times H/B,$$

and by the definition of internal direct product, $BA/B \triangleleft G/B$, and $H/B \triangleleft G/B$, and $BA/B \cap H/B = 1$. Now assume $g \in A \cap H$, and therefore $Bg \in BA/B \cap H/B = B$. This implies $Bg = B$, which shows $g \in B$. Therefore, $g \in A \cap B = 1$, hence, $g = 1$.

By the Correspondence theorem, $H \triangleleft G$ (because $H/B \triangleleft G/B$), and $A \triangleleft G$. It remains to show that $G = AH$. We will show this by proving $AH \subseteq G$, and $|AH| = |G|$. By the definition of quotient groups, we have

$$|\overline{G}| = \frac{|G|}{p},$$

and

$$|\overline{G}| = |\overline{A}||\overline{H}| = |A|\frac{|H|}{p},$$

combining to yield $|G| = |A||H|$. Finally, we have $|AH| = |A||H|/|A \cap H| = |A||H|$, since $A \cap H$ is trivial. It remains to show that this decomposition is unique. □

12 Lecture 10: Wed. Mar. 6

I was sick. Ring theory introduction.

13 Lecture 11: Mon. Mar. 11

13.1 Characteristic

Definition 13.1 (Characteristic of Ring Elements)**.** Let R be a ring, and $r \in R$. If r has finite additive order k, then r is said to have characteristic k. Otherwise, r is said to have characteristic 0.

Example 13.2. For the ring of integers $\mathbb{Z}$, the additive identity 0 has characteristic 1. All the non-zero elements have characteristic 0.

Example 13.3. For the ring of integers mod n, $\mathbb{Z}/n\mathbb{Z}$, $a \in \mathbb{Z}/n\mathbb{Z}$ has characteristic $n/(n,a)$. If n is prime, then every non-zero element in $\mathbb{Z}/n\mathbb{Z}$ has characteristic n,

Theorem 13.4 (Characteristic of Elements)**.** *If R is a ring with identity and no zero divisors, then all non-zero elements of R have the same characteristic, which is either 0, or a prime p.*

Definition 13.5 (Characteristic of a Ring)**.** Let R be a ring. If there exists a positive integer k, such that $kr = 0$ for all $r \in R$, then the smallest such integer is called the characteristic of R. If no such positive integer exists, then R has characteristic 0.

Example 13.6. The ring of integers mod n, $\mathbb{Z}/n\mathbb{Z}$ has characteristic n. The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, have characteristic 0.

Theorem 13.7 (Positive Characteristic of Rings)**.** *Let R be a ring with identity and no zero divisors. Then the characteristic of R is either 0 or some prime p.*

Corollary 13.7.1 (Additive Group of Finite Rings)**.** *Let R be as in Theorem 13.7. Assume R is finite. Then the additive group of R is an elementary abelian p-group.*

Definition 13.8 (Integral Domain)**.** The ring R is an integral domain if R has an identity, and R has no zero divisors.

Example 13.9. The ring of integers is an integral domain. The ring of quaternions is an integral domain.

Definition 13.10 (Division Ring)**.** The ring R is a division ring if

(a). with identity $1 \neq 0$,

(a). every non-zero element has a multiplicative inverse.

A division ring is an integral domain.

Definition 13.11 (Field)**.** A commutative division ring is a field.

Theorem 13.12 (Finite Commutative Domain is a Field)**.** *A finite commutative integral domain R is a field.*

Proof. Denote the non-zero elements of R by R^*. For $a \in R^*$, define a mapping $f_a \colon R \mapsto R$ by $f_a(r) = ar$, for all $r \in R$. We will use the finiteness and commutativity of R to show that f_a is a bijection for all $a \in R^*$. We show that f_a is surjective as follows. Let $r_1 \neq r_2 \in R$. Assume $f_a(r_1) = f_a(r_2)$. Therefore, $ar_1 = ar_2$, and by the integral domain laws, the cancellation laws hold, and therefore, $r_1 = r_2$. Therefore, we have a contradiction, and $f_a(r_1) \neq f_a(r_2)$. Since the image and domain sets of f_a have the same size, f_a is a bijection.

Now, we want to show R has an identity. For $a \in R^*$, there exists $e \in R$ s.t. $f_a(e) = ae = a$, because f_a is a bijection. Fix another $r \in R^*$, and again, as f_a is bijective, there exists $b \in R$ s.t. $f_a(b) = ab = r$. We have that $re = abe = aeb = ab = r$. Using a similar calculation, we find that $er = r$. Therefore, e is the identity.

Lastly, for $a \in R^*$, there exists $b \in R^*$ such that $f_a(b) = e$. Therefore, $ba = ab = e$, which shows that b is the multiplicative inverse of a. □

14 Lecture 12: Mon. Mar. 18

14.1 Examples of Rings

Example 14.1 (Polynomial Rings)**.** Let R be a commutative ring with an identity, and let x be an indeterminate. Then $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + ax + a_0 \mid a_i \in R\}$. If R is commutative, then $R[x]$ is commutative. Regard R as a subring of $R[x]$. For $a \in R$, a as an element in $R[x]$ is a constant polynomial. If $1 \in R$ is the identity, it is not hard to see that 1 is the identity of $R[x]$.

Proposition 14.2. *Let R be a commutative ring with identity. Let $p(x), q(x)$ be nonzero elements of $R[x]$. Then $\deg p(x)q(x) = \deg p(x) + \deg q(x)$. Furthermore, the units of $R[x]$ are the units of R. Also, if R is a domain, then $R[x]$ is a domain.*

Proof. Suppose our first fact is true, and let $p(x) \in R[x]$ be a unit. Then there is some $q(x) \in R[x]$, such that $p(x)q(x) = 1$. By our first fact, $\deg p(x)q(x) = \deg p(x) + \deg q(x) = 0$. Since degrees of polynomials are nonnegative, clearly $\deg p(x) = \deg q(x) = 0$.

To prove our third fact, by contrapositive, suppose $p(x)$ is a zero divisor of $R[x]$. Therefore, let $q(x) \neq 0$ such that $p(x)q(x) = 0$. Assume the leading term of $p(x)$ is $a_m x^m$, and likewise, assume the leading term of $q(x) = b_n x^n$, with $a_m, b_n \in R, a_n, b_n$ are nonzero. Hence, $a_m x^m \cdot b_n x^m = 0$, which implies $a_m b_n = 0$, which shows either a_m or b_n is a zero divisor. □

Example 14.3. Let R be a ring, and n a positive integer. Let $M_n(R)$ be the set of all $n \times n$ matrices over R. Then $M_n(R)$ is a ring with respect to matrix addition and matrix multiplication.

Proposition 14.4. *If R is nontrivial, and $n \geq 2$, then $M_n(R)$ is noncommutative and has zero divisors.*

Proof by example. Consider $n = 2$. Consider

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ab \\ 0 & 0 \end{pmatrix},$$

and

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

□

Proposition 14.5. *The ring R is a subring of $M_n(R)$.*

14.2 Ideals

Definition 14.6 (Left/Right/Two-sided Rings)**.** Let R be a ring, and U a subring of R. We say U is a left ideal, written $U \lhd_l R$ if $ra \in U$ for all $r \in R$ and $a \in U$. The right ideal is written $U \lhd_r R$. Some authors say that U is an ideal (written $U \lhd R$) if it is a left and right ideal of R. Some authors call U a two-sided ideal.

In R, there are two trivial ideals: $\{0\}$, and R. hence, a *proper ideal* is a nontrivial ideal. If R is commutative, left ideals and right ideals of R coincide.

Example 14.7 (Ideals of Integer Ring)**.** For $\mathbb{Z}$, and $n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$. Every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.

Example 14.8. Let R be a commutative ring and $n \geq 2$, and as before $M_n(R)$ is a noncommutative ring. Let $J \triangleleft R$. Consider $M_n(J)$, the set of all $n \times n$ matrices over J. We claim that $M_n(J) \triangleleft M_n(R)$.

Example 14.9. Let R be a nontrivial commutative ring with $n \geq 2$. For $1 \leq j \leq n$, let L_j be the subset of $M_n(R)$ with arbitrary jth column and zero in all the other columns. We claim $L_j \triangleleft_L M_n(R)$, but $L_j \not\triangleleft_r M_n(R)$.

Consider

$$L_j = \left\{ \begin{pmatrix} 0 & b_{12} \\ 0 & b_{22} \end{pmatrix} \;\middle|\; b_{12}, b_{22} \in R \right\}.$$

Definition 14.10 (Principal Ideals)**.** Let R be a ring and $a \in R$. Then

$$aR = \{ar \mid r \in R\}$$

is the principal right ideal in R generated by a. Hence, Ra is the principal left ideal in R generated by a. When R is commutative, some authors write $(a) = aR = Ra$.

Example 14.11 (Principal Ideals)**.** The multiples of n in $\mathbb{Z}$, $n\mathbb{Z}$ is a principal ideal in $\mathbb{Z}$.

Example 14.12. Let R be a commutative ring, and $f(x) \in R[x]$. Then $(f(x)) = \{f(x)g(x) \mid g(x) \in R[x]\}$.

14.2.1 Properties of Ideals

Theorem 14.13 (Addition, Intersection, and Product of Ideals)**.** *Let R be a ring, and U, V right ideals of R. Then*

(a). $U \cap V \triangleleft_r R$,

(b). $U + V = \{u + v \mid u \in U, v \in V\} \triangleleft_r R$,

(c). $UV = \{u_1v_1 + \cdots + u_nv_n \mid u_i \in U, v_i \in V, n \in Z_+\} \triangleleft_r R$.

How to prove (c). Take an two elements $s = u_1v_1 + \cdots + u_nv_n$, $t = u_1'v_1' + \cdots + u_n'v_n' \in UV$. Prove UV is a subring of R (closed under addition, closed under multiplication). Prove UV is a right ideal of R. □

Theorem 14.13 can be generalized to left ideals, and two-sided ideals, and it can be extended to finitely many ideals.

Theorem 14.14 (Product of Ideals (Incomplete))**.** *Let R be a commutative ring, and $U, V, W \triangleleft_l R$. Then*

(a). if $1 \in R$, then $R^2 = RR = R$, and $RU = U$.

15 Lecture 13: Wed. Mar. 20

Theorem 15.1 (Product and Intersection of Ideals)**.** *Let R be a commutative ring with identity. Suppose $U_1, U_2, \ldots, U_n$ are ideals of R. If $U_i + U_k = R$, whenever $i \neq k$, then*

(a). for any $1 \leq j < n$, $U_1U_2 \cdots U_j + U_{j+1} = R$,

(b). $U_1U_2 \cdots U_n = U_1 \cap U_2 \cap \ldots \cap U_n$.

In particular, if $U, V \triangleleft R$, and $U + V = R$, then $UV = U \cap V$, and $UV \subseteq U \cap V$.

Proof of (a). Let $n = 2$, $U_1 + U_2 = R$. Assume the conclusion holds true for n. Let $U_1, \ldots, U_n, U_{n+1}$ be ideals of R s.t. $U_i + U_k = R$, for $i \neq k$. We have

$$\begin{aligned} R = R^2 &= (U_1 + U_{n+1})(U_2 U_3 \ldots U_n + U_{n+1}) \\ &\subseteq U_1 U_2 \ldots U_n + U_{n+1}. \end{aligned}$$

□

15.1 Ring Homomorphism

Definition 15.2. Let R, S be two rings. A function $\phi\colon R \to S$ is called a ring homomorphism if, for $a, b \in R$, $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$.

Definition 15.3. If ϕ is also a bijection, ϕ is a ring isomorphism.

Definition 15.4. If ϕ is injective, then R is isomorphic to $\phi(R)$, where $\phi(R) \subseteq S$, and we say R is embedded in S.

Definition 15.5. The kernel of ϕ, denoted $\ker \phi$ is

$$\ker \phi = \{a \in R \mid \phi(a) = 0\}.$$

Ring homomorphisms inherit properties from group homomorphisms, namely $\phi(0) = 0$, and $\phi(-a) = -\phi(a)$.

Definition 15.6 (Group of Units)**.** Let R be a commutative ring with identity. Define $U(R)$ to be the group of units of R. Explicitly, $U(R) = \{a \in R \mid \exists\, b \in R, ab = 1\}$.

Example 15.7 (Ring Homomorphisms)**.** Here are some examples of ring homomorphisms.

1. Let $J(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ under usual $+$ and $\cdot$ in $\mathbb{R}$, $J(\sqrt{2})$ is a commutative ring. Let $U(J(\sqrt{2})) = \{\pm 1\}$. Define $\phi\colon J(\sqrt{2}) \to J(\sqrt{2})$ such that $\phi(a + b\sqrt{2}) \mapsto (a - b\sqrt{2})$. Then ϕ is a ring isomorphism from $J(\sqrt{2})$ to itself. Some authors call ϕ a ring automorphism.

2. Let R be the set of real valued continuous functions on $[0, 1]$. Then R is a commutative ring with identity w.r.t. usual function addition and multiplication. Let $\phi\colon R \to \mathbb{R}$, such that $\phi(f) = f(1/2)$. Then $\ker \phi = \{f \in R \mid f(1/2) = 0\}$.

3. Let $n \geq 2$. Consider $\phi\colon \mathbb{Z} \to n\mathbb{Z}$, where $\phi(a) = na$, for $a \in \mathbb{Z}$. We claim ϕ is a group homomorphism from $(\mathbb{Z}, +) \to (n\mathbb{Z}, +)$. However, since $n = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = n^2$, we have $n \in \{0, 1\}$, but $n \geq 2$, so ϕ is not a ring homomorphism.

Lemma 15.8 (Properties of Ring Homomorphism)**.** *For R, S rings, let $\phi\colon R \to S$ be a ring homomorphism. Then*

(a). $\ker \phi \triangleleft S$,

(b). *ϕ is injective iff* $\ker \phi = 0$.

Theorem 15.9 (Ring Homomorphism and Ideals)**.** *Let R, S be rings, and $\phi\colon R \mapsto S$. If ϕ is surjective and U is a left/right/two-sided ideal of R, then $\phi(U)$ is a left/right/two-sided ideal of S.*

Furthermore, if R contains an identity 1, then $\phi(1)$ is the identity in S, and $\phi(U(R)) \subseteq U(S)$.

Example 15.10. For R a ring, consider $\phi\colon R \to M_2(R)$, where

$$\phi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

Obviously, ϕ is not surjective, but it is a ring homomorphism. Therefore, $\phi(R)$ is not an ideal in $M_2(R)$.

Example 15.11. The units $U(R[x])$ of R are equal to the units of R. We can prove this by building a surjective ring homomorphism $\phi\colon R[x] \to R$, where

$$\phi(f(x)) = \phi\left(\sum_{i=0}^{n} a_i x^i\right) = a_0.$$

By our theorem, $\phi(U(R[x])) \subseteq U(R)$, and it is not hard to prove the reverse containment.

Theorem 15.12 (Quotient/Factor Rings)**.** *Let R be a ring and $U \triangleleft R$. Set*

$$R/U = \{U + r \mid r \in R\}$$

to be the quotient group of R by U. Under the multiplication $(U + r)(U + s) = U + rs$, for all $r, s \in R$, R/U forms a ring called the quotient ring of R by U.

Furthermore, R/U is commutative if R is commutative, and if R has an identity, then R/U has an identity.

Theorem 15.13 (Canonical Projection)**.** *Let U be an ideal of a ring R. Then $\phi\colon R \to R/U$ such that $\phi(r) = U + r$ for $r \in R$ is a surjective ring homomorphism with $\ker\phi = U$. There is a one-to-one correspondence between ideals of R and kernels of ring homomorphisms from R to other rings.*

Theorem 15.14 (Ring Isomorphism Theorem)**.** *Let $\phi\colon R \to S$ be a surjective ring homomorphism. Let T be a subring of R, and let $U \subset V \subset R$ be ideals of R. Then*

(i). $S \cong R/\ker\phi$,

(ii). $(T + U)/U \cong T/(T \cap U)$,

(iii). $(R/U)/(V/U) \cong R/V$.

16 Lecture 14: Mon. Apr. 1

16.1 Commutative Ring Ideals

Throughout this lecture, let R be a ring with identity $1 \neq 0$.

Definition 16.1 (Ideals Generated by a Subset)**.** Let A be a subset of the ring R. Let (A) denote the smallest ideal containing A. We call (A) the ideal generated by A.

If $|A| = 1$, and R is commutative, then $(A) = (a)$, the principal ideal generated by a. If R is commutative and $A = \{a_1, \ldots, a_n\}$, then $(A) = \{a_1r_1 + a_2r_2 + \ldots + a_nr_n \mid r_1, \ldots, r_n \in R\}$. Generally, $(A) = \bigcap_{A \subseteq I \subseteq R} I$, for I an ideal of R. Any non empty intersection of a collection of ideals is also an ideal. A is contained in at least one ideal, R.

Example 16.2. Let $m, n \in \mathbb{Z}, A = \{m, n\}$, then $(A) = (m, n)$. Also, if $\gcd(m, n) = d$, then $(m, n) = (d)$. Every ideal in $\mathbb{Z}$ is a principal ideal.

Example 16.3. For x, $(2, x)$ is not a principal ideal in $\mathbb{Z}[x]$. To see this, write

$$(2, x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\},$$

and we see that $(2, x)$ consists of all polynomials with even constant terms. Hence, $(2, x)$ is a proper ideal. Assume $(2, x) = \big(a(x)\big)$, $a(x) \in \mathbb{Z}[x]$. Since $2 \in \big(a(x)\big)$, write $2 = a(x)b(x)$. We know $\{a(x), b(x)\} = \{\pm 1, \pm 2\}$. If $a(x) = \pm 1, \big(a(x)\big) = (\pm 1) = \mathbb{Z}[x]$, which is impossible since $(2, x)$ is proper. If $a(x) = \pm 2$, then $x \in \big(a(x)\big) = (\pm 2)$, hence $x = \pm 2c(x)$, where $x \in \mathbb{Z}[x]$, which is a contradiction.

Proposition 16.4 (Proper Ideals)**.** *Let I be an ideal of R. Then*

(1). $I = R$ iff I contains a unit,

(2). if R is commutative, then R is a field iff its only ideals are 0, and R.

Proof of (1), $\Rightarrow$. If $I = R$, then $1 \in I$. If $u \in U(R)$ and $u \in I$, let v be its inverse. For any $r \in R$, $r = r1 = r(vu) = (rv)u \in I$. Hence, $I = R$. □

Proof of (2). If R is a field, let U be a nonzero ideal of R. Then there exists a nonzero $u \in R$ such that $u \in U$. Consider $u^{-1}y = 1 \in U$, by part (1), $U = R$.

Now assume R is commutative, and that its only ideals are 0 and R. Suppose $a \in R$ is a nonzero element. Consider (a), and since $(a) \neq 0$, $(a) = R$. Then $1 \in (a)$, which implies that there exists some $b \in R$ such that $ab = ba = 1$, hence b is the inverse of a, and so R is a field. □

Definition 16.5 (Maximal Ideals)**.** An ideal M in a ring R is a maximal ideal if $M \neq R$, and the only ideals containing m are M and R.

Example 16.6. In $\mathbb{Z}$, an ideal (n) is maximal iff n is prime. The key point is that (n) is a subideal of (m) if and only if $m \mid n$.

Example 16.7. In $\mathbb{Z}[x]$, $(2, x)$ is a maximal ideal. Assume $U \triangleleft \mathbb{Z}[x]$, and $(2, x) \subset U$. Then there exist $p(x) \in U \setminus (2, x)$. Then the constant term of $p(x)$ must be odd. Then $p(x) + 1 \in (2, x) \subseteq U$, hence $p(x) + 1 - p(x) = 1 \in U$, which implies $U = \mathbb{Z}[x]$.

Proposition 16.8 (Maximal Ideal Containment)**.** *In a ring with identity, every proper ideal is contained in a maximal ideal.*

Proposition 16.9 (Proper Ideal Containment)**.** *Let R be a commutative ring, and suppose M is a proper ideal of R. Then M contains all proper ideals of R iff $M = R \setminus U(R)$ is an ideal.*

$\Rightarrow$. Since M is a proper ideal, then we know $M \subseteq R \setminus U(R)$. First, assume M contains all proper ideals of R. Then take $a \in R \setminus M$. Then (a) is a nonzero ideal, and $(a) \nsubseteq M$. So (a) cannot be a proper ideal, hence $(a) = R$, which implies a is a unit. □

17 Lecture 15: Wed. Apr. 3

$\Leftarrow$. Assume $M = R \setminus U(R)$ is an ideal. Then for each proper ideal U, and each $a \in U$, we must have $a \notin U(R)$. Therefore, $a \in M$, and $U \subseteq M$. □

17.1 Maximal and Prime Ideals

Theorem 17.1 (Characterization of Maximal Ideal)**.** *Assume R is a commutative ring with identity $1 \neq 0$. The ideal M is maximal in R iff R/M is a field.*

Proof. We know that R/M is a field iff R/M has no proper ideals. By the ring correspondence theorem, there is a one-to-one correspondence between the ideals of R/M and the ideals of R containing M. Therefore, the only ideals in R containing M are M and R. Hence, M is maximal in R. □

Example 17.2. In the ring of integers $\mathbb{Z}$, given $p \in \mathbb{Z}$, for prime p, the principal ideal (p) is a maximal ideal in $\mathbb{Z}$, hence $\mathbb{Z}/(p)$ is a field, namely, $\mathbb{Z}/(p) \cong \mathbb{Z}_p$.

Definition 17.3 (Prime Ideals)**.** Assume R is a commutative ring with identity $1 \neq 0$. An ideal P is a prime ideal of R if $P \neq R$, and for $a, b \in R$, with $ab \in P$, either $a \in P$, or $b \in P$.

Example 17.4. In the ring of integers $\mathbb{Z}$, the principal ideal (n) is a prime ideal if and only if n is prime. If we assume (n) is a prime ideal, by definition, for $a, b \in \mathbb{Z}$, $ab \in (n)$ implies either $a \in (n)$ or $b \in (n)$. That is, $n \mid ab$, which implies $n \mid a$, or $n \mid b$, which holds iff n is prime.

Example 17.5. Consider $\mathbb{Q}[x]$, and let $p(x)$ be an irreducible polynomial over $\mathbb{Q}$. Then $\big(p(x)\big)$ is a prime ideal in $\mathbb{Q}[x]$. Let $a(x), b(x) \in \mathbb{Q}[x]$, and suppose $a(x)b(x) \in \big(p(x)\big)$. Therefore, $p(x) \mid a(x)b(x)$. Since $p(x)$ is irreducible, we must have that either $p(x) \mid a(x)$ or $p(x) \mid b(x)$. Namely, $a(x) \in \big(p(x)\big)$ or $b(x) \in \big(p(x)\big)$.

Theorem 17.6 (Characterization of Prime Ideals)**.** *Assume that R is a commutative ring with identity $1 \neq 0$. The ideal P is a prime ideal of R iff the quotient ring R/P is an integral domain.*

Proof. We will prove the converse by contrapositive, so assume that P is not a prime ideal. Then there exists $ab \in P$, with $a, b \notin P, a, b \in R$. Consider the product $(a + P)(b + P) = ab + P$. Since $a \notin P$, $a + P \neq P$, and likewise, $b + P \neq P$. However, $ab + P$, so that $(a + P)(b + P) = P$, and thus R/P is not an integral domain. The forward implication is proven very similarly. □

Corollary 17.6.1 (Maximal Ideals and Prime Ideals)**.** *Assume R is a commutative ring with identity $1 \neq 0$. Every maximal ideal is a prime ideal.*

Proof. All fields are integral domains. □

17.2 Rings of Fractions

Consider the relation between $\mathbb{Z}$ and $\mathbb{Q}$. Its clear that $\mathbb{Z}$ is a subring of $\mathbb{Q}$. Furthermore, $\mathbb{Q} = \{ab^{-1} \mid a, b \in \mathbb{Z}, b \neq 0\}$. We claim that $\mathbb{Q}$ is the smallest ring containing $\mathbb{Z}$ such that all nonzero element in $\mathbb{Z}$ is a unit.

Theorem 17.7 (Rings of Fractions)**.** *Let R be a commutative ring with identity $1 \neq 0$, and let D be any nonempty subset of R that does not contain 0 nor any zero divisors, and is closed under multiplication. Then there is a commutative ring Q with identity such that Q contains R as a subring, and every element of D is a unit in Q. Also, Q satisfies the following.*

(1). Every element of Q is of the form rd^{-1} for $r \in R$, and $d \in D$. In particular, if $D = R \setminus \{0\}$, then Q is a field.

(2). The ring Q is the smallest ring containing R in which all elements of D become units.

Proof. Much of the proof of this theorem is lengthy routine verification; we won't prove most of it. Let $F = \{(r,d) \mid r \in R, d \in D\}$, and define the relation $\sim$ on F by $(r,d) \sim (s,e)$, iff $re = sd$. We want to verify that $\sim$ is reflexive, symmetric, and transitive. For instance, transitivity follows from the following line of computation: $(r,d) \sim (s,e) \Rightarrow (re - sd) = 0$, and $(s,e) \sim (t,f) \Rightarrow (sf - te) = 0$, together implies $(rf - td)e = 0$, and since $e \in D$, $rf = td \Rightarrow (r,d) \sim (t,f)$. The remaining properties are relatively easy too.

Altogether we will find that $\sim$ is an equivalence relation. Hence, denote the equivalence class containing (r,d) by $r/d = \{(a,b) \mid a \in R, b \in D, rb = ad\}$. Then let Q be the set of equivalence classes under $\sim$. Note that $r/d = (re)/(de)$ in Q for all $e \in D$. Define addition and multiplication on Q as $a/b + c/d = (ad + bc)/bd$, and $(a/b)(c/d) = (ac)/(bd)$. What is left is to verify Q is a commutative ring. □

18 Lecture 16: Mon. Apr. 8

18.1 Divisibility

Theorem 18.1 (Fundamental Theorem of Arithmetic)**.** *Each $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ has a unique prime factorization.*

Definition 18.2 (Divisibility in commutative rings)**.** Let R be a commutative ring, and $r, d \in R$, with $d \neq 0$. Then d divides r, $d \mid r$ if $r = ds$ for some $s \in R$. Also, $d \mid r$ if and only if $r \in (d)$.

Lemma 18.3 (Some properties of divisibility)**.** *For all $d \in R^*$, $d \mid 0$. If $1 \in R$, $1 \mid r$ for each $r \in R$. If $d \mid r$, and $d \mid s$, then $d \mid (ar + bs)$ for all $a, b \in R$.*

Lemma 18.4 (Divisibility in integral domains)**.** *Let D be a commutative integral domain. Let $a, b \in D^*$. Then $a \mid b$ and $b \mid a$ if and only if $a = bu$ for some $u \in U(D)$.*

Proof. If $a \mid b$ and $b \mid a$, then there exists $u, v \in D$, such that $b = av$, $a = bu$. We have $a = avu$. Because D is an integral domain, $vu = 1$. Hence, u is a unit. For the converse, $a = bu \Leftrightarrow b = au^{-1}$. □

Definition 18.5 (Associate)**.** Let R be a commutative ring with identity $1 \neq 0$. Two elements a, b of R are associate in R if $a = bu$ and $b = au^{-1}$ for some $u \in U(R)$

18.2 Irreducibility, Primes

Definition 18.6 (Irreducible and prime elements)**.** Let D be a commutative integral domain. We call $r \in D$ irreducible if $r = st$ for $s, t \in D$ implies $s \in U(D)$ or $t \in U(D)$. We call $r \in D$ prime if $r \mid st$, $s, t \in D$ implies $r \mid s$ or $r \mid t$.

Example 18.7. Let $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ with $\alpha^2 \in \mathbb{Z}$. Consider the ring $\mathbb{Z}[\alpha] = \{a + \beta\alpha \mid a, b \in \mathbb{Z}\}$. Then $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{C}$. Define $\sigma \colon \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]$ as $\sigma(a + b\alpha) = a - b\alpha$. We claim σ is a ring isomorphism. For $r = a + b\alpha \in \mathbb{Z}[\alpha]$, the norm of r is defined to be $N(r) = r\sigma(r) = (a + b\alpha)(a - b\alpha) = a^2 + b^2\alpha^2 \in \mathbb{Z}$. For $r, s \in \mathbb{Z}[\alpha]$, $N(rs) = N(r)N(s)$. For $n \in \mathbb{Z}$, $N(nr) = n^2 N(r)$. We claim that $u \in U(\mathbb{Z}[\alpha])$ if and only if $N(u) = \pm 1$.

Example 18.8. Let $\alpha = \sqrt{-19}$, and consider the ring $\mathbb{Z}[\alpha]$. Now for any $r = a + b\alpha$, $N(r) = a^2 + 19b^2$. Now we have, $N(r) \neq 2, 5, 10$. Fix $r = 1 + \alpha$. Then $N(r) = 20$. Consider $r = st$, for $s, t \in Z[\alpha]$. Consider $20 = N(r) = N(st) = N(s)N(t)$. The only possibility for this to hold is that

$\{N(s), N(t)\} = \{\pm 1, \pm 20\}$. Therefore, $N(s) = 1$, or $N(t) = 1 \Leftrightarrow s \in U(\mathbb{Z}[\alpha]) \vee t \in U(\mathbb{Z}[\alpha]) \Leftrightarrow r$ is irreducible.

On the other hand, r is not prime. By definition, $r \mid N(r)$, or $r \mid 20$. We know $20 = 4 \cdot 5$. We want to show $r \nmid 4$ and $r \nmid 5$. Assume $r \mid 4$. Then $rs = 4$, $s \in \mathbb{Z}[\alpha]$. We have $N(rs) = N(r)N(s) = 20N(s) = N(4) = 16$, but this is impossible because $N(s) \in \mathbb{Z}$. Likewise, we can derive that $r \nmid 5$, so that r is not prime.

Theorem 18.9 (Relation between prime and irreducible elements)**.** *Let D be a commutative integral domain. Let $p \in D^*$. Then p is a prime iff (p) is a prime ideal. Secondly, if p is prime, then p is irreducible.*

Proof. To prove the first claim, use the fact that $a \in (p) \Leftrightarrow p \mid a$. The second claim is slightly nontrivial. Let $p = rs$, $r, s \in D^*$. Assume that p is prime. Now either $p \mid r$, or $p \mid s$. Without loss of generality, we assume $p \mid r$. Now, $r = pt$, for $t \in D$, and we have $p = pts$. By the cancellation law, $ts = 1$, implying s is a unit. □

Lemma 18.10 (Property of prime elements)**.** *Let D be commutative integral domain. If $p \mid r_1 r_2 \cdots r_n$, then $p \mid r_i$ for some i.*

Theorem 18.11 (Factorization into product of prime and irreducible elements)**.** *Let D be a commutative integral domain. Suppose $p_1 p_2 \cdots p_m = u r_1 r_2 \cdots r_n$, where each p_i is prime, and each r_i is irreducible, and $u \in U(D)$. Then $m = n$, and up to relabeling, $p_i = u_i r_i$, for some $u_i \in U(D)$.*

Proof. We will use induction on m. For $m = 1$, $p_1 = u r_1 \cdots r_n$. Since p_1 is prime, $p_1 \mid r_1 r_2 \cdots r_n \Rightarrow p_1 \mid r_i$, $p_1 \mid r_1 r_2 \cdots r_n \Rightarrow p_1 \mid r_i$, for some i. W.l.o.g. assume $p_1 \mid r_1$. Then $r_1 = \theta p_1$, $\theta \in D$. Now $p_1 = u\theta p_1 r_2 \cdots r_n$, such that $1 = u\theta r_2 \cdots r_n$. This implies that $r_2, \ldots, r_n \in U(D)$ contradicting the fact that r_i are irreducible. This forces $n = 1$, and that $p_1 = u r_1$, proving the base case.

Assume the conclusion holds true for all $m \geq 1$. Consider

$$p_1 p_2 \cdots p_{m+1} = u r_1 \cdots r_n.$$

Then $p_{m+1} \mid r_1 r_2 \cdots r_n \Rightarrow p_{m+1} \mid r_n$. Use inductive hypothesis to finish proof. □

19 Lecture 17: Wed. Apr. 10

19.1 Principal Ideal Domains

Definition 19.1 (PID)**.** An integral domain D is a principal ideal domain (PID) if every ideal of D is principal. If $U \triangleleft D$, then there exists some $a \in D$ such that $U = (a)$.

Example 19.2. The ring of integers $\mathbb{Z}$ is a PID.

Example 19.3. The ring of polynomials over the integers, $\mathbb{Z}[x]$, is not a PID, since $(2, x)$ cannot be principal.

Example 19.4. Let $R = \mathbb{Z}[\sqrt{-5}]$. We can show that $(3, 2 + \sqrt{-5})$ is not a principal ideal.

Definition 19.5 (Greatest Common Divisor (gcd))**.** Take S to be a nonempty subset of the commutative integral domain D. Then d is a common divisor of S if $d \mid s$ for $s \in S$. A common divisor d of s is a greatest common divisor (gcd) if whenever c is a common divisor of S, then $c \mid d$. here, we will use $\gcd(S)$ to denote the set of greatest common divisors of S.

Proposition 19.6. *Consider a commutative integral domain D, and S a nonempty subset of D. Let $d \in \gcd(S)$, then $\gcd(S) = \{du \mid u \in U(D)\}$.*

Lemma 19.7. *Let D be a PID, and $S = \{s_1, \ldots, s_k\}$ be a nonempty finite set of elements of $D^* \setminus U(D)$. Then there exists $d \in \gcd(S)$ which is unique up to units, which can be written as $d = c_1 s_1 + c_2 s_2 + \cdots + c_k s_k$, $c_i \in D$.*

Proof. Note that (S) is an ideal of D generated by S. Since D is a PID there exists some $d \in D$, with $(s) = (d)$. Note that $S = \{a_1 s_1 + \cdots + a_k s_k \mid a_i, \ldots, a_k \in D\}$. Here $d = c_1 s_1 + \cdots + c_k s_k$ for $c_i \in D$. For any $s \in S$, $s \in (s)$, and $s \in (S) = (d) \Rightarrow d \mid s \Rightarrow d$ is a common divisor of s. Suppose a is a common divisor of s. Then $a \mid s_i$, for $1 \leq i \leq k$. Then $s_i = ar_i$, for $1 \leq i \leq k$. Then $d = c_1 a r_1 + c_2 a r_2 + \cdots c_k a r_k \Rightarrow a \mid d$. Then $d \in \gcd(S)$. □

Theorem 19.8 (Relation of primes and irreducibles in PID)**.** *Let D be a PID, and $r \in D^*$. The following are equivalent:*

(1). r is prime,

(2). r is irreducible,

(3). (r) is maximal.

Proof. Assume (1), and we have proven (1) ⇒ (2) for commutative integral domains. Assume (2), and let $I \triangleleft D$, where $(r) \subseteq I \subseteq D$. Since D is a PID, there exists $d \in D$ s.t. $I = (d)$. Therefore, $(r) \subseteq (d) \subseteq D$. Thus, $r = cd$, where $c \in D$. Since r is irreducible, either c is a unit, or d is a unit. If c is a unit, then the ideal $(r) = (cd) = (d)$. Otherwise, if d is a unit, then $(d) = D$. Hence, (r) is maximal. Finally, (3) ⇒ (1) is immediate, since (r) maximal ⇒ (r) is prime ⇒ r is prime. □

19.2 Unique Factorization Domains

Definition 19.9 (UFDs)**.** A commutative integral domain is a *unique factorization domain* if the following hold.

(1). Each nonzero element is either a unit or can be written as a product of irreducible elements of D.

(2). The decomposition / factorization in part (1) is unique up to the ordering of irreducibles and units.

Example 19.10. A field is trivially a UFD.

Proposition 19.11. *If R is a UFD, then so is $R[x]$.*

Example 19.12. Consider the ring of Gaussian integers, $\mathbb{Z}[i] = \{a + bi \mid a, b \in Z\}$, $i^2 = -1$. Consider the subring $R = \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$. Then R is not a UFD. Consider $4 = 2 \cdot 2 = (2i) \cdot (-2i)$.

Theorem 19.13 (Greatest common divisors in a UFD)**.** *Let D be a UFD, and consider $S = \{s_1, \ldots, s_n\} \subseteq D^* \setminus U(D)$. Then there exists nonassociate irreducibles $p_1, p_2, \ldots, p_m$ such that $s_i = u_i p_1^{f(i,1)} p_2^{f(i,2)} \cdots p_m^{f(i,m)}$, where $u_i \in U(D)$, and $f(i,j) \geq 0$. Furthermore, $s_i \mid s_j$ iff $f(i,k) \leq f(j,k)$ for $1 \leq k \leq m$.*

20 Lecture 18: Mon. Apr. 15

20.1 More on UFDs, PIDs

Lemma 20.1 (Equivalence of primes and irreducibles in UFD)**.** *Let D be a UFD, and let $r \in D$. Then r is irreducible iff r is prime.*

Proof. The converse is true for any commutative integral domain. Suppose r is irreducible in D, and let $r \mid ab$, $a, b \in D$. Then let $ab = rs$ for $s \in D$. If a or b are units then we may conclude r is prime. So assume that a, b are not units. Now, note that we can write $a = u_a a_1 a_2 \cdots c_m$ where $u_a \in U(D)$, and $a_1, \ldots, a_m$ are irreducibles. Similarly, write $b = u_b b_1 \cdots b_n$, for $u_b \in U(D)$, and b_i irreducibles. And write $s = u_s s_1 \cdots s_\ell$, $u_s \in U(D), s_i$ irreducible. Thus, $u_a u_b a_1 \cdots a_m b_1 \cdots b_n = U_s r s_1 \cdots s_\ell$. Since r is irreducible, we know that there is some a_i or b_j which is associate with r. Then we are done, since $r \mid a$, or $r \mid b$. □

Theorem 20.2 (PIDs are UFDs)**.** *If D is a PID, then D is a UFD.*

Proof. Suppose $up_1 \cdots p_m = vr_1 \cdots r_n$, where $u, v \in U(D)$, p_i, r_j are irreducibles. Because D is a PID, irreducibles are primes. By Theorem 18.11, we know $m = n$, up to relabelling, p_i and r_i are associate.

Now, we claim for each $t \in D^* \setminus U(D)$, there exists an irreducible in D which divides t. If t itself is irreducible, then we are done. If t is not irreducible, then $t = r_1 s_1$, $r_1, s_1 \notin U(D)$. If either r_1, s_1 are irreducible, the we are done. If neither of r_1, s_1 are irreducible, write $s_1 = r_2 s_2$, with $r_2, s_2 \notin U(D)$. We repeat this process until step n, in which we have $s_{n-1} = r_n s_n$. If either s_n, r_n are irreducible, then we are done. The only way that this decomposition process does not terminate is that we have an infinite sequence of non-irreducible non-unit $\{s_i\}_{i=1}^{\infty}$, such that $s_i \mid s_{i+1}$. Now consider the infinite chain of principal ideals $(s_1) \subset (s_2) \subset \cdots \subset (s_i) \subset \cdots$. We claim (s_i) is a proper ideal of (s_{i+1}). Otherwise, suppose $(s_i) = (s_{i+1}) = (r_{i+1} s_{i+1}) \Rightarrow r_{i+1} \in U(D)$, which is a contradiction.

Consider $I = \bigcup_{i=1}^{\infty}(s_i)$. We claim $I \triangleleft D$. Since D is a PID, there exists some $d \in D$ such that $I = (d)$. Since $\{s_i\}_{i=1}^{\infty}$ is a sequence of nonirreducible elements, I cannot contain a unit. If a unit $u \in I$, then $u \in (s_i)$, for some i, hence $(s_i) = D$. This implies $s_i \in U(D)$, which is impossible. Since $I = (d)$ is a proper ideal of D, $d \in D^* \setminus U(D)$. Since $d \in I$, then $d \in (s_i)$, where i is the smallest possible integer. Now, $(d) \subseteq (s_i)$. Recall $I = \bigcup_{i=1}^{\infty}(s_i)$, therefore, $I = (s_i)$, which is a contradiction, since for any k, $k > i$, $s_k \notin (s_i)$, and $s_k \notin I$, but I shall contain s_k.

Now, for $t \in D^* \setminus U(D)$, let r_1 be an irreducible factor of t. Then $t = r_1 x_1$, for some $x_1 \in D$. If $x_1 \in U(D)$, we are done. If $x_1 \in D^* \setminus U(D)$, then $x_1 = r_2 x_2$, and where r_2 is irreducible. If this decomposition process terminates at step n, then we have our $x_{n-1} = r_n x_n$, with $x_n \in U(D)$, we have found a decomposition for t. If this process does not terminate, then we may extract $\{x_i\}_{i=1}^{\infty}$ an infinite sequence of nonunit nonirreducible elements, with $x_i \mid x_{i+1}$. However, we have already shown that such infinite sequences cannot exist. □

21 Lecture 19: Wed. Apr. 17

21.1 Euclidean Domains

Example 21.1 (Division Algorithm in $\mathbb{Z}$)**.** In $\mathbb{Z}$, there exists a natural norm $d(a) = |a|$ for each $a \in \mathbb{Z}$. Let $a, b \in \mathbb{Z}$, be nonzero, and let $b > 0$. Then there exists $q \in \mathbb{Z}$ such that $a = qb + r$, for $r = 0$, or $|r| < |b|$. Suppose $b < 0$, then $-b > 0$, and there exists some $q \in \mathbb{Z}$ s.t. $a = q(-b) + r$, where $r = 0$, or $|r| < |-b|$.

Definition 21.2 (Euclidean norm, Euclidean domain)**.** Let D be a commutative integral domain. A euclidean norm is a function $d\colon D^* \to \mathbb{Z}_+ \cup \{0\}$. For $a, b \in D^*$, the following hold true:

(1) $d(a) \leq d(ab)$,

(2) $\exists\, q, r \in D$, s.t. $a = qb + r$, where $r = 0$, or $d(r) < d(b)$.

The ring D is called a Euclidean domain if there exists a Euclidean norm on D.

Note. In some textbooks, $d\colon D \to \mathbb{Z}_+ \cup \{0\}$, where $d(0) = 0$, and only (2) holds.

Example 21.3 (Trivial euclidean norms)**.** Suppose $\mathbb{F}$ is a field, then define a trivial norm, $d(a) = 0$, for $a \in \mathbb{F}^*$.

Example 21.4 (Polynomial ring euclidean norms)**.** Define $d\colon \mathbb{F}[x]^* \to \mathbb{Z}_+ \cup \{0\}$, where for each $f \in F[x]^*$, $d(f) = \deg(f)$. To verify that d is a euclidean norm, let $f(x), g(x) \in \mathbb{F}[x]^*$. Since degrees are nonnegative, $d(f(x)) = \deg(f(x)) \leq \deg(f(x)) + \deg(g(x)) = \deg(f(x)g(x)) = d(f(x)g(x))$. Also, we can always find some $q(x), r(x) \in \mathbb{F}[x]$ s.t. $f(x) = q(x)g(q) + r(x)$, where $r(x) = 0$, or $\deg(r(x)) < \deg(g(x))$.

Theorem 21.5 (Division Algorithm in Euclidean Domains)**.** *Let b be a euclidean domain, with euclidean norm d. Let $a, b \in D^*$. Then $a = q_0 b + r_0$. If $r_0 = 0$, then we are done, and we have found that* $\gcd(a, b) = b$*. Otherwise, $d(r_0) < d(b)$, and we let $b = q_1 r_0 + r_1$, where if $r_1 = 0$, then* $\gcd(a, b) = r_0$*, otherwise $r_0 = q_2 r + r_2$. This process must terminate at some nth step, where we find $r_{n-1} = q_n r_n$, and* $\gcd(a, b) = r_n$.

Sketch. Since the norm of each remainder is strictly less than its quotient, this process must terminate. □

Theorem 21.6 (Gcds in Euclidean Domain)**.** *Let D be a euclidean domain, with a euclidean norm d. Let $a, b \in D^*$. Then* $\gcd(a, b)$ *can be derived from the division algorithm.*

Theorem 21.7 (Euclidean domains are PIDs)**.** *If D is a euclidean domain, then D is a PID.*

Proof. Let d be a euclidean norm on D. Let $I \trianglelefteq D$. It suffices to find $u \in D$, $u \in D$, s.t. $I = (u)$. If $I = (0)$, then take $u = 0$, and we are done. If $I \neq (0)$, then select an element $u \in I \setminus \{0\}$, such that $d(u) \leq d(v)$ for all $v \in I$ which we find since we assume the well-ordering principle. For any $v \in I$, write $v = qu + r$, subject to $r = 0$, or $d(r) < d(u)$. Since $r = v - qu \in I$, we cannot have $d(r) < d(u)$, hence, $r = 0$. Hence, $v = qu$, therefore $I = (u)$. Therefore, D is a PID. □

Example 21.8 ($\mathbb{Z}[x]$ is not a Euclidean domain)**.** It suffices to prove that $\mathbb{Z}[x]$ is not a PID. We know $\mathbb{Z}[x]$ is not a PID because $(2, x)$ is not principal.

Lemma 21.9 (Euclidean norm and units)**.** *Let D be a euclidean domain with euclidean norm d. Then $d(1) \leq d(r)$, for all $r \in D^*$, and for $u \in D^*$, $u \in U(D)$ iff $d(u) = d(1)$.*

Proof. For all $r \in D^*$, $d(1) \leq d(1r) = d(r)$. Since $u \in U(D)$, $u \neq 0$, which implies $d(u) \geq 1$. Also, $d(u) \leq d(uu^{-1}) = d(1)$, so $d(u) = d(1)$. For the converse, apply the division algorithm to 1 and $u \in D^*$, so that $1 = qu + r$. If $r = 0$, we are done, since q has an inverse. Otherwise, $d(r) < d(u)$, but $d(u) = d(1)$, and $d(1) \leq d(r)$ for all $r \in D^*$, so this is a contradiction. □

Example 21.10. Recall the norm we defined over the Gaussian integers. That is, $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$. It is nontrivial to show that N is a euclidean norm, but given this, an element $u \in \mathbb{Z}[i]$ is a unit iff $N(u) = N(1) = 1$, that is $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$.

21.2 Multiplicative Norms

Definition 21.11 (Multiplicative norm)**.** Let D be a commutative integral domain $d\colon D \to \mathbb{Z}_+ \cup \{0\}$ be a function satisfying

(1) $d(r) = 0$ iff $r = 0$,

(2) $d(rs) = d(r)d(s)$ for all $r, s \in D$.

Then d is called a multiplicative norm on D.

Example 21.12. As before, the norm N we defined over the Gaussian integers is a multiplicative norm.

22 Lecture 20: Mon. Apr. 22

Lemma 22.1 (Multiplicative norms)**.** *Let D be an integral domain with multiplicative norm d. The following holds true:*

(1) for all $u \in U(D)$, $d(u) = 1$. If d is also a Euclidean norm, then $d(u) = 1$ if and only if $u \in U(D)$,

(2) $d(r) \leq d(rs)$ for all $r, s \in D^*$.

(3) If $r \in D$ satisfies $d(r)$ for some prime p, then r is an irreducible in D.

Proof of (1). Since $d(1) = d(11) = d(1)d(1)$. We know $d(1) = 0$ or $d(1) = 1$. Take $u \in U(D)$, and consider $d(u)d(u^{-1}) = d(1) = 1$. □

Proof of (3). Let $r = ab$, $a, b \in D$. Suppose $d(r) = p$. Then $p = d(r) = d(ab) = d(a)d(b)$. From this we get $d(a) = 1$ or $d(b) = 1$, so that a or b is a unit. Therefore, r is irreducible. □

Example 22.2. Consider $\mathbb{Z}[i]$, and define the norm N, $N(a + bi) = a^2 + b^2$. Then we claim N is a multiplicative norm.

22.1 Polynomial Rings

Proposition 22.3 (Polynomial ring over integral domain)**.** *See Proposition 14.2.*

Example 22.4. Let $R = \mathbb{Z}_4$, which is not an integral domain. Then $R[\mathbb{Z}_4]$ is not an integral domain. Let $f(x) = 2x$, and $g(x) = 2(x) + 1$. Then $\deg(f(x)g(x)) = \deg(2x(2x + 1)) = \deg(4x^2 + 2x) = \deg(2x) = 1$, but $\deg(f(x)) + \deg(g(x)) = 2$.

Proposition 22.5 (Ideals in R and $R[x]$)**.** *Let I be an ideal of the commutative ring R. Let $(I) = I[x]$. Then (I) is the ideal of $R[x]$ generated by I. Also, $R[x]/(I) \cong (R/I)[x]$. In particular, if I is a prime ideal of R, then (I) is a prime ideal of $R[x]$.*

Proof. There is a natural mapping $\varphi\colon R[x] \to (R/I)[x]$, where φ is operated by taking modulo I for each coefficient of a polynomial in $R[x]$. We claim φ is a surjective ring homomorphism. Consider $\ker\varphi = \{f(x) \in R[x] \mid \varphi(f) = 0\}$. Then $\ker\varphi$ is the set of all elements whose coefficients are elements of I. This is precisely $I[x]$, which we set to (I). By the first isomorphism theorem, $R[x]/(I) \cong (R/I)[x]$. Suppose I is a prime ideal of R. Then R/I is an integral domain, and therefore, $(R/I)[x]$ is an integral domain. This forces (I) to be a prime ideal of $R[x]$. □

Example 22.6. Let $n\mathbb{Z}$ be an ideal of $\mathbb{Z}$. Then $\mathbb{Z}[x]/n\mathbb{Z}[x] \cong (\mathbb{Z}/n\mathbb{Z})[x]$. If n is prime, then $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, which implies $p\mathbb{Z}[x]$ is a prime ideal of $\mathbb{Z}[x]$. Hence $\mathbb{Z}[x]/p\mathbb{Z}[x]$ and $\mathbb{Z}/p\mathbb{Z}[x]$ are integral domains.

Lemma 22.7 (Polynomial Evalutation)**.** *Let S be a subring of R. For any element $\alpha \in R$, define the mapping $\phi_\alpha \colon S[x] \to R$ such that for $f(x) \in S[x]$, $\phi_\alpha = f(\alpha)$. We claim ϕ_α is a ring homomorphism, called the evaluation at α.*

Definition 22.8 (Zeros of a polynomial)**.** Let S be a subring of R. Let f be a nonzero polynomial and $\alpha \in R$. Then $\phi_\alpha(f)$, the evaluation of f at α is denoted $f(\alpha)$. If $f(\alpha) = 0$, then α is a zero or root of f in R.

Lemma 22.9 (Roots and divisibility)**.** *Suppose $R[x]$ is a UFD. Let $f \in R[x]$. Then $\alpha \in R$ is a root of $f(x)$ if and only if $(x - \alpha) \mid f(x)$.*

Proof. Assuming the converse, we can write $f(x) = (x-\alpha)g(x)$, for $g(x) \in R[x]$. Clearly $f(\alpha) = 0$. Let $\alpha \in R$ be a zero of $f(x) \in R[x]$. Since $R[x]$ is a UFD, then we can write $f = up_1p_2 \dots p_k$, with $u \in U(R[x])$, and p_i irreducible. Then

$$0 = f(\alpha) = u(\alpha)p_1(\alpha) \dots p_k(\alpha),$$

and since $R[x]$ is an integral domain, at least one of p_i is such that $p_i(\alpha) = 0$. Assume w.l.o.g. $p_1(\alpha) = 0$. Write $r_1 = p_1 \in R[x]$, and let $d_1 = \deg(r_1)$. Let c_1 be the leading coefficient of r_1. Let $r_2(x) = r_1(x) - c_1x^{d_1-1}(x - \alpha)$. Let $d_2 = \deg(r_2(x)) < d_1$. Now, $r_2(\alpha) = 0$. If $r_2(x) = 0$, since $r_1(x) = c_1x^{d_1-1}(x - \alpha)$. If $r_2(x) \neq 0$, continue this process. □

23 Lecture 21: Wed. Apr. 24

23.1 Roots of Polynomials

Corollary 23.0.1 (Degree and number of roots)**.** *Suppose $R[x]$ is a UFD and let $f \in S[x]$ with S being a subring of R and $\deg(f) = d \geq 1$. Then $f(x)$ has at most d roots in R.*

23.2 Polynomial Rings as Euclidean Domains and PIDs

Theorem 23.1 (Polynomial rings over fields as Euclidean domains)**.** *Let $\mathbb{F}$ be a field. Then the polynomial ring $\mathbb{F}[x]$ is a Euclidean domain. Specifically if $a(x)$ and $b(x)$ are two polynomials in $\mathbb{F}[x]$, with $b(x)$ nonzero, then there exists unique $q(x), r(x) \in \mathbb{F}[x]$ such that $a(x) = q(x)b(x) + r(x)$, with $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$.*

Proof. If $a(x) = 0$, take $q(x) = r(x) = 0$. Assume $a(x) \neq 0$. Let $\deg(a(x)) = n$, $\deg(b(x)) = m$. If $n < m$, then set $q(x) = 0$, and $r(x) = a(x)$, so assume $n \geq m$. We proceed by induction on n. Let $n = 1$, then $a(x) = a_1x + a_0$, and $b(x)$ is either b_0 or $b_1x + b_0$. In both cases, the division is straightforward. Assume that the conclusion holds for each $a(x)$ with degree less than n. Consider $a(x)$ with degree n. Write

$$a(x) = \sum_{i=0}^{n} a_ix^i,\ a_n \neq 0$$

and

$$b(x) = \sum_{i=0}^{m} b_ix^i,\ b_n \neq 0.$$

Consider $a'(x) = a(x) - (a_n/b_m)x^{n-m}b(x)$, and we have $\deg(a'(x)) < n$. By hypothesis, there exists $q'(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that $a'(x) = q'(x)b(x) + r(x)$, with $r(x) = 0$, or $\deg(r(x)) < \deg(b(x))$. Let $q(x) = q'(x) + (a_n/b_m)x^{n-m}$. Then $a(x) = q(x)b(x) + r(x)$.

To prove uniqueness, assume $a(x) = q(x)b(x) + r(x)$, $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$, and $a(x) = q'(x)b(x) + r'(x)$ with $r'(x) = 0$ or $\deg(r'(x)) < \deg(b(x))$. Then $r(x) = a(x) - q(x)b(x)$, $r'(x) = a(x) - q'(x)b(x)$, which gives us

$$r(x) - r'(x) = (q'(x) - q(x))b(x).$$

Since

$$\deg(r(x) - r'(x)) \leq \max\{\deg(r(x)), \deg(r'(x))\},$$

and

$$\deg((q'(x) - q(x))b(x)) = \deg(q(x) - q(x)) + \deg(b(x)) \geq \deg(b(x)),$$

we get

$$\deg(b(x)) \leq \max\{\deg(r(x)), \deg(r'(x))\},$$

precisely a contradiction. □

Corollary 23.1.1. *If $\mathbb{F}$ is a field, $\mathbb{F}[x]$ is a euclidean domain, implying $\mathbb{F}[x]$ is a PID.*

Example 23.2. Let p be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is a field, and thus $\mathbb{Z}/p\mathbb{Z}[x]$ is a PID. Also, $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{Z}/p\mathbb{Z}[x]$, so $\mathbb{Z}[x]/p\mathbb{Z}[x]$ is a PID.

Example 23.3. Consider $\mathbb{Q}[x, y] = (\mathbb{Q}[x])[y]$. Then $\mathbb{Q}[x, y]$ is not a PID. To prove this, consider (x, y), which is not a principal ideal in $\mathbb{Q}[x, y]$.

Theorem 23.4. *Let $\mathbb{F}$ be a field, and $U \trianglelefteq \mathbb{F}[x]$. Then $U = (0)$, or $U = (f(x))$, where $f(x)$ is the unique monic polynomial of least degree in U.*

Proof. Since $\mathbb{F}[x]$ is a PID, $U = (h(x))$ for some $h(x) \in \mathbb{F}[x]$. If $h(x) = 0$, then $U = (0)$. If $h(x) \neq 0$, let λ be the leading term of $h(x)$, and set $f(x) = \lambda^{-1}h(x)$, and f is monic. Clearly, $U = (h(x)) = f(x)$. If $g(x) \in U$, then $g(x) = f(x)a(x)$, and $\deg(g(x)) \geq \deg(f(x))$. Let $f'(x)$ be a monic polynomial in U such that $U = (f'(x))$. Then $\deg(f'(x)) = \deg(f(x))$. Since $f'(x), f(x)$ are both monic, $f'(x) - f(x)$ should have degree less than $f(x)$, but this is a contradiction, since we assumed $f(x)$ has the minimal degree in U. □

Example 23.5. The ring $\mathbb{Z}[x]$ is not a PID. Choose a proper ideal (m) of $\mathbb{Z}$, with $m \geq 2$. Define an ideal $U \trianglelefteq \mathbb{Z}[x]$ by letting $U = \{f(x) \in \mathbb{Z}[x] \mid f(0) \in (m)\}$. Suppose $U = (f)$ for some $f \in \mathbb{Z}[x]$. Since $f(x) + m \in U$, we have $f(x) + m = g(x)f(x)$, $g(x) \in \mathbb{Z}[x]$. Therefore, $(1 - g(x))f(x) = m$, so $f(x) \mid m$, therefore $f(x) = \pm m$, ($f(x)$ cannot be a proper divisor of m) and $U = (m)$. However, note that $x + m \in U = (m)$, so $x + m = mj(x)$, for some $j(x) \in \mathbb{Z}[x]$. Then there exits some $a \in \mathbb{Z}$, $am = 1$, but $m \geq 2$.

24 Lecture 22: Sick again

24.1 Primitive Polynomials

In this lecture, we cover primitive polynomials, and Gauss' lemma for $\mathbb{Z}[x]$. Let $f(x) \in \mathbb{Z}[x]$. We call $f(x)$ primitive if the greatest common divisor of all its coefficients is 1. Gauss' Lemma for $\mathbb{Z}[x]$ states that $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if f is irreducible in $\mathbb{Q}[x]$.

Definition 24.1 (Primitive polynomial)**.** Let D be a commutative integral domain, and $f \in D[x]$. The content of $f(x)$, denoted by $c(f)$ is the greatest common divisor of the coefficients of $f(x)$. If $c(f)$ is a unit, then $f(x)$ is a primitive polynomial.

Lemma 24.2 (Product of primitive polynomials)**.** *Let D be a UFD, and $f, g \in D[x]$ be primitive polynomials. Then fg is a primitive polynomial.*

Corollary 24.2.1. *Let D be a UFD and $f, g \in D[x]$. Then $c(fg)$ and $c(f)c(g)$ differ by a unit.*

Lemma 24.3 (Gauss' Lemma)**.** *Let R be a UFD, with field of fractions F, and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$, then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$, and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.*

Proof. The coefficients of the polynomials on the right hand side of the equation $p(x) = A(x)B(x)$ are elements in the field F, hence are quotients of elements from the UFD R. Multiplying through by a common denominator for all these coefficients, we obtain $dp(x) = a'(x)b'(x)$, where now $a'(x)$ and $b'(x)$ are elements of $R[x]$ and d is a nonzero element of R. If d is a unit in R, the proposition is true with $a(x) = d^{-1}a'(x)$ and $b(x) = b'(x)$. Assume d is not a unit and write d as a product of irreducibles in R, say $d = p_1 \cdots p_n$. Since p_1 is irreducible in R, the ideal (p_1) is prime, so the ideal $p_1R[x]$ is prime in $R[x]$, and $(R/p_1R)[x]$ is an integral domain. Reducing the equation $dp(x) = a'(x)b'(x)$ modulo p_1, we obtain $0 = \overline{a'(x)b'(x)}$ in this integral domain. Hence, one of the two factors, say $\overline{a'(x)}$ must be 0. But this means that all the coefficients of $a'(x)$ are divisible by p_1, so that $\frac{1}{p_1}a'(x)$ also has coefficients in R. In other words, in the equation $dp(x) = a'(x)b'(x)$, we can cancel a factor of $p+1$ from d on the left, and from either $a'(x)$ or $b'(x)$ on the right, and still have an equation in $R[x]$. But now the factor d on the left hand side has one fewer irreducible factors. Proceeding in the same fashion with each of the remaining factors of d, we can cancel all of the factors of d into the two polynomials on the right hand side, leaving an equation $p(x) = a(x)b(x)$ with $a(x), b(x) \in R[x]$ and with $a(x), b(x)$ being F-multiples of $A(x), B(x)$ respectively. □

Lemma 24.4 (Factorization of primitive polynomials)**.** *Let D be a UFD and $f \in D[x]$ be a primitive polynomial. Then $f(x)$ can be written uniquely as the product of irreducible elements in $D[x]$.*

Theorem 24.5. *The ring R is a UFD if and only if $R[x]$ is a UFD.*

Proof. Since R is a subring of $R[x]$, then $R[x]$ being a UFD implies R is a UFD. For the forward implication, let $f(x) \in R[x]$. We can write $f(x) = ap(x)$, for $a = c(f) \in R$, and $p(x) \in R[x]$ primitive. Since R is a UFD, a has a unique factorization into irreducibles in R, which are also irreducibles in $R[x]$. Also, $p(x)$ has a unique factorization into irreducibles in $R[x]$. □

Corollary 24.5.1. *If R is a UFD, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a UFD.*

25 Lecture 23: Wed. May 1

25.1 Irreducibility Criterion

For some polynomial p, its irreducibility can be easily deduced by checking its coefficients.

Proposition 25.1 (Restricting Rational Roots of Polynomials)**.** *Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, with $a_i \in \mathbb{Z}$, and $a_n \neq 0$. If $r/s \in \mathbb{Q}$ with $\gcd(r,s) = 1$ is a root of $p(x)$, then $r \mid a_0$ and $s \mid a_n$. In particular, if $p(x)$ is monic, and $p(d) \neq 0$, for all integers d, $d \mid a_0$, then $p(x)$ has no roots in $\mathbb{Q}$.*

Proof. Let r/s be a root to a monic polynomial $p(x)$, where $gcd(r,s) = 1$. Let us assume for now that $r \mid a_0$ and $s \mid a_n = 1$, which forces $s = \pm 1$. Then the integral root r must divide a_0. For the first claim, if we know $p(r/s) = 0$, then we simply plug in r/s into p, yielding

$$\begin{aligned} p(r/s) &= a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s) = 0 \\ p(r/s)s^n &= a_n r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0 \\ &\Rightarrow a_n r^n = s(-a_{n-1}r^{n-1} - \cdots - a_0 s^{n-1}), \end{aligned}$$

so $s \mid a_n r^n$, and by assumption, s, r are corpime, so $s \mid a_n$. Similarly, solving the equation for $a_0 s^n$ shows $r \mid a_0$. □

Example 25.2. Let p be a prime. Then $x^2 - p$ and $x^3 - p$ are irreducible in $\mathbb{Q}$.

Example 25.3. Consider $p(x) = x^2 + x + 1 \in \mathbb{Z}[x]$, and reduce it modulo 2, yielding $\overline{p(x)} = x^2 + x + 1 \in \mathbb{Z}_2[x]$. We claim that $\overline{p(x)}$ is irreducible over $\mathbb{Z}_2[x]$. We claim that this is sufficient to show that $p(x)$ is irreducible in $\mathbb{Z}[x]$.

Proposition 25.4 (Reducing modulo an ideal to test for irreducibility)**.** *Let I be a proper ideal in the commutative integral domain R and let $p(x)$ be a nonconstant monic polnyomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials with smaller degree, then $p(x)$ is irreducible in $R[x]$.*

Proof. Let I be a proper ideal of R. By contrapositive, asssume $p(x)$ is reducible in $R[x]$. Then $p(x) = a(x)b(x)$, with $a(x), b(x) \in a(x), b(x) \in R[x]$, $\deg(a) > 0$, $\deg(b) > 0$. Since p is monic, then the leading coefficients of a, b are not in I, since I is proper. Reduce the coefficients in $p(x) = a(x)b(x)$ modulo I We want to assert that $\deg(a(x)) = \deg(\overline{a(x)}) > 0$, and vice versa for $b(x)$, since otherwise $\overline{p(x)}$ is a trivial factorization. Assuming this, we have found a nontrivial factorization of $\overline{p(x)}$ in $(R/I)[x]$, hence, $\overline{p(x)}$ is reducible in $(R/I)[x]$. □

Example 25.5. The polynomial $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$.

Theorem 25.6 (Eisenstein's Criterion)**.** *Let P be a prime ideal of the commutative integral domain R, and let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$, with $n \geq 1$. Suppose $a_{n-1}, a_{n-2}, \ldots, a_0 \in P$, and $a_0 \notin P^2$. Then $p(x)$ is irreducible over $R[x]$.*

Proof. Assume by contradiction that $p(x)$ is reducible, given the criterion. Then $p(x) = a(x)b(x)$, $a(x), b(x) \in R[x]$, $\deg(a) \geq \deg(b) > 0$. Reduce p by modulo P, and now, $\overline{p(x)} = x^n$. Since P is a prime ideal, R/P is a integral domain. We claim both $\overline{a(x)}, \overline{b(x)}$ have no constant terms. The proof of this lies in the expansion of $a(x)b(x)$. Then the constant term of $p(x)$ is in P^2, but this is contradicting our criterion. □

Corollary 25.6.1 (Eisenstein's Criterion for $\mathbb{Z}[x]$)**.** *Let p be a prime in $\mathbb{Z}$ and $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$, for $n \geq 1$. Then suppose $p \mid a_i, 0 \leq i \leq n-1$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.*

Example 25.7. Let $f(x) = x^4 + 1 \in \mathbb{Z}[x]$. Set $g(x) = f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2 \in \mathbb{Z}[x]$. Apply Eisenstein's criterion for $p = 2$, and find $g(x)$ is irreducible. This implies that $f(x)$ is also irreducible. If $f(x) = a(x)b(x)$, then $g(x) = f(x+1) = a(x+1)b(x+1)$.

Example 25.8. Let $R = \mathbb{Q}[x]$, and let $n \in \mathbb{Z}$, $n \geq 0$. Consider the polynomial $y^n - x \in R[y] = \mathbb{Q}[x][y] = \mathbb{Q}[x, y]$. We claim (x) is a prime ideal of R. This is clear since $R/(x) \cong \mathbb{Q}$, and $\mathbb{Q}$ is a field, which is an integral domain, implying (x) is prime. Apply Eisenstein's criterion for $P = (x)$, and $R = \mathbb{Q}[x]$.

26 Lecture 24: Mon. May 6

26.1 Field Theory

Example 26.1. For p a prime, $\mathbb{Z}_p$ is a field of order p, denoted F_p.

Definition 26.2 (Subfield and Extension Field)**.** Let F be a field. A subset $K \subseteq F$ which is a field with respect to the operations in F is a subfield. We call F an extension field of K, denoted F/K. When $K \neq F$, K is a proper subfield, and F is a proper extension field of K.

Example 26.3. Let K be a subfield of F_p, then K is 0 or F_p.

Example 26.4. Let $p(x) = x^2 - x \in \mathbb{Q}[x]$. By Eisenstein's criterion, $p(x)$ is irreducible over $\mathbb{Q}$. Let θ be a root of $p(x)$ ($\theta = \pm\sqrt{2}$). Denote $\mathbb{Q}(\theta)$ as the field $\mathbb{Q}(\theta) = \{a + b\theta \mid a, b \in \mathbb{Q}\}$. Firstly, $\mathbb{Q}(\theta)/\mathbb{Q}$ can be realized by adjoining a root θ of an irreducible polynomial $p(q)$ over $\mathbb{Q}$. Second, $\mathbb{Q}(\theta)$ is a 2-dimensional vector space over $\mathbb{Q}$.

Definition 26.5 (Prime Field)**.** A field containing no proper subfield is called a prime field. Recall that if R is a ring with identity and no zero divisors, the characteristic of R is either 0 or p, for some prime p.

Theorem 26.6 (Chracteristic of a prime field)**.** *Let F be a prime field with characteristic c. If $c = 0$, then F is isomorphic to $\mathbb{Q}$. If $c = p$, p prime, then F is isomorphic $\mathbb{F}_p$.*

Proof. If $c = p$, then define $\phi\colon \mathbb{Z} \to F$, where $\phi(m) = m \cdot 1_F$. Then $\ker \phi = p\mathbb{Z}$. Then $\mathbb{Z}/p\mathbb{Z} \cong F$. □

Example 26.7. The Euclidean domain $F_p[x]$ has characteristic p. The field of rational functions (field of fractions of $F_p[x]$) is $F_p(x) = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in F_p[x], g(x) \neq 0\}$. The prime field of $F_p(x)$ is F_p.

Proposition 26.8. *Every field is an extension of a prime field.*

Definition 26.9 (Field extensions by adjoining elements)**.** Let F, K, F/K. Let $S \subseteq F$. The field $K(S)$ is defined as the intersection of all subfields F containing S, K, and is the extension field of K. For finite $S = \{\alpha_1, \ldots, \alpha_n\}$, if $|S| = 1$, then $K(S)$ is a simple extension of K, and α is a defining element E over K.

Example 26.10. The real numbers $\mathbb{R}$ are a subfield of $\mathbb{C}$. Adjoining $i \in \mathbb{C}/\mathbb{R}$ to $\mathbb{R}$, we get $\mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$. Alternatively, $x^2 + 1$ is the unique monic irreducible polynomial in $\mathbb{R}[x]$ having i as a root. Now, $(x^2 + 1)$ is a maximal ideal of $\mathbb{R}[x]$. We claim $\mathbb{R}[x]/(x^2 + 1) = \{a + bx \mid a, b \in \mathbb{R}\} \cong \mathbb{C}$. Observe that in $\mathbb{R}[x]/(x^2 + 1)$, $x^2 = -1$.

26.2 Algebraic Extensions

Definition 26.11 (Algebraic Extension)**.** Let F, K, F/K, and let $\alpha \in F$. If α is a root of a nonzero polynomial $f \in K[x]$, then α is algebraic over K. An extension field E is algebraic over K if each element of E is algebraic over K.

Proposition 26.12. *Suppose $\alpha \in F$ is algebraic in K. Set $U = \{f \in K[x] \mid f(x) = 0\}$. Then $U \neq \{0\}$, $U \triangleleft K[x]$. Also, since $K[x]$ is a PID, U is principal for some monic* ***irreducible*** *polynomial $m \in K[x]$, $U = (m)$.*

Lemma 26.13 (Minimal polynomial)**.** *Let $\alpha \in F$ be algebraic over K with minimal polynomial $m(x)$ over K. Then*

(1) $m(x)$ is irreducible over K,

(2) m is the monic polynomial in $K[x]$ of least degree having α as a root,

(3) α is a root of $f \in K[x]$ if and only if $m \mid f$.

26.3 Vector Spaces

Definition 26.14 (Vector space)**.** Let K be a field. A set V is a vector space over K if

(1) $(V, +)$ is an abelian group,

(2) $a(u + v) = au + av$, $(a + b)v = av + bv$, for $u, v \in V$, $a, b \in K$.

(3) $(ab)v = a(bv)$ for $v \in V, a, b \in K$,

(4) $1v = v$, for $v \in V, 1 \in K$.

Example 26.15. If F, K, F/K, F is a vector space over K.

Definition 26.16 (Degree of field extension)**.** Let $F, K, F/K$. Then F is a finite extension of K if F is a finite dimensional vector space over K. The degree of extension is $\dim_K F$.

Example 26.17. The complex numbers $\mathbb{C}$ are a degree 2 extension over $\mathbb{R}$ ($\dim_{\mathbb{R}} \mathbb{C} = 2$), with the basis $\{1, i\}$.

Example 26.18. The field of rational functions $\mathbb{R}(x)$ is an infinite degree extension over $\mathbb{R}$.

Lemma 26.19 (Degree of field extension)**.** *Let E/F, F/K be finite extensions. Then E/K is a finite extension.*

27 Lecture 25: Wed. May 8

27.1 Minimal Polynomials

Theorem 27.1 (Finite extension is algebraic)**.** *Every finite extension of K is algebraic over K.*

Proof. Let F be a finite extension of K; let $\deg_K F = d < \infty$. Choose $\alpha \in F$, and consider $A = \{\alpha^j \mid 0 \leq j \leq d\}$. Then A must be linearly dependent over K. Then there exists $a_0, \ldots, a_d$, not all zero, such that $\sum_{j=0}^{d} a_j \alpha^j = 0$. Hence, $f(x) = \sum_{j=0}^{d} a_j x^j \in K[x]$ is a nonzero polynomial having α as a root. This shows precisely that α is algebraic over K. □

27.2 Simple Extensions

Theorem 27.2 (Simple extensions)**.** *Let $\alpha \in F$ be algebraic of degree d over K, and let $m \in K[x]$ be the minimal polynomial of α over K. We have the following*

(1). $K(\alpha) \cong K[x]/(m)$,

(2). $\deg_K K(\alpha) = d$, and $\{x^i \mid 0 \leq i \leq d-1\}$ is a basis for $K(\alpha)/K$.

(3). Every $\beta \in K(\alpha)$ is algebraic over K, and its degree over K is a divisor of d.

Proof. For (1), define a mapping from $\phi\colon K[x] \to K(\alpha)$ such that $\phi(f(x)) = f(\alpha)$. It is clear ϕ is surjective. Then $\ker\phi = \{f \in K[x] \mid f(\alpha) = 0\}$. By definition, this is also equal to the minimal polynomial m over K. Our result follows by the first isomorphism theorem. For (2), observe that α is not a root of a polynomial over K with degree less than d. Then $\{\alpha^i \mid 0 \leq i \leq d-1\}$ is linearly independent over K. By (1), every $\beta \in K(\alpha)$ can be written as $\beta = f(\alpha)$. We know $K[x]$ is a Euclidean domain, so $f(x) = q(x)m(x) + r(x)$ satisfying $r(x) = 0$ or $\deg(r(x)) < \deg(m(x))$. Now, $\beta = f(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = r(\alpha)$. If $r(\alpha) = 0$, then $\beta = 0$. If $\deg(r(x)) < \deg(m(x)) = d$, then $\beta \in \langle \alpha^i \mid 0 \leq i \leq d-1\rangle_K$. Hence, $\{\alpha^i \mid 0 \leq i \leq d-1\}$ is a spanning set of $K(\alpha)$ over K, and since it is linearly independent, it shall be a basis. For (3), since $K(\alpha)/K$ is finite, it is algebraic. Finally, $\deg_K(K(\alpha)) = \deg_{K(\beta)}(K(\alpha))\deg_K(K(\beta))$. □

Theorem 27.3 (Simple extensions driven by irreducible polynomials)**.** *Let $f \in K[x]$ be an irreducible polynomial over K. Then there exists a simple algebraic extension of K with a root of f as its defining element.*

Example 27.4. Consider $f(x) = x^2 + 2x + 3$ over F_5. One can check that $f(x)$ has no roots over F_5, so that it is irreducible over F_5. Assume α is a root of $f(x)$, and apply Theorem 27.2 to find that $F_5(\alpha) \cong F_5[x]/(t)$, for t being the minimal polynomial over F_5.

27.3 Intro to Finite Fields

In 888, we proved that all finite fields have order p^k, for some prime p, k integer. The proof is elegant, but I won't show it to you.

Lemma 27.5 (Defining elements in simple extensions)**.** *Let $f \in K[x]$ be irreducible. If α, β are roots of f, then $K(\alpha)$ and $K(\beta)$ are isomorphic under an isomorphism mapping α to β, and fix every element of K.*

28 Lecture 26: Mon. May 13

28.1 Splitting Fields

Let $f(x) \in F[x]$. Recall that there exists an extension field K over F containing a root α of $f(x)$. Equivalently $x - \alpha$ is a factor of $f(x)$ in $K[x]$.

Definition 28.1 (Splitting field)**.** The extension field K of F is a splitting field for $f(x) \in F[x]$ if $f(x)$ factors completely into linear terms in $K[x]$ (some authors say that $f(x)$ splits in K) and if $f(x)$ does not split in any proper subfield of K.

Example 28.2. Suppose for $f(x) \in K[x]$, $\alpha_1, \ldots, \alpha_n$ are all the roots of $f(x)$. Then a splitting field of f over K is $K(\alpha_1, \ldots, \alpha_n)$.

Example 28.3 (Cyclotomic fields)**.** Consider the splitting field of $x^n - 1$ over $\mathbb{Q}$. That is, $\mathbb{Q}(\omega_1, \ldots, \omega_n)$, for $\omega_j = e^{\frac{2\pi j}{n}}$, for $j \in [n]$. We also claim that $\{\omega_1, \ldots, \omega_n\} = \langle \omega_1 \rangle$.

Proposition 28.4 (Bound for extension degrees)**.** *Let $f \in K[x]$ of degree $d > 0$. Then there exists an extension field F/K in which f has a root. Moreover, $[F : K] \leq d$.*

Theorem 28.5 (Splitting field)**.** *Let K be a field, and $f \in K[x]$ be a polynomial with $\deg(f) = d \geq 1$. Then there exists a splitting field of F/K with degree at most $d!$. Furthermore, any two splitting fields of f over K are isomorphic under an isomorphism fixing each element of K.*

Proof. With some hand waving, assume f has roots $\alpha_1, \ldots, \alpha_d$. Suppose F_i is an extension field of F_{i-1} containing $\alpha_1, \ldots, \alpha_i$, for $i \in [n]$. Suppose F_d contains each root of f. Then $[F_d : K] = [F_1 : K][F_2 : F_1] \cdots [F_d : F_{d-1}] \leq d!$. □

28.2 Finite Fields

Theorem 28.6 (Additive structure of finite fields)**.** *The order of a finite field is a power of a prime p. Moreover, $(F, +)$ is an elementary abelian p-group.*

Proof. A finite field is a finite commutative integral domain. Recall that F_p is the prime subfield of any field with characteristic p, for some prime p. Then F is an n-dimensional vector space over F_p. Thus, $|F| = p^n$ for $n \geq 1$. Moreover, by the fundamental theorem of finite abelian groups, $(F, +) \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_n}}$. Since F has characteristic p,

$$(F, +) \cong \overbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}^{n \text{ times}}.$$

□

Example 28.7. We claim there is a unique irreducible polynomial of degree 2 in $F_2[x]$, namely, $f(x) = x^2 + x + 1$. Let α be a root of $f(x)$. Then consider $K = F_2(\alpha) = F_2(\alpha)/(x^2 + x + 1)$. Now $[F_2(\alpha) : F_2] = 2$, and $|K| = 2^2 = 4$. To list the elements, and to prove that the nonzero elements are a cyclic group under multiplication, is part of the homework.

Proposition 28.8 (Order and splitness of $x^q - x$)**.** *Let L be a field of prime characteristic p, and let q be a power of p. Then L contains a subfield of order q if and only if the polynomial $x^q - x$ splits over L. Moreover, $E = \langle \alpha \in L \mid \alpha^q = \alpha \rangle$ is the unique subfield of L with order q.*

Proof. Since $\text{char}(L) = P$ and q is a power of p, then it is routine to verify $E = \{x \in L \mid \alpha^q = \alpha\}$ is a subfield of L. Let $f(x) = x^q - x$, and we claim that E is the set of all roots of f in L. Hence $|E| \leq \deg(f) = q$. Under the definition of a formal derivative, consider $f'(x) = qx^{q-1} - 1 = -1$, which tells us that f has no multiple roots, and thus, $|E| = q$. For the converse, assume that $x^q - x$ splits over L. This tells us that all q roots of $x^q - x$ are in L, and that $|E| = q$. To complete the proof, we need to show that E is unique. □

29 Lecture 27: Wed. May 15

Uniqueness of Proposition 28.8. Let $f(x) = x^q - x$. The conclusion follows if $K \subseteq E$. Suppose $\alpha \in K$. If $\alpha = 0$, then $\alpha \in E$. If $\alpha \neq 0$, then $\alpha \in K^*$. Since K^* is a group under multiplication, $\alpha^{q-1} = 1$. Then $\alpha^q = \alpha$, so $\alpha \in E$. Therefore, $K \subseteq E$. □

Example 29.1. Consider F_8, with degree 3 over F_2. The elements of F_8 will be the eight roots of $x^8 - x = x(x-1)(x^3+x+1)(x^3+x^2+1)$.

Theorem 29.2 (Existence and uniqueness of finite fields of prime power order)**.** *Let q be a power of a prime p. Then there exists a finite field of order q, and every such field is a splitting field of $x^q - x$, over F_p. In particular, all fields of order q are isomorphic.*

Proof. Let L be a splitting field for $f(x) = x^q - x$ over F_p. Then there exists a subfield E of L with $|E| = q$. Consider E_0 to be any field of order q, with prime subfield F_p. By Proposition 28.8, set $L = E_0$. Then there exists a subfield $L_0 \subseteq E_0$, $|L_0| = q$. Then $L_0 = E_0$ is a splitting field of f over F_p. Then $L \cong L_0$. Consider the orders, $q = |E| \leq |L| = |L_0| \leq |E_0| = q$. Hence, $E = L \cong L_0 = E_0$. □

Theorem 29.3 (Subfields of finite fields)**.** *Let F_q be the finite field on order $q = p^n$. Every subfield of F_q has order p^m, $m \mid n$. Conversely, if $m \mid n$, then F_q contains a unique subfield F_{p^m}.*

Proof. Let K be a subfield of F_q with order $k = p^m$. Then F_q is an extension field of K. Then there exists $d \geq 1$ such that $[F_q : k] = d$. Then $|F_q| = |k|^d = k^d = p^{md} = p^n$. Hence $m \mid n$. Conversely if $m \mid n$, then $x^{p^m} - x \mid x^{p^n} - x$. All the roots of $x^{p^m} - x$ are roots of $x^{p^n} - x$. Then F_q contains all the roots of $x^{p^m} - x$. Also, all the roots of $x^{p^m} - x$ form a finite field of order p^m, F_{p^m}. Assume that F'_{p^m} is another subfield of F_q, distinctive from F_{p^m}. Then $|F_{p^m} \cup F'_{p^m}| > p^m$, which implies $x^{p^m} - x$ has more than p^m roots. □

Lemma 29.4. *Let G be a finite group of order n such that for every divisor d of n, there are at most d solutions of $x^d = 1$. Then G is cyclic.*

Proof. Let nd denote the number of order d elements in G. If $a \in G$, $|a| = d$, then the set $\{a^i \mid 0 \leq i \leq d-1\}$ contains all the solutions of $x^d = 1$ in G. Within $\{a^i \mid 0 \leq i \leq d-1\}$, precisely $\phi(d)$ elements have order d. Then $n_d = \phi(d)$ if $d \mid n$ and G contains an order d element, and 0 otherwise. By Lagrange, $n = \sum_{d|n} n_d \leq \sum_{d|n} \phi(d) = n$. So $n_d = \phi(d)$ for each $d \mid n$, and $n_n = \phi(n) \geq 1$. Hence, G must be cyclic. □

Theorem 29.5 (Multiplicative structure of finite fields)**.** *The multiplicative group of a finite field is cyclic.*

Proof. Let F_q be a finite field. Then F_q^* is a finite group of order $q-1$. Consider $x^d = 1$ in F_q^* for each divisor d of n. This equation has at most d roots, so F_q^* is cyclic. □