ALGEBRA I FALL 2023, A. KUSTIN, CLASS NOTES

1. THE RULES AND THE COURSE OUTLINE.

1.A. **Homework.** I will assign and grade homework. Please take it seriously. Please turn the homework in on-time.

Please type your solutions and e-mail me a .pdf version.

Each student should write up a solution to each problem (even if some problems were solved by a group of students.) Write in a professional manner. Make clear claims (not vague claims.) Write in complete sentences; use proper English; define all new terms carefully and completely; and define all notation carefully and completely.

It is a good idea to do some problems on your own. It is also valuable (and much fun) to work with other people. It is legal to look things up as you are doing homework; indeed, if you look hard enough, you can probably find the solution to anything I am likely to ask some place on the Internet.

Arrive at your solution however you like: by yourself, using the Internet, working with other people. Write the answer up by yourself in your own words. Make your answer as clear, understandable, and complete as possible. Give all details in your answer. Explain all notation and new concepts that you use. **Acknowledge all of your sources.**

1.B. **Exams.** There will be three in-class exams (Wednesday, September 20 Wednesday, October 18, and Monday, November 20) and one final exam (Friday, December 15, 4:00–6:30 PM). I'll ask some questions. You will do the best you can with them.

1.C. **Class Attendance.** I expect my students to attend class.

1.D. **Office Hours.** My office hours are 5:15–6:30 Monday and Wednesday.

I do respond to e-mail.

1.E. **References.** I will post my lecture notes on the web. These notes will serve as the text book for the course. I will re-write the notes as the course progresses. One of the main sources will be the notes I used in the past when I taught the course. These older notes were mainly taken from Jacobson [6]. (Dover has reprinted an inexpensive version of this book.) Jacobson was an excellent mathematician and he writes well. (He includes some topics that I don't like; I just skip them.) Also I taught the course from Artin [2] a few times. Artin is a very excellent mathematician. (Artin's book might be pegged at a slightly lower level than the course you are taking. The charming thing about it is that it covers topics that are not usually covered in the first year Algebra course.) In the 1990's every one took Algebra from Hungerford's book [5]; but I am not particularly fond of it. I took many courses from Rotman when I was a graduate student and a copy of an early edition of [8] sits on my desk. I know that other books by Rotman have lots of motivation and are well-organized. There is a decent chance that some of your course will come from [8]. Professors Ballard and Duncan taught 701 from Aluffi [1] in 2015–2016 and 2016–2017, respectively. It is a much different treatment of the material than the course I will teach. I do not have access to a copy. Professors Thorne and Vraciu taught from Dummit and Foote in 2017–2018 and 2018–2019, respectively. Dummit and Foote is the book "everybody learns Algebra from" now-a-days. I do have e-access to it. I may open it during your course; I may not.

The main thing is, make sure you know the name of the topic we are studying at any given time. Once you know the name the topic, then the Internet will lead you to all sorts of treatments of the topic. Find one treatment (from class, or from the Internet, or from some textbook) that resonates with you and then learn the topic very thoroughly.

If I happen to be following some source fairly closely, I will let you know (and if I forget, feel free to ask).

1.F. **What we study.** [1]

We study groups, rings, and fields. I think it is important to keep in mind that these notions are not handed down from on high; they grew organically.

A group is a set of invertible functions from a set to itself; this set is closed under composition. The set of all permutations of a finite set is the prototype of a group. Lagrange (1770) was one of the first to think about the set of permutations. Galois (1830) used groups of permutations as a way of describing which polynomials (in one variable with rational coefficients) can be "solved by radical". Felix Klein (1870) thought about "symmetry groups" of geometric objects. Groups were used by Gauss (1777-1855), Kronecker (1823-1891), and Kummer (1810-1893) in projects involving number theory. I visualize that Lagrange proved results about permutations, Klein proved results about symmetries of geometric objects, and Galois, Gauss, Kronecker, and Kummer proved results about number theory; before Cayley (1854) said "Hey! All of you proved the same result and it does not have anything to do with permutations, geometric objects, or number theory. It holds whenever one has … " At this point Cayley gave the abstract axioms for a group.

I think the idea of algebra is "Lets focus on the essential underlying idea rather than the specific example that we seem to be studying."

Commutative ring theory has a similar history. The main focus of number theory in the nineteenth history was to obtain a proof of Fermat's Last Theorem (that there do not exist positive integers a, b and c with $a^n + b^n = c^n$ when n is an integer at least three.) Fermat (1607-1665) wrote "I have discovered a truly remarkable proof of this theorem which this margin is too small to contain" in his copy of Arithmetica of Diophantus. One style of argument was to factor $x^n + y^n - z^n$ over $\mathbb{Z}$ with all of the n^{th} roots of one adjoined. This style of argument works when n is a prime integer and the "coefficient ring" is a "Unique Factorization Domain" (UFD). Alas, when $n = 23$, the coefficient ring is not a UFD. (Andrew Wiles proved Fermat's Last Theorem in 1995.)

[1] This material is mainly taken from [7, 9, 10].

In the meantime algebraic geometers were thinking about curves, surfaces, three-folds, etc. One way to study a geometric object X is to consider all of the (appropriate) functions from X back to the base field (say $\mathbb{R}$). Algebraic geometers especially care about polynomial maps. Differential Geometers and Functional Analysts probably want continuous maps. In all of these cases, the set of functionals (the set of maps from the geometric object to the base field) automatically form a ring. If f and g are functions from X to $\mathbb{R}$, then define $f + g : X \to \mathbb{R}$ to be the map that sends $x \in X$ to $f(x) + g(x)$ and define $f \times g$ from X to $\mathbb{R}$ to be $(f \times g)(x) = f(x) \cdot g(x)$. Algebraic Geometers call the set of functionals on X the coordinate ring of X; Functional Analysts call the set of functionals on X the dual Banach space of X.

Dedekind (or maybe Kronecker) observed you number theorists and you algebraic geometers are really proving the same theorems and the results are not really about number theory or curves, surfaces, and three-folds, they are really results about ... and at this point he defined an abstract ring.

The fact that fields were studied long before the official definition of field was given is quite clear. As humanity wanted to measure more quantities, do calculus, and solve more equations, humanity understood the (field of) rational numbers, the (field of) constructible numbers, the (field of) real numbers and (the field) of complex numbers. The official definition of an abstract field is probably due to Weber (1893) although Dedekind (1871) had an algebraic version and Kronecker (1881) had a more analytic version.

1.G. **Actions.** Groups act on sets. (In fact, so far I have only said that a group is a set of invertible functions from a set to itself.) One learns about the set by way of this group action and learns about the group by way of this group action. It is quite amazing.

Rings act on modules. A module is an Abelian group with a scalar multiplication. If $\boldsymbol{R}$ is the ring then the direct sum of copies of $\boldsymbol{R}$ (for example $\boldsymbol{R} \oplus \boldsymbol{R}$) is an $\boldsymbol{R}$-module and any subset of an $\boldsymbol{R}$-module which is closed under addition and scalar multiplication is another $\boldsymbol{R}$-module.

A field is a special kind of ring. So, every field also acts on modules. It turns out that every module over a field $\boldsymbol{k}$ is a direct sum of copies of $\boldsymbol{k}$. Modules over a field are called vector spaces.

1.H. **Some of the highlights of the course.**

1. Groups
   (a) We prove the Sylow Theorems about finite groups. Given a finite group we predict the sizes of some of its subgroups and we give information about how many such subgroups exist. These results are established by cleverly examining actions of the finite group.
   (b) We study "solvable groups" and we prove that the group of all permutations of a five element set is not solvable. (We pick this idea up again in 1.1.(3d).)
2. Rings
   (a) We study Principal Ideal Domains (PID). The ring of integers and the ring of polynomials over a field are examples of PIDs.
   (b) We prove that every PID is a Unique Factorization Domain. (Keep in mind that the notion of unique factorization is central to both Number Theory and Algebraic Geometry.)

(c) We find the structure of all finitely generated modules over a PID. (Keep in mind that a finitely generated module over a field is just a finite dimensional vector space. One can write down a basis for such a thing. It is easy. A finitely generated module over an arbitrary ring might be very complicated. But there is structure theorem for a finitely generated module over a PID. This is an awesome theorem.) Here are two applications of this theorem.
   (i) We record the structure of all finitely generated Abelian groups.
   (ii) We record the canonical forms for matrices. Let $\boldsymbol{k}$ be the field of complex numbers, V be an n-dimensional vector space over $\boldsymbol{k}$, and $T : V \to V$ be a linear transformation. One would like a basis for V that makes T as pretty as possible. Maybe T is diagonalizable; that would be pretty. In general, the Jordan canonical form of T looks like
$$\begin{bmatrix} J_{a_1}(\lambda_1) & 0 & 0 & \dots & 0 \\ 0 & J_{a_2}(\lambda_2) & 0 & \dots & 0 \\ 0 & 0 & J_{a_3}(\lambda_3) & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \dots & J_{a_s}(\lambda_s) \end{bmatrix},$$
where $J_a(\lambda)$ is the $a \times a$ matrix
$$J_a(\lambda) = \begin{bmatrix} \lambda & 0 & \dots & \dots & 0 \\ 1 & \lambda & 0 & \ddots & \vdots \\ 0 & 1 & \lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 & \lambda \end{bmatrix}.$$
The Jordan canonical form of T is unique (up to rearranging order of the Jordan blocks $J_{a_i}(\lambda_i)$. At any rate, T is diagonalizable if and only if each a_i is 1. (I have come upon elementary linear algebra books that say a square matrix over $\mathbb{C}$ is "defective" if it isn't diagonalizable. I scratch my head and think, "The matrix isn't defective; it merely has a more complicated Jordan canonical form than simply being diagonalizable.) I emphasize that there is nothing numerical about the theory of canonical forms of matrices. One is merely describing the structure of modules over Principal Ideal Domains; in other words, this result is exactly the same as the result which gives the structure of finitely generated Abelian groups. I have to point out how the data $(\boldsymbol{k}, V, T)$ involves a module over a PID. One says V is a module over the polynomial ring $\boldsymbol{k}[x]$, where the scalar multiplication xv is given by $xv = T(v)$ for all $v \in V$.

3. Galois Theory.

1.1. Let $f(x)$ be a polynomial with rational coefficients and let F be the smallest subfield of $\mathbb{C}$ which contains $\mathbb{Q}$ and the roots of f. We associate a group G to the pair of fields $\mathbb{Q} \subseteq F$. We prove the following statements.

(a) The group G is finite and the number of elements in G is equal to the dimension of F as a vector space over $\mathbb{Q}$.

(b) There is a one-to-one correspondence between the subgroups of G and the intermediate fields K with $\mathbb{Q} \subseteq K \subseteq F$. (The Sylow theorems give us information about the subgroups of a group!)
(c) The polynomial f is **solvable by radical** if and only if G is solvable.
(d) There are fifth degree polynomials which are not solvable by radical. In other words, **it is not possible to give a formula for the solutions of a fifth degree polynomial equation in terms of a finite iteration of taking roots and doing addition, subtraction, multiplication, and division.** Of course, the quadratic formula gives the solutions of a quadratic polynomial equation. The course will include the formulas for finding the solutions of third and fourth degree polynomial equations.

1.I. **Some of the reasons that I really like Algebra.**

(a) In algebra, one states up front what the rules are.
(b) Algebra is not confined to studying something that "is already there". That is, one can change the rules. For example, one can decree, "Today, two is equal to zero." Henceforth, now one has $(x+y)^2 = x^2 + y^2$.
(c) In algebra, the words are well-defined.
(d) Algebra provides tools for proving statements and making calculations. Here are some examples.
    (i) One often calculates the multiplicity of an intersection by calculating the length of a local ring.
    (ii) One often proves that two topological spaces are not homeomorphic by showing that some algebraic invariant of the spaces are different.
    (iii) Algebra provides interesting things for combinatorists to count; and algebra provides new techniques for counting things.

2. GROUPS.

2.A. **The definition and elementary properties of groups.**

Definition 2.1. A group is a set G together with a function $G \times G \to G$, given by $(g_1, g_2) \mapsto g_1 * g_2$, for $g_i \in G$, which satisfies the following properties.

(a) If g_1, g_2, and g_3 are elements of G, then $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$.
(b) There is an element e in G with $e * g = g$ and $g * e = g$ for all g in G.
(c) For each g in G, there exists an element g' with $g * g' = e$ and $g' * g = e$.

If G also satisfies $g_1 * g_2 = g_2 * g_1$ for all g_i in G, then G is called an Abelian group.

Remarks 2.2. (a) The function $*$ of is usually called an "operation" on G.
(b) One emphasizes that $g_1 * g_2$ is in G for all pairs of elements of G by saying that "G is closed under the operation $*$".
(c) Property (a) is called the associative property of the group $(G, *)$.
(d) The element e of (b) is called an "identity" element of the group $(G, *)$.
(e) The element g' of (c) is called an "inverse" of g.
(f) If $(G, *)$ is a group and H is a non-empty subset of G which is closed under $*$ and closed under the process of taking inverses, then $(H, *)$ is also a group and $(H, *)$ is called a subgroup of G.

Observation 2.3. *Let $(G, *)$ be a group. Then the following statements hold.*

(a) *The identity element of G is unique.*
(b) *If g is an element of G, then the inverse of g is unique.*
(c) *If g is an element of G and g' is the inverse of g, then g is the inverse of g'.*

Proof.
(a) If e and e_0 both are identity elements of G, then

$$e_0 = e * e_0 = e.$$

The equality on the left holds because e is an identity element of G. The equality on the right holds because e_0 is an identity element of G.
(b) If h and h_0 both are inverses of the element g of G, then

$$\begin{aligned}
h_0 &= e * h_0, && \text{because } e \text{ is the identity element of } (G, *),\\
&= (h * g) * h_0, && \text{because } h \text{ is an inverse of } g,\\
&= h * (g * h_0), && \text{because } * \text{ is an associative operation on } G,\\
&= h * e, && \text{because } h_0 \text{ is an inverse of } g,\\
&= h, && \text{because } e \text{ is the identity element of } (G, *).
\end{aligned}$$

(c) The hypothesis that g' is the inverse of g guarantees that $g' * g = e$ and $g * g' = e$. These two equations also demonstrate that g acts like an inverse of g'. Apply (b) to see that the inverse of g' in G is unique. It follows that g is the inverse of g'. $\square$

2.B. **Examples of groups.**

Example 2.4. The set of integers under addition is an Abelian group, denoted $(\mathbb{Z}, +)$.

Example 2.5. The set of non-zero complex numbers under multiplication is an Abelian group, denoted $\mathbb{C}^* = (\mathbb{C} \setminus \{0\}, \times)$.

Example 2.6. The set of invertible $n \times n$ matrices with complex entries under multiplication is a non-Abelian group, denoted $\mathrm{GL}_n(\mathbb{C})$. (The symbol GL stands for General Linear.)

Example 2.7. The set of $n \times n$ matrices with complex entries and determinant one is a non-Abelian group, denoted $\mathrm{SL}_n(\mathbb{C})$. (The symbol SL stands for Special Linear.)

Example 2.8. The set of permutations of the set $\{1, 2, 3, \dots, n\}$ under composition forms a group, denoted S_n.

We study S_3 in more detail. First we will list the elements of S_3 using two-rowed notation. Then we will list the elements of S_3 using one-rowed notation. (It is perfectly obvious what the two-rowed notation means; but it takes much too much effort to write an element down. One must think about what one-rowed notation means; but it clearly is more convenient to use.)

The notation
$$\begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$
means that $1 \mapsto a$, $2 \mapsto b$, and $3 \mapsto c$. The elements of S_3 are
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$
Instead of two-rowed notation we use cycle notation (or one-rowed) notation:
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3),$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3), \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3).$$
The cycle $(1,2,3)$ represents
$$\begin{tikzcd} 1 \arrow[rr] & & 2 \arrow[dl] \\ & 3 \arrow[ul] & \end{tikzcd}$$

Compose permutations the same way you always compose functions; in other words,
$$(f \circ g)(x) = f(g(x)).$$
In particular,
$$(1,2) \quad \underbrace{(1,3)}_{\text{Apply this function first}} \quad = (1,3,2)$$
If it is necessary, think in the two-rowed language
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

In a similar manner

$$(1,3)(1,2) = (1,2,3).$$

We are about to record the multiplication table for S_3. Take $\sigma = (1,2)$ and $\rho = (1,2,3)$. We should verify that all six permutations of $\{1,2,3\}$ can be expressed in the form $\sigma^i\rho^j$ with $0 \le i \le 1$ and $0 \le j \le 2$. Also, record the multiplication table for S_3.

Exercise. Here is a small problem. Let $\sigma = (1,2)$ and $\rho = (1,2,3)$.

(i) Show that

$$S_3 = \{\sigma^i\rho^j \mid \mid 0 \le i \le 1 \text{ and } 0 \le j \le 2\}$$

(ii) Fill in the multiplication table

	id	ρ	ρ^2	σ	$\sigma\rho$	$\sigma\rho^2$
id						
ρ						
ρ^2						
σ						
$\sigma\rho$						
$\sigma\rho^2$						

Answers. Here are my answers:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = (1) = \sigma^0, \quad \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1,3,2) = \rho^2, \quad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1,2,3) = \rho,$$

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1,2) = \sigma, \quad \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (1,3) = \sigma\rho, \quad \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (2,3) = \sigma\rho^2.$$

	id	ρ	ρ^2	σ	$\sigma\rho$	$\sigma\rho^2$
id	id	ρ	ρ^2	σ	$\sigma\rho$	$\sigma\rho^2$
ρ	ρ	ρ^2	id	$\sigma\rho^2$	σ	$\sigma\rho$
ρ^2	ρ^2	id	ρ	$\sigma\rho$	$\sigma\rho^2$	σ
σ	σ	$\sigma\rho$	$\sigma\rho^2$	id	ρ	ρ^2
$\sigma\rho$	$\sigma\rho$	$\sigma\rho^2$	σ	ρ^2	id	ρ
$\sigma\rho^2$	$\sigma\rho^2$	σ	$\sigma\rho$	ρ	ρ^2	id

Example 2.9. Let G be the set of rotations of the xy-plane which fix the origin. It is easy to see that G is an Abelian group.

Example 2.10. Let $\mathcal{G}$ be

$$\begin{aligned}&\{\text{rotations of the } xy\text{-plane which fix the origin}\}\\ \cup\ &\{\text{reflections of the } xy\text{-plane across a line through the origin}\}.\end{aligned}$$

In Homework problem 1, you will show that G is a group. I propose that you use the following technique. Let $\begin{bmatrix}x\\y\end{bmatrix}$ represent the vector which joins origin to the point (x,y) in the xy-plane. Let

$f : \mathbb{R}^2 \to \mathbb{R}^2$ be the function which fixes the origin and rotates each vector in $\mathbb{R}^2$ by the angle θ. Find the matrix M with the property that

$$f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = M \begin{bmatrix} x \\ y \end{bmatrix}.$$

Let ℓ be the line through the origin which passes through the origin and makes the angle θ_1 with the positive x-axis and let $f_1 : \mathbb{R}^2 \to \mathbb{R}^2$ be the function which reflects each vector $\begin{bmatrix} x \\ y \end{bmatrix}$ across ℓ. Find the matrix M_1 with the property that

$$f_1\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = M_1 \begin{bmatrix} x \\ y \end{bmatrix}.$$

As you examine the matrices, it will become obvious that G is closed under composition; and hence is a group. (It turns out that the matrices that arise in Example 2.9 form the group which is called the Special Orthogonal group $\mathrm{SO}_2(\mathbb{R})$ and the matrices that arise in Example 2.10 form the group which is called the Orthogonal group $\mathrm{O}_2(\mathbb{R})$. (The matrix M of $\mathrm{GL}_n(\mathbb{R})$ is in $\mathrm{O}_n(\mathbb{R})$ if $M^{-1} = M^{\mathrm{T}}$. The matrix M of $\mathrm{O}_n(\mathbb{R})$ is in $\mathrm{SO}_n(\mathbb{R})$ if $\det M = 1$.) [2]

Definition. Let n be an integer with $3 \le n$. For each non-negative j, let v_j be the point $(\cos \frac{2\pi j}{n}, \sin \frac{2\pi j}{n})$ in the xy-plane. The standard regular n-gon is the polygon with vertices $\{v_j \mid 0 \le j \le n-1\}$ and edges

$$\{\text{the line segment which join } v_j \text{ to } v_{j+1} \mid 0 \le j \le n-1\}.$$

Example 2.11. Let $\mathcal{G}$ be the group of Example 2.10. Fix an integer n with $3 \le n$. Let D_n be the subgroup of $\mathcal{G}$ which carries the regular n-gon onto itself. (The group D_n is called the n^{th} Dihedral group.) The regular n-gon has n sides of equal length, center at $(0,0)$, and one vertex at $(1,0)$.

Example. In particular, the regular 3-gon has vertices $(1,0)$, $(-1/2, \sqrt{3}/2)$, and $(-1/2, -\sqrt{3}/2)$. Label these vertices 1, 2, 3. The elements of D_3 are the identity (this is the permutation (1) of the vertices), rotation by $2\pi/3$ radians (this is the permutation $(1,2,3)$ of the vertices), rotation by $4\pi/3$ radians (this is the permutation $(1,3,2)$ of the vertices), reflection across the x-axis (this is the permutation $(2,3)$ of the vertices), reflection across the line through the origin and vertex 2 (this is the permutation $(1,3)$ of the vertices), and reflection across the line through the origin and vertex 3 (this is the permutation $(1,2)$ of the vertices). Observe that D_3 is equal to S_3.

Theorem 2.11.1. *Let ρ be rotation by $\frac{2\pi}{n}$ and σ be reflection across the x-axis. Then every element of D_n can be written uniquely in the form*

$$\sigma^i \rho^j \textit{ with } 0 \le i \le 1 \textit{ and } 0 \le j \le n-1.$$

In particular, D_n has $2n$ elements.

Proof.
Part one. We show that every element of D_n can be written in the given form.

[2] In general we will write M^{T} for the transpose of the matrix M. If $m_{i,j}$ is in row i, column j of M, then $m_{i,j}$ is in row j, column i of M^{T}.

It is clear that the only rotations from $\mathscr{G}$ that carry the n-gon to it self are ρ^j for $0 \le j \le n-1$.

Suppose τ is a reflection from $\mathscr{G}$ and τ carries the n-gon to itself. You will show in Homework 1, that $\sigma\tau$ is a rotation. Thus, $\sigma\tau = \rho^j$ for some j. Multiply both sides of the equation on the left by σ to see that $\tau = \sigma\rho^j$.

Part two. We show uniqueness.

Suppose $\sigma^{i'}\rho^{j'} = \sigma^i\rho^j$ with $j' \le j$. Then

$$\underbrace{\sigma^{0 \text{ or } 1}}_{\text{We fix vertex 1}} = \rho^{j-j'}.$$

If $j - j'$ is positive, then the right side moves every vertex. Thus, $j - j' = 0$ and hence $i = i'$. $\square$

Example. The group D_4 consists of the identity map, three rotations, and reflection across the x-axis, $\underbrace{y = x}_{\ell_1}$, the $\underbrace{y\text{-axis}}_{\ell_2}$, and $\underbrace{y = -x}_{\ell_3}$. DRAW A PICTURE. In Homework 2, among other things, you will write the reflections across ℓ_1, ℓ_2, and ℓ_3 in the form of Theorem 2.11.1.

Example 2.12. Return to the group $\mathbb{C}^* = (\mathbb{C} \setminus \{0\}, \times)$ of Example 2.5.

Facts-Definitions

(a) If $z = x + \mathbb{i}y$ with $x, y \in \mathbb{R}$, then $z = r(\cos\theta + \mathbb{i}\sin\theta)$ with r and θ in $\mathbb{R}$. DRAW A PICTURE.
(b) If z is the complex number of (a), then $|z| = \sqrt{x^2 + y^2} = |r|$.
(c) If r_1, r_2, θ_1, and θ_2 are real numbers, then

$$r_1(\cos\theta_1 + \mathbb{i}\sin\theta_1) \cdot r_2(\cos\theta_2 + \mathbb{i}\sin\theta_2) = r_1r_2(\cos(\theta_1+\theta_2) + \mathbb{i}\sin(\theta_1+\theta_2)).$$

(d) If $\theta \in \mathbb{R}$, then $\cos\theta + \mathbb{i}\sin\theta = e^{\mathbb{i}\theta}$.

My favorite way to think of these "facts" is through Taylor's series from calculus. Recall, from calculus, that the following equations hold for all real numbers x:

$$\begin{aligned} e^x &= \sum_{n=0}^{\infty} \frac{x^n}{n!}, \\ \sin x &= \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}, \quad \text{and} \\ \cos x &= \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}. \end{aligned}$$

The Taylor series for the exponential function continues to hold if x is replaced by a complex number. Thus, if θ is a real number then

$$\begin{aligned} e^{\mathbb{i}\theta} &= 1 + (\mathbb{i}\theta) + \frac{(\mathbb{i}\theta)^2}{2!} + \frac{(\mathbb{i}\theta)^3}{3!} + \frac{(\mathbb{i}\theta)^4}{4!} + \dots \\ &= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} + \dots\right) + i\left(\theta - \frac{\theta^3}{3!} + \dots\right) \\ &= \cos\theta + \mathbb{i}\sin\theta. \end{aligned}$$

This "explains" (d).

If $z = r(\cos\theta + \mathbb{i}\sin\theta)$ and one believes (d), then (a) yields that $z = re^{\mathbb{i}\theta}$.

If $z = re^{\mathbb{i}\theta}$, then (b) yields $|z| = |r|$ and $|e^{\mathbb{i}\theta}| = 1$. (The non-negative real number $|z|$ is called the modulus of z. If $z = a + b\mathbb{i}$ with a and b real, then $|z| = \sqrt{a^2 + b^2} = \sqrt{\bar{z}z}$, where $\bar{z} = a - b\mathbb{i}$, is the complex conjugate of z.)

If $z_j = r_j e^{\mathbb{i}\theta_j}$, then (c) becomes

$$r_1 e^{\mathbb{i}\theta_1} \cdot r_2 e^{\mathbb{i}\theta_2} = r_1 r_2 e^{\mathbb{i}(\theta_1+\theta_2)}$$

Example 2.12.1. Let U be the subgroup of $\mathbb{C}^*$ consisting of all elements of modulus 1. Then U is a group.

Example 2.12.2. Some finite subgroups of $\mathbb{C}^*$ are $\{1\}$, $\{1, -1\}$, $\{1, \mathbb{i}, -1, -\mathbb{i}\}$. Homework problem 3 asks you to find all finite subgroups of $\mathbb{C}^*$.

Example 2.13. Let I be an index set. Suppose that for each $i \in I$, G_i is a group. The direct product of $\{G_i \mid i \in I\}$ is the group

$$\prod_{i\in I}(G_i, *_i) = \{(g_i)_{i\in I} | g_i \in I\}.$$

The operation in the direct product is given component-wise. That is, the i-tuple $(g_i)_{i\in I}$ times the i-tuple $(g_i')_{i\in I}$ is equal to the i-tuple

$$(g_i *_i g_i')_{i\in I}.$$

The direct sum of the G_i is the group

$$\bigoplus_{i\in I} G_i = \{(g_i)_{i\in I} | g_i \in I \text{ and at most finitely many } g_i \text{ are not } 1\}.$$

The operation in the direct sum is also given component-wise. Of course, if $I = \{1, \dots, n\}$, then

$$G_1 \oplus G_2 \oplus \dots \oplus G_n = G_1 \times G_2 \times \cdots \times G_n.$$

Let C_2 be the group with two elements. In Homework problem 4, I have asked you to count the number of four element subgroups of $C_2 \times C_2 \times C_2 \times C_2$.

Direct product and direct sum satisfy the following universal mapping properties. (One could define direct sum and direct product by way of these UMPs.)

Observation. *Let I be an index set. Suppose that for each $i \in I$, G_i is a group.*

(a) *Let G be a group and, for each i, let $\phi_i : G \to G_i$ be a group homomorphism. Then there exists a unique group homomorphism $\Phi : G \to \prod_{i\in I} G_i$ so that the diagram*

$$\begin{tikzcd} G \arrow[r, dashed, "\exists!\Phi"] \arrow[dr, "\phi_{i_0}"'] & \prod_{i\in I} G_i \arrow[d, "\mathrm{proj}_{i_0}"] \\ & G_{i_0} \end{tikzcd}$$

commutes for all $i_0 \in I$.

(b) *Let G be an Abelian group and, for each i, let $\phi_i : G_i \to G$ be a group homomorphism. Then there exists a unique group homomorphism $\Phi : \bigoplus_{i\in I} G_i \to G$ so that the diagram*

$$\begin{tikzcd}
G & \bigoplus_{i\in I} G_i \arrow[l, dashed, "\exists!\Phi"'] \\
& G_{i_0} \arrow[ul, "\phi_{i_0}"] \arrow[u, "\mathrm{incl}_{i_0}"']
\end{tikzcd}$$

commutes for all $i_0 \in I$.

Note. You should write down complete proofs for these small facts.

Definition 2.14. If G and G' are groups then a function $\phi : G \to G'$ is a group homomorphism if

$$\phi(g_1g_2) = \phi(g_1)\phi(g_2),$$

for all g_1, g_2 in G. The operation on the left takes place in G. the operation on the right takes place in G'.

Elementary Properties. Let $\phi : G \to G'$ be a group homomorphism. The following statements hold.

- If e is the identity element of G, then $\phi(e)$ is the identity element of G'.
- The homomorphism ϕ carries the inverse of g to the inverse of $\phi(g)$ for all $g \in G$.

Note. You should write down complete proofs for these small facts.

Last time we said that if G and G' are groups, then a function $\phi : G \to G'$ is a group homomorphism if

$$\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$$

for all $g_1, g_2 \in G$.

A group homomorphism which is one-to-one and onto is called a group isomorphism.

Example 2.14.1. The function $\phi : (\mathbb{R}, +) \to (\{r \in \mathbb{R} \mid 0 < r\}, \times)$, given by $\phi(r) = e^r$ is a group isomorphism because

$$\phi(r_1 + r_2) = e^{r_1+r_2} = e^{r_1}e^{r_2} = \phi(r_1)\phi(r_2).$$

ϕ is surjective. Take s in the target. Observe that $\ln s$ is in the source and $\phi(\ln s) = e^{\ln s} = s$.

ϕ is injective. Suppose r_1 and r_2 are in the source with $\phi(r_1) = \phi(r_2)$. Then $e^{r_1} = e^{e_2}$. Apply ln to both sides to learn that $r_1 = r_2$.

Example 2.14.2. The function $\phi : (\mathbb{R}, +) \to U$, which is given by

$$\phi(\theta) = e^{i\theta}$$

is a surjective group homomorphism which is not injective.

Example 2.14.3. The function $\phi : U \to \mathrm{SO}_2(\mathbb{R})$, which is given by

$$\phi(e^{i\theta}) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},$$

is a group isomorphism. The most interesting part of this claim is making sure that "ϕ is well-defined". That is, one must show that if $e^{i\theta} = e^{i\theta'}$, then

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} \cos\theta' & -\sin\theta' \\ \sin\theta' & \cos\theta' \end{bmatrix}.$$

Example 2.15. Let G be the collection of rotations of $\mathbb{R}^3$ which fix a line through the origin.

Claim 2.15.1. *The set G forms a group.*

Notice that every element of G is given by matrix multiplication. Indeed, if f is rotation about the z-axis, then f is rotation of the xy-plane and you will show in Homework 1 that f is given by matrix multiplication. Observe that rotation about the line ℓ through the origin is the composition

(2.15.2) $\qquad$ (move the z-axis to ℓ)$\circ$(rotate about the z-axis)$\circ$(move ℓ to the z-axis)

Each of the three functions in (2.15.2) is given by matrix multiplication[3] and the composition is given by the product of the three matrices.

Claim 2.15.3. *Let $f : \mathbb{R}^3 \to \mathbb{R}^3$ be a function and M be a matrix in* $\mathrm{GL}_3(\mathbb{R})$ *with*

$$f\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right) = M\begin{bmatrix} x \\ y \\ z \end{bmatrix},$$

for all

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3.$$

Then

$$f \in G \iff M \in \mathrm{SO}_3(\mathbb{R}).$$

Observe that Claim 2.15.3 implies Claim 2.15.1. We prove Claim 2.15.3.

(Recall that a 3×3 matrix M with real entries is in $\mathrm{SO}_3(\mathbb{R})$ if and only if MM^{T} is the 3×3 identity matrix and $\det M = 1$.)

Proof. ($\Rightarrow$)[4] Let ℓ be a line through the origin in $\mathbb{R}^3$ and f be rotation which fixes ℓ. Let

(2.15.4) $\qquad$ v_1, v_2, v_3 be an orthonormal basis for $\mathbb{R}^3$ with v_3 on ℓ.

Recall the following statements.

(a) The vectors v_1, v_2, v_3 are an orthonormal basis for $\mathbb{R}^3$ if $v_i^{\mathrm{T}} v_j$ is equal to the Kronecker delta, for $1 \le i, j \le 3$.[5]

[3] When we "move ℓ to the z-axis" we want to do this in a systematic manner!

[4] In Homework problem 6 you will carry out this procedure for some explicit specific data.

[5] We use $(-)^{\mathrm{T}}$ to mean "transpose".

(b) One way to get vectors as described in (2.15.4) is to start with a unit vector v_3 on ℓ, extend v_3 to be a basis of $\mathbb{R}^3$, and then apply Gram-Schmidt orthogonalization.

We compute the matrix for f as described in (2.15.2). One good matrix for moving the z-axis to ℓ is

$$Q = \left[\ v_1 \mid v_2 \mid v_3\ \right].$$

The matrix Q sends the x-axis to the line containing v_1 and the origin. The matrix Q also sends the y-axis to the line containing v_2 and the origin. The inverse of Q sends ℓ to the z-axis. Of course, the columns of Q are an orthonormal set; so the inverse of Q is Q^{T}. According to Homework problem 1, the matrix for rotation around the z-axis has the form

$$N = \left[\begin{array}{c|c} M' & 0 \\ \hline 0 & 1 \end{array}\right],$$

for some M' in $\mathrm{SO}_2(\mathbb{R})$. Thus, the matrix for f is

$$M = QNQ^{\mathrm{T}}.$$

Observe that M is an orthogonal matrix because

$$M^{\mathrm{T}} = (Q^{\mathrm{T}})^{\mathrm{T}} N^{\mathrm{T}} Q^{\mathrm{T}} = QNQ^{\mathrm{T}} = M.$$

Furthermore, $\det N = 1$ and $\det Q = \det Q^{\mathrm{T}}$ with $\det Q \det Q^{\mathrm{T}} = \det I = 1$. Thus, $\det Q = \det Q^{\mathrm{T}} = \pm 1$ and $\det M = 1$. We have proven that $M \in \mathrm{SO}_3(\mathbb{R})$.

($\Leftarrow$) Let M be an element of $\mathrm{SO}_3(\mathbb{R})$. We will show that there exists a line ℓ through the origin and an angle θ so that Mv is the vector that is obtained by rotating v about ℓ by the angle θ, for all v in $\mathbb{R}^3$.

Theorem. *Let G be the following set of functions together with the operation composition:*

$$G = \{f : \mathbb{R}^3 \to \mathbb{R}^3 \mid f \textit{ is a rotation of } \mathbb{R}^3 \textit{ which fixes a line through the origin}\}.$$

Then

(1) *Each element of G is given by matrix multiplication.*
(2) *The set $(G, \circ)$ is a group.*
(3) *The groups $(G, \circ)$ and $\mathrm{SO}_3(\mathbb{R})$ are isomorphic.*

The proposed isomorphism is

$$\mathrm{SO}_3(\mathbb{R}) \to G$$

is the function which sends $M \in \mathrm{SO}_3(\mathbb{R})$ to the function $\mathrm{mult}_M : \mathbb{R}^3 \to \mathbb{R}^3$, where

$$\mathrm{mult}_M(v) = Mv,$$

for $v \in \mathbb{R}^3$. (The vector space $\mathbb{R}^3$ is the Abelian group of column vectors with three real entries.)

Last time we established (1) and we showed that if $f \in G$ is multiplication by M, then M is an element of $\mathrm{SO}_3(\mathbb{R})$.

Today we show that if $M \in \mathrm{SO}_3(\mathbb{R})$, then the function $\mathbb{R}^3 \to \mathbb{R}^3$ which is given $v \mapsto Mv$ is rotation by some angle about a line through the origin.

In particular, we must show that if M is in $\mathrm{SO}_3(\mathbb{R})$, then M fixes some non-zero vector v and M carries the plane perpendicular to v to itself.

In Homework problem 5, you will prove that M is diagonalizable over $\mathbb{C}$. In other words, you will prove that there are complex numbers λ_1, λ_2 and λ_3 and linearly independent vectors v_1, v_2, and v_3 in $\mathbb{C}^3$ such that $Mv_i = \lambda_i v_i$, for $1 \le i \le 3$. Observe that

(a) If λ is an eigenvalue of M, then $\bar{\lambda}$ is an eigenvalue of M.
(b) $\prod \lambda_i = 1$
(c) $|\lambda_i| = 1$ for $1 \le i \le 3$.
(d) the product $(1 - \bar{\lambda}_i\lambda_j)\bar{v}_i^{\mathrm{T}}v_j$ is zero for all i and j.

For (a), notice that if $Mv = \lambda v$, then $\bar{M}\bar{v} = \bar{\lambda}\bar{v}$; but M has real entries, so $\bar{M} = M$ and therefore, $M\bar{v} = \bar{\lambda}\bar{v}$. Conclude that $\bar{\lambda}$ is an eigenvalue of M.

For (b), the matrix M is similar to the diagonal matrix with the eigenvalues on the main diagonal. Similar matrices have the same determinant. The determinant of M is 1. It follows that $\prod \lambda_i = 1$.

For (c), observe that if $Mv = \lambda v$, with $v \neq 0$, then

$$\bar{v}^{\mathrm{T}}v = \bar{v}^{\mathrm{T}}\bar{M}^{\mathrm{T}}Mv = (\overline{Mv})^{\mathrm{T}}Mv = (\overline{\lambda v})^{\mathrm{T}}\lambda v = \bar{\lambda}\lambda\bar{v}^{\mathrm{T}}v.$$

The complex number $\bar{v}^{\mathrm{T}}v$ is not zero; hence the complex number $\bar{\lambda}\lambda$ must be 1. In other words, the modulus of λ must be 1.[6]

For (d)[7], observe that

$$\bar{v}_i^{\mathrm{T}}v_j = \bar{v}_i^{\mathrm{T}}\bar{M}^{\mathrm{T}}Mv_j = (\overline{Mv_i})^{\mathrm{T}}Mv_j = (\overline{\lambda_i v_i})^{\mathrm{T}}\lambda_j v_j = \bar{\lambda}_i\lambda_j\bar{v}_i^{\mathrm{T}}v_j.$$

It follows immediately from (a)–(c) that at least one of the eigenvalues of M is real; hence the eigenvalues of M are:

$$1, 1, 1 \quad \text{or} \quad 1, -1, -1 \quad \text{or} \quad 1, a + b\mathfrak{i}, a - b\mathfrak{i}$$

with b not zero and $\sqrt{a^2 + b^2} = 1$.

If the eigenvalues of M are $1, 1, 1$, then M is the identity matrix which is rotation fixing the z-axis by angle zero.

If the eigenvalues of M are $1, -1, -1$, (and M is diagonalizable) then there are linearly independent vectors $v_1, v_2, v_3 \in \mathbb{R}^3$ with $Mv_i = \lambda_i v_i$ with $\lambda_1 = 1$, $\lambda_2 = \lambda_3 = -1$.[8] Apply (d) to see that v_1 is perpendicular to both v_2 and v_3. Observe that M is the matrix for rotation by π about the line containing v_1.

Now we focus on the case where the eigenvalues of M are 1, $a + b\mathfrak{i}$, and $a - b\mathfrak{i}$ with a and b in $\mathbb{R}$ with $a^2 + b^2 = 1$ and b not zero. Let $u_1 + \mathfrak{i}u_2$ be a non-zero eigenvector of M associated to 1, $w_1 + \mathfrak{i}w_2$ be a non-zero eigenvector of M associated to $a + b\mathfrak{i}$, and $w_3 + \mathfrak{i}w_4$ be a non-zero eigenvector of M associated to $a - b\mathfrak{i}$ with $u_1, u_2, w_1, w_2, w_3, w_4 \in \mathbb{R}^3$. It is clear that u_1 and u_2

[6] If $\lambda = a + b\mathfrak{i}$ is a complex number with a and b real, then $\sqrt{a^2 + b^2}$ is called the modulus of λ and is denoted $|\lambda|$.

[7] Of course, one can prove (c) and (d) simultaneously.

[8] The fact that there exist linearly independent $v_1, v_2, v_3 \in \mathbb{R}^3$ with $Mv_i = \lambda_i v_i$ requires a small amount of argument. At first, we are guaranteed linearly independent w_1, w_2, w_3 in $\mathbb{C}^3$ with $M_i w_i = \lambda_i w_i$ for $\lambda_1 = 1$ and $\lambda_2 = \lambda_3 = -1$. But $w_i = a_i + \mathfrak{i}b_i$ with $a_i, b_i \in \mathbb{R}^3$. The vectors a_i and b_i are necessarily eigenvectors of M associated to λ_i. It is possible to pick v_1 from the set $\{a_1, b_1\}$ and v_2, v_3 from the set $\{a_2, b_2, a_3, b_3\}$.

each are eigenvectors of M belonging to 1. At least one of the vectors u_1 and u_2 is non-zero; we have identified a non-zero vector $v_1 \in \mathbb{R}^3$ with $Mv_1 = v_1$. (We may as well insist that v_1 is a unit vector.) According to (d), the vectors w_1, w_2, w_3, and w_4 of $\mathbb{R}^3$ all are in the plane perpendicular to v_1. The vectors $w_1 + iw_2$ and $w_3 + iw_4$ span a two dimensional subspace of of $\mathbb{C}_2$; so the vectors w_1, w_2, w_3, and w_4 of $\mathbb{R}^3$ can not lie on a line; they must span the plane in $\mathbb{R}^3$ perpendicular to v_1. Pick an orthogonal set v_1, v_2, v_3. Noticed that the vector spaces (w_1, w_2, w_3, w_4) and (v_2, v_3) are equal. The hypothesis that $w_1 + iw_2$ and $w_3 + iw_4$ are eigenvectors of M ensure that Mv_2 and Mv_3 are both in (v_2, v_3). The matrix for M with respect to the basis v_1, v_2, v_3 has the form

$$\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & M' \end{array}\right].$$

The matrix M is in $\mathrm{SO}_3(\mathbb{R})$; hence, the matrix M' is in $\mathrm{SO}_2(\mathbb{R})$. You proved in Homework 1, that the matrices of $\mathrm{SO}_2(\boldsymbol{R})$ are rotation matrices. Thus, multiplication by M fixes the line containing v_1 and rotates the plane perpendicular to v_1. $\square$

2.C. **Cayley's Theorem.** What you should take away from HW2:

- problem 3: For each positive integer n, there is exactly one subgroup of $\mathbb{C}^*$ of order n, namely $U_n = \{e^{\frac{2\pi i j}{n}} \mid 0 \leq j \leq n-1\}$. This is the group of n^{th} roots of 1 in $\mathbb{C}$.
- problem 4: Each element in a direct sum is interesting. (If G_1 and G_2 are groups, then the element (g_1, g_2) is just interesting as the elements (g_1, id_{G_2}) and (id_{G_1}, g_2), where $g_i \in G_i$ and id_{G_i} is the identity element of G_i.)

  If you recognized that "each element in a direct sum is interesting", but did not count well, then work on your counting skills. (One way to do this is to teach Math 574 or 374 ...).
- problem 5: Wow. There is so much to learn from problem 5.
  - The $n \times n$ matrix M with entries in the field F is diagonalizable if and only if F^n has a basis of eigenvectors. (I did not know that you wouldn't know this. In fact, I introduced the expression "diagonalizable" by accident. I wanted you to prove that if $M \in SO_3(\mathbb{R})$, then $\mathbb{R}^3$ has a basis of eigenvectors. I swapped the desired condition for an equivalent but irrelevant condition without realizing that I had done it.) Nonetheless, many folks taught themselves this result and wrote down a proof. Excellent!
  - It is good to understand the assertion that if V is subspace of F^n, F is an algebraically closed field, M is an $n \times n$ matrix with entries in F, and $Mv \in V$ for all $v \in V$, then M has an eigenvector in V.
  - It is worth your while to know the concept "diagonalizable" because our unit on canonical forms of matrices answers the question "Well, if a square matrix is not diagonalizable, why isn't it and what is it."
  - By the way nilpotent matrices are not diagonalizable:

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

    and the sum of a diagonal matrix and a nilpotent matrix is not diagonalizable

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

  - Let M be an $n \times n$ matrix over the field F. It is very much the philosophy of our course to consider subspaces V of F^n with $Mv \in V$ for all $v \in V$. (This makes V an $F[M]$-module or an $F[x]$-module where xv is defined to be Mv.) If v is an eigenvector of M then Fv is a one-dimensional vector space which is an $F[M]$-module.
  - Orthogonal matrices over $\mathbb{R}$ preserve length and angle. (I had not stated this explicitly; indeed, I had not thought it explicitly; but I was asked about it after class the other day and it is such a good question, that I want to share it with every body). If M is an $n \times n$ matrix with real entries and $MM^{\mathrm{T}} = I = M^{\mathrm{T}}M$, then $(Mv)^{\mathrm{T}}(Mv) = v^{\mathrm{T}}v$; so v and Mv have the same length for each $v \in \mathbb{R}^n$. Furthermore $(Mv)^{\mathrm{T}}Mw = v^{\mathrm{T}}w$ for all v and w in $\mathbb{R}^n$. So, the angle between v and w is the same as the angle between Mv and Mw. (Recall that the dot product of two vectors is the length of the first vector times the length of the second vector times the cosine of the angle between them.)
  - One proves the result of problem 5 by induction. My argument decomposes an $F[M]$-module as a direct sum of two smaller $F[M]$-modules. This argument is also very much in keeping with the philosophy of our course.
- Problem 6. If one has to make a dirty calculation, then make it all the way to the bitter end and then clean it up. Now one has a chance of making sure that one has the correct answer. This philosophy comes into play when I am teaching and when I am writing research papers.

My answer to number 5:

Theorem. *Every unitary matrix from* $\mathrm{GL}_n(\mathbb{C})$ *is diagonalizable.*

The proof is a consequence of the following Claim; just take V to be all of $\mathbb{C}^n$.

Claim. *Let M be a unitary $n \times n$ matrix with complex entries and let V be a subspace of $\mathbb{C}^n$ with the property that $MV \subseteq V$. Then the restriction of M to V is diagonalizable.*

Proof. Write $M|_V$ for the "restriction of M to V".

We prove the claim by induction on the dimension of V. If $\dim V = 1$, and v is a non-zero element of V, then v is a basis for V. The hypothesis that $MV \subseteq V$ guarantees that v is an eigenvalue of M and hence $M|_V$ is diagonalizable.

Now suppose that $1 < \dim V$. Recall that $M|_V$ has a non-zero eigenvector. [9]

Let v_0 be a non-zero eigenvector of $M|_V$ which belongs to the eigenvalue λ_0. (The matrix M is non-singular, so $\lambda_0 \neq 0$.) Let

$$W = \{w \in V \mid \bar{w}^{\mathrm{T}} v_0 = 0\}.$$

It is clear that W is a vector space. Observe that

- $V = \mathbb{C}v_0 \oplus W$, and

[9] Indeed, the characteristic polynomial of $M|_V$ is a polynomial in one variable with complex coefficients. Such a polynomial has a root, say λ_1 in $\mathbb{C}$ (by the "Fundamental Theorem of Algebra"). Thus $M|_V - \lambda_1$ id is a singular matrix. Any non-zero vector in the null space of $M|_V - \lambda_1$ id is an eigenvector of $M|_V$.

- $MW \subseteq W$.

Once we are confident with these assertions then the proof of the claim is complete by induction because $\dim W < \dim V$. We establish the two assertions.

We first show that $MW \subseteq W$. If $w \in W$, then $\bar{w}^{\mathrm{T}} v_0 = 0$ and

$$(\overline{Mw})^{\mathrm{T}} v_0 = \frac{1}{\lambda_0}(\overline{Mw})^{\mathrm{T}} M v_0 = \frac{1}{\lambda_0}\bar{w}^{\mathrm{T}}\overline{M}^{\mathrm{T}} M v_0 = \frac{1}{\lambda_0}\bar{w}^{\mathrm{T}} \operatorname{id} v_0 = \bar{w}^{\mathrm{T}} v_0 = 0;$$

hence, Mw is in W, as claimed.

Now we show that V is contained in the sum of W and $\mathbb{C}v_0$. If v is an arbitrary element of V, then

$$v = (v - \frac{\bar{v}^{\mathrm{T}} v_0}{\bar{v}_0^{\mathrm{T}} v_0} \cdot v_0) + \frac{\bar{v}^{\mathrm{T}} v_0}{\bar{v}_0^{\mathrm{T}} v_0} \cdot v_0$$

with $(v - \frac{\bar{v}^{\mathrm{T}} v_0}{\bar{v}_0^{\mathrm{T}} v_0} \cdot v_0) \in W$ and $\frac{\bar{v}^{\mathrm{T}} v_0}{\bar{v}_0^{\mathrm{T}} v_0} \cdot v_0 \in \mathbb{C}v_0$

Finally, the intersection of W and $\mathbb{C}v_0$ is zero because $\bar{v}_0^{\mathrm{T}} v_0$ is not zero. □

The Claim has been established. Thus, as was noted above the claim, the Theorem is also established.

We return to the regularly scheduled programming:

Theorem 2.16. (Cayley) *Every group is isomorphic to a group of permutations.*

Proof. Let G be a group. If $g \in G$, then let $g_L : G \to G$ be the function $g_L(g_1) = gg_1$ for all $g_1 \in G$. Notice that g_L is a permutation of G!

Let $G_L = \{g_L : G \to G \mid g \in G\}$.

Observe $(G_L, \circ)$ is a group.

- If $h, g \in G$, then $h_L \circ g_L = (hg)_L$. (So G_L is closed under $\circ$.)
- If e is the identity element of G, then e_L is the identity element of G_L.
- If $g \in G$, then $(g^{-1})_L = (g_L)^{-1}$.
- Function composition always associates.

Observe that $\phi : G \to G_L$, which is defined by $\phi(g) = g_L$ is a group isomorphism.

Indeed,

- we already saw that $\phi(hg) = \phi(h) \circ \phi(g)$,
- if g_L is an arbitrary element of G_L, for some $g \in G$, then $g_L = \phi(g)$,
- if $\phi(g) = \phi(h)$, then the functions g_L and h_L of G_L are equal. In particular, if e is the identity element of G, then

$$g = ge = g_L(e) = h_L(e) = he = h.$$

□

Corollary 2.17. *If G is a group of order*[10] *n, then G is isomorphic to a subgroup of S_n.*

Of course, there is more nothing to prove. The proof we gave also establishes the Corollary.

[10]The order of a group is the number of elements in the group.

Example 2.18. Lets use Cayley's Theorem to exhibit S_3 as a subgroup of S_6. Write S_3 as

$$a_1 = (1), \quad a_2 = (1,2), \quad a_3 = (1,3), \quad a_4 = (2,3), \quad a_5 = (1,2,3), \quad \text{and} \quad a_6 = (1,3,2).$$

Observe that

$$(a_2)_L : S_3 \to S_3$$

is

$$\begin{aligned} a_1 &\mapsto a_2 \\ a_2 &\mapsto a_1 \\ a_3 &\mapsto (1,2)(1,3) = (1,3,2) = a_6 \\ a_4 &\mapsto (1,2)(2,3) = (1,2,3) = a_5 \\ a_5 &\mapsto (1,2)(1,2,3) = (2,3) = a_4 \\ a_6 &\mapsto (1,2)(1,3,2) = (1,3) = a_3. \end{aligned}$$

So $(1,2)_L = (1,2)(3,6)(4,5)$. Similarly,

$$(a_5)_L : S_3 \to S_3$$

is

$$\begin{aligned} a_1 &\mapsto a_5 \\ a_2 &\mapsto (1,2,3)(1,2) = (1,3) = a_3 \\ a_3 &\mapsto (1,2,3)(1,3) = (2,3) = a_4 \\ a_4 &\mapsto (1,2,3)(2,3) = (1,2) = a_2 \\ a_5 &\mapsto (1,2,3)(1,2,3) = (1,3,2) = a_6 \\ a_6 &\mapsto (1,2,3)(1,3,2) = (1) = a_1. \end{aligned}$$

So $(1,2,3)_L = (1,5,6)(2,3,4)$.

In Homework 1, you saw that S_3 is generated by $(1,2)$ and $(1,2,3)$. Thus, the proof of Cayley's theorem shows that S_3 is isomorphic to the subgroup of S_6 which is generated by $(1,2)(3,6)(4,5)$ and $(1,5,6)(2,3,4)$.

Example 2.19. This is a more interesting example. Does there exist an 8-element group

$$\{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

which satisfies

$$a^4 = 1, \quad a^2 = b^2, \quad \text{and} \quad ba = a^3b?$$

Step 1. If there exists such a group; it could only have one multiplication table

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	1	a^3	a^2

We still do not know if this multiplication associates and we certainly do not know if all eight names are distinct. In Homework problem 7 in problem set three, I will ask you to apply the technique of the proof of Cayley's Theorem in order to identify an eight element subgroup of S_8 that has this multiplication table.

At home you obtained an eight element subgroup of S_8 with distinct elements of the form $a^i b^j$, with $0 \le i \le 3$ and $0 \le j \le 1$ whose elements satisfy $a^4 = 1$, $b^2 = a^2$, $ba = a^3 b$.

Remark. This problem is part of a larger problem; namely, find all groups of order 8. It turns out that (up to isomorphism) there are 5 groups of order 8: 3 Abelian groups, D_4, and this group. This group is called the Quaternion group Q_8. By the way, it is clear that D_4 and Q_8 are not isomorphic. Indeed, D_4 has 5 elements of order[11] 2 and 2 elements of order 4; whereas, Q_8 has 1 element of order 2 and 6 elements of order 4.

Actually, something much deeper is going on. It is reasonable to ask: suppose I have a group with a finite set of generators and and a finite set of relations. Is there an algorithm for determining if a given word is the identity element? This problem is called the "word problem". It was shown by Pyotr Novikov (1955) and William Boone (1958) that the word problem is undecidable. (Look at the Wikipedia page for the Word problem for groups.)

[11]The <u>order</u> of an element g in the group G is the number of elements in the subgroup of G which is generated by g. In particular, the order of g is the least positive integer n with g^n equal to the identity element, if such an integer n exists.

September 20, 2023

2.D. **Cyclic groups.**

Definition 2.20. The group G is a cyclic group if there exists an element g in G with

$$G = \{g^k \mid k \in \mathbb{Z}\}.$$

Examples 2.21. The group $(\mathbb{Z}, +)$ is cyclic of infinite order. The group $U_n = \{e^{\frac{2j\pi i}{n}} | j \in \mathbb{Z}\}$, which is equal to the group of n^{th} roots of 1 in $\mathbb{C}^*$, and the subgroup $\{(1, 2, \dots, n)^j | j \in \mathbb{Z}\}$ of S_n are cyclic groups of order n.

Observation 2.22. *Two cyclic groups are isomorphic if and only if they have the same order.*

Proof.
($\Rightarrow$) This direction is clear. An isomorphism is always a bijection.

($\Leftarrow$) We treat two cases: infinite cyclic groups and finite cyclic groups.

• We show that every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$. (This is good enough because the relation "are isomorphic" is an equivalence relation on the set of groups. You should prove this, if necessary.[12]) If G is a cyclic group with generator g and operation $*$, then

$$\phi : \mathbb{Z} \to G,$$

given by $\phi(j) = g^j$, is an isomorphism. Of course,

$$g^j \text{ means } \begin{cases} \underbrace{g * g * \cdots * g}_{j \text{ times}}, & \text{if } 0 < j, \\ \text{identity element}, & \text{if } j = 0, \\ \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{|j| \text{ times}}, & \text{if } 0 < j. \end{cases}$$

(Please check, if necessary, that $\phi(j + k) = \phi(j) * \phi(k)$, ϕ is one-to-one, and ϕ is onto.)

• Suppose $A = \langle a \rangle$ and $B = \langle b \rangle$ are both cyclic groups of order n, where n is a finite positive integer. The elements of A are $\{a^j | 0 \le j \le n-1\}$ and the elements of B are $\{b^j | 0 \le j \le n-1\}$, where a^0 is the identity element of A and b^0 is the identity element of B. It is clear that

$$\phi : A \to B,$$

given by $\phi(a^j) = b^j$, for $0 \le j \le n-1$, is a bijection. We show that ϕ is a homomorphism. If $0 \le i, j \le n-1$, then $i + j = k + rn$ for some integers k and r with $0 \le k \le n-1$. Observe that

$$\phi(a^i \cdot a^j) = \phi(a^{i+j}) = \phi(a^{k+rn}) = \phi(a^k \cdot (a^n)^r) = \phi(a^k) = b^k = b^{k+rn} = b^{i+j} = b^i \cdot b^j = \phi(a^i) \cdot \phi(a^j).$$

□

The next project is: What are the subgroups of a cyclic group?

---

[12] A relation ($\sim$) on the set S is an equivalence relation if it is reflexive ($s \sim s$ for all $s \in S$), symmetric ($s \sim s' \Rightarrow s' \sim s$, for all $s, s' \in S$) and transitive ($s \sim s'$ and $s' \sim s''$ for $s, s', s'' \in S$ implies $s \sim s''$).

Example 2.23.

- What are the subgroups of $\mathbb{Z}$?
  Some subgroups that come to mind are:
  $$\langle 0\rangle, \quad \langle 1\rangle, \quad \langle 2\rangle, \quad \langle 3\rangle, \quad \langle 4\rangle, \quad \langle 5\rangle, \quad etc.$$
- What are the subgroups of U_{24}?
  Some subgroups that come to mind are
  $$U_1, \quad U_2, \quad U_3, \quad U_4, \quad U_6, \quad U_8, \quad U_{12}, \quad U_{24}.$$

Proposition 2.24. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle g\rangle$ be a cyclic and let H be a subgroup of G. If H consists only of the identity element, then H is certainly cyclic. Otherwise, there is some positive integer s with $g^s \in H$. Pick s to be the least positive integer with $g^s \in H$. We claim $H = \langle g^s\rangle$.

The inclusion $\supseteq$ is obvious.

We prove the inclusion $\subseteq$. Let $h = g^r$ be an arbitrary element of H. Write $r = \ell s + m$ for integers ℓ and m with $0 \le m \le s-1$. It follows that $g^m \in H$. We picked s to have the property that if $1 \le i \le s-1$, then $g^i \notin H$. Thus, $m = 0$ and
$$h = g^r = g^{\ell s+m} = g^{\ell s} = (g^s)^{\ell} \in \langle g^s\rangle.$$
□

Corollary 2.25. *If G is a finite cyclic group of order n, then G has exactly one subgroup of order d for each divisor d of n.*

Remark 2.26. In Example 2.23 we listed all of the subgroups of U_{24}.

Proof. Let $G = \langle g\rangle$. Fix a divisor d of n. Observe that $\langle g^{n/d}\rangle$ has order d. On the other hand, if H is a subgroup of G of order d, then the proof of Proposition 2.24 shows that $H = \langle g^s\rangle$ where s is the smallest positive exponent with g^s in H. Furthermore, the proof of Proposition 2.24 shows that this s must divide n (otherwise, there is a smaller exponent with g to that exponent is in H) and $\frac{n}{s}$ is the order of H. □

2.E. **Lagrange's Theorem.**

Theorem 2.27. *If H is a subgroup of a finite group G, then the order of H divides the order of G.*

We prove Lagrange's theorem by partitioning G into a bunch of cosets. Each element of G is in exactly one coset. Each coset has the same number of elements as H has.

Before I define coset, I want to point out that the set of cosets of H are an interesting mathematical object. They continue to be interesting even if H and G are infinite.

2.27.1. The group G acts on the set of cosets of H in G. We use this action when we prove the Sylow Theorems.

2.27.2. If H is a "normal" subgroup of G, then the set of cosets of H in G is a new group.

We first prove Lagrange's Theorem.

Theorem. *If H is a subgroup of a finite group G, then the order of H divides the order of G.*

Definition 2.28. If H is a subgroup of the group G and $g \in G$, then

- $gH = \{gh | h \in H\}$ is a left coset of H in G and
- $Hg = \{hg | h \in H\}$ is a right coset of H in G.

The proof of Lagrange's Theorem. Let H be a subgroup of the group G. (Assertions (a) and (b) hold even if the group G is infinite.) We show:

(a) Every element g of G is in exactly one left coset of H in G.
(b) There is a one-to-one correspondence between the the elements of H and the elements of gH for each element g in G.

Once (a) and (b) are established, we apply this information in the case that G is finite to conclude that

the number of elements in G = (the number of left cosets of H in G)×(the number of elements in H).

Proof of (a). Clearly $g \in gH$. If $g \in g_1H$, for some $g_1 \in G$, then we will prove that $gH = g_1H$. Well $g = g_1h_1$ for some $h_1 \in H$.
We show $gH \subseteq g_1H$: If $h \in H$, then $gh = g_1h_1h \in g_1H$.
We show $g_1H \subseteq gH$: If $h \in H$, then $g_1h = gh_1^{-1}h \in gH$.

Proof of (b). Let g be in G. Observe that the function $f : H \to gH$, which is given by $f(h) = gh$, for $h \in H$, is a bijection.

The function f is injective: If $f(h) = f(h')$, for $h, h' \in H$, then $gh = gh'$. Multiply both sides of the equation on the left by g^{-1} to conclude $h = h'$.

The function f is surjective: A typical element in the target of f is equal to gh for some h in H. We see that $f(h)$ is equal to this typical element. □

Corollary 2.29. *If G is a finite Abelian group, then G is cyclic if and only if the order of G is equal to the exponent of G.*

Remarks. (a) The order of the group G is the number of elements in G. The exponent of the group G is the least power n for which g^n is equal to the identity element for all $g \in G$.
(b) One consequence of Lagrange's Theorem is that if G is any finite group then $g^{|G|}$ is the identity element of G for every element g in G. (I used $|G|$ for the order of G.) Thus, the exponent of G is finite (when G is a finite group) and is at most the order of G
(c) In Corollary 2.29, the direction $\Rightarrow$ is obvious.
(d) Corollary 2.29 would be false, if the hypothesis "Abelian" were removed. The group S_3 has order 6 and exponent 6, but is not cyclic.
(e) Corollary 2.29 is an immediate consequence of the structure theorem of finite Abelian groups. (You may use the structure Theorem of finite Abelian group to decide if some claim makes

sense; but you are not allowed to use it to prove results until we prove it.) At any rate, here is the invariant factor form of the structure of Finite Abelian Groups:

If G is a finite Abelian group, then G is isomorphic to

$$C_{d_1} \oplus C_{d_2} \oplus \ldots \oplus C_{d_r} \tag{2.29.1}$$

for some positive integers $d_1, \ldots, d_r$ with $d_1|d_2| \cdots |d_r$, where C_i is the cyclic group of order i.

It is clear that the exponent of the group (2.29.1) is d_r and the order of G is $\prod d_i$. It follows that the exponent of (2.29.1) is equal to the order of (2.29.1) if and only if $r = 1$.

There is also an elementary divisor form of this structure theorem. The invariant factor form corresponds to the rational canonical form of a matrix. The elementary divisor form of the structure of finite Abelian groups corresponds to the Jordan canonical form of a matrix.

We prove Corollary 2.29. We use two Lemmas. The second Lemma (2.31) requires that we know every integer can be factored uniquely into irreducible elements. This is one of my favorite Theorems. (Every PID is a UFD.) We aren't scheduled to prove it until the Chapter on Ring Theory; nonetheless, I like it too much to just fake it here. So, I will prove that the ring $\mathbb{Z}$ is a UFD, but I will do it in a group theory context. The general argument is exactly the same. I might skip it when we get there.

Note. The next Lemma reminds me of one of my favorite ways of getting test questions. Every result has hypotheses and every hypothesis is there for a reason. I often ask for an example that shows that a given hypothesis is necessary. This is also healthy way to study mathematics even if one is not thinking about exams.

Lemma 2.30. *Let x and y be elements in the group G. Suppose x and y have each have finite order, $xy = yx$, and $\langle x\rangle \cap \langle y\rangle = \langle \mathrm{id}\rangle$. Then the order of xy is equal to the least common multiple*[13] *of the order of x and the order of y.*

Proof. It is clear that $(xy)^{\mathrm{lcm}\{o(x),o(y)\}} = \mathrm{id}$. It suffices to prove that $o(x)$ and $o(y)$ both divide $o(xy)$.

Let $r = o(xy)$. It follows that $x^r = y^{-r} \in \langle x\rangle \cap \langle y\rangle = \langle \mathrm{id}\rangle$. Thus $x^r = y^r = \mathrm{id}$. Thus $o(x)|r$, $o(y)|r$, and the proof is complete. □

Lemma 2.31. *If x is an element of the finite Abelian group G and the order of x is maximal among all orders of elements of G, then the order of x is equal to the exponent of G.*

The proof of Lemma 2.31 uses the following Theorem.

Definition 2.32. A non-zero non-unit[14] element r of $\mathbb{Z}$ is <u>irreducible</u> if the only proper subgroup of $\mathbb{Z}$ which contains r is $\langle r\rangle$.

---

[13] We write lcm for least common multiple. The lcm of two integers a and b is the least non-negative integer that a and b both divide.

[14] The units of $\mathbb{Z}$ are $+1$ and -1.

Theorem 2.33. *Every non-zero non-unit of $\mathbb{Z}$ is equal to a finite product of irreducible elements of $\mathbb{Z}$. Furthermore, this factorization into irreducible elements is unique in the sense that if*

$$\prod_{i=1}^{a} r_i = \prod_{j=1}^{b} s_j,$$

with r_i and s_j irreducible integers, then $a = b$, and, after renumbering $r_i = s_i$ for all i.

Lemma 2.34. *The subgroups of $\mathbb{Z}$ satisfy the Ascending Chain Condition* (ACC). *In other words, every ascending chain of subgroups of $\mathbb{Z}$ stabilizes, in the following sense: If*

$$H_1 \subseteq H_2 \subseteq H_3 \subseteq \dots$$

is a chain of subgroups of $\mathbb{Z}$, then there exists an index n with H_n equal to H_m for all m with $n \le m$.

Remark 2.35. The subgroups of $\mathbb{Z}$ do not satisfy the Descending Chain Condition (DCC). Indeed,

$$\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 2^2\mathbb{Z} \supsetneq 2^3\mathbb{Z} \supsetneq \cdots$$

is an infinite properly decreasing chain of subgroups of $\mathbb{Z}$.

Proof of Lemma 2.34. Observe that $\cup_i H_i$ is a subgroup of $\mathbb{Z}$. Every subgroup of $\mathbb{Z}$ is cyclic. Thus $\cup_i H_i = \langle h \rangle$ for some $h \in \mathbb{Z}$. Thus $h \in H_n$, for some n, and $H_n = H_m$ for all m with $n \le m$. □

Lemma 2.36. *If n is an non-zero, non-unit integer, then $n \in \langle r \rangle$ for some irreducible integer r.*

Proof. Suppose n is not in $\langle r \rangle$ for any irreducible integer r. Then n is not irreducible, hence $n = n_0 n_0'$ with neither n_0 nor n_0' a unit.

But n_0 is not irreducible (otherwise $n \in \langle n_0 \rangle$ and n_0 is irreducible); thus, $n_0 = n_1 n_1'$ with neither n_1 nor n_1' a unit.

But n_1 is not irreducible (otherwise $n \in \langle n_1 \rangle$ and n_1 is irreducible); thus, $n_1 = n_2 n_2'$ with neither n_2 nor n_2' a unit.

We have produced an infinite strictly increasing chain of subgroups of $\mathbb{Z}$:

$$\langle n \rangle \subsetneq \langle n_0 \rangle \subsetneq \langle n_1 \rangle \subsetneq \dots \quad .$$

This is a contradiction. □

Lemma 2.37. *If n is a non-zero non-unit element of $\mathbb{Z}$, then n is a finite product of irreducible elements of $\mathbb{Z}$.*

Proof. Apply Lemma 2.36 multiple times

$$n = r_1 n_1 \text{ with } r_1 \text{ an irreducible integer and } n_1 \text{ an integer}$$

If n_1 is not a unit, then

$$n_1 = r_2 n_2 \text{ with } r_2 \text{ an irreducible integer and } n_2 \text{ an integer}$$

If n_2 is not a unit, then

$$n_2 = r_3 n_3 \text{ with } r_3 \text{ an irreducible integer and } n_3 \text{ an integer.}$$

Observe that if n_ℓ is not a unit, then

$$\langle n\rangle \subsetneq \langle n_1\rangle \subsetneq \langle n_2\rangle \subsetneq \langle n_3\rangle \subsetneq \cdots \subsetneq \langle n_{\ell+1}\rangle$$

is a strictly increasing chain of subgroups of $\mathbb{Z}$. The subgroups of $\mathbb{Z}$ satisfy (ACC); so, for some ℓ n_ℓ, is a unit and

$$n = r_1 \cdots r_{\ell-1}(r_\ell n_\ell)$$

is a finite product of irreducible integers. □

September 27, 2023

Due Monday Oct 2, HW3

Due Monday Oct 9, HW4

Exam Wed Oct 18

Are there questions?

Last time we proved that every integer (other than $0, 1, -1$) is equal to a finite product of irreducible integers.

We next prove that is factorization is unique in the sense that if

$$\prod_{i=1}^{s} p_i = \prod_{j=1}^{t} q_j,$$

with p_i and q_j irreducible integers, then $s = t$ and after re-numbering $\langle p_i\rangle = \langle q_i\rangle$ for each i.

Then we prove

Corollary. *If G is a finite Abelian group, then G is cyclic if and only if the order of G is equal to the exponent of G.*

The direction ($\Leftarrow$) is obvious. I owe you ($\Rightarrow$).

We prove 2 Lemmas in order to prove the Corollary.

We have a cool consequence of the Corollary. (But we give a proof that is not yet complete.)

We get to work:

Definition 2.38. The non-zero non-unit integer r is a prime integer if whenever a and b are integers with $ab \in \langle r\rangle$, then $a \in \langle r\rangle$ or $b \in \langle r\rangle$.

Observation 2.39. *Let n be an integer. Then n is prime if and only if n is irreducible.*

Proof. In this argument, n is a non-zero non-unit element of $\mathbb{Z}$.

Assume n is prime integer. We show that n is irreducible. Suppose $\langle a\rangle$ is a proper subgroup of $\mathbb{Z}$ and $n \in \langle a\rangle$. Thus $n = ab$ for some integer b and a is not a unit. The hypothesis that n is prime ensures that $a \in \langle n\rangle$ or $b \in \langle n\rangle$. Observe that $b \notin \langle n\rangle$. Indeed, if $b \in \langle n\rangle$, then $b = b'n$, for some integer b', and $n = ab = ab'n$[15]. Thus, $1 = ab'$ which is absurd because a is not a unit.

[15] Remember that we are thinking about the Abelian group $(\mathbb{Z}, +)$. When we write $n(1 - ab') = 0$, we mean n added to itself $(1 - ab')$ times is zero. Every non-zero element of $(\mathbb{Z}, +)$ has infinite order. The integer n is not zero; hence the integer $1 - ab'$ must be zero.

Thus $a \in \langle n \rangle$ and $a = a'n$, for some integer a', and $n = ab = a'nb$. It follows that $1 = a'b$ and $\langle n \rangle = \langle a \rangle$. We have shown that n is an irreducible element of $\mathbb{Z}$.

Now suppose that n is an irreducible element of $\mathbb{Z}$. We show that n is a prime element of $\mathbb{Z}$. Let a and b be integers with $a \notin \langle n \rangle$ and $b \notin \langle n \rangle$. Apply the definition of irreducible element to see that the subgroups $\langle n, a \rangle$ and $\langle n, b \rangle$ both must equal $\mathbb{Z}$. Thus, there are integers c_1, c_2, d_1, d_2 with

$$1 = c_1 n + c_2 a \quad 1 = d_1 n + d_2 b.$$

Observe that $1 \in \langle n, ab \rangle$. Conclude that $ab \notin \langle n \rangle$. Hence n is a prime element of $\mathbb{Z}$. □

Proof of Theorem 2.33. It suffices to prove that the factorization into irreducible elements is unique. Suppose

$$\prod_{i=1}^{a} r_i = \prod_{j=1}^{b} s_j,$$

with r_i and s_j irreducible integers. The integer r_1 is prime and $\prod_{j=1}^{b} s_j \in \langle r_1 \rangle$; thus some $s_j \in \langle r_1 \rangle$. Renumber the s's, if necessary, to obtain $s_1 \in \langle r_1 \rangle$. The integer s_1 is irreducible; hence $\langle s_1 \rangle = \langle r_1 \rangle$. Thus $s_1 = \pm r_1$ and

$$\prod_{i=2}^{a} r_i = \prod_{j=2}^{b} s_j.$$

Iterate (or induct) to finish the proof. □

We proved the result about factorization in order to prove the following two Lemmas.

Lemma. 2.30 *Let x and y be elements in the group G. Suppose x and y have each have finite order, $xy = yx$, and $\langle x \rangle \cap \langle y \rangle = \langle \mathrm{id} \rangle$. Then the order of xy is equal to the least common multiple*[16] *of the order of x and the order of y.*

Proof. It is clear that $(xy)^{\operatorname{lcm}\{o(x),o(y)\}} = \mathrm{id}$. It suffices to prove that $o(x)$ and $o(y)$ both divide $o(xy)$.

Let $r = o(xy)$. It follows that $x^r = y^{-r} \in \langle x \rangle \cap \langle y \rangle = \langle \mathrm{id} \rangle$. Thus $x^r = y^r = \mathrm{id}$. Thus $o(x)|r$, $o(y)|r$, and the proof is complete. □

Remark. Let x and y be elements of a group. Suppose x and y commute and have relatively prime order. Then the order of xy is the order of x times the order of y

Lemma. 2.31 *If x is an element of the finite Abelian group G and the order of x is maximal among all orders of elements of G, then the order of x is equal to the exponent of G.*

Proof. Let y be an element of G. Suppose that

$$\begin{array}{ll} \text{the order of } x \text{ is} & p_1^{e_1} \cdots p_s^{e_s} \\ \text{the order of } y \text{ is} & p_1^{f_1} \cdots p_s^{f_s}, \end{array}$$

[16] We write lcm for least common multiple. The lcm of two integers a and b is the least non-negative integer that a and b both divide.

where $p_1, \dots, p_s$ are distinct positive prime integers. It suffices to show that $f_i \le e_i$ for all i. We prove this by contradiction. Renumber the p_i, if necessary, and suppose $e_1 < f_1$. We will draw a contradiction.

Observe that the order of $x^{p_1^{e_1}}$ is $p_2^{e_2} \cdots p_s^{e_s}$ and the order of $y^{p_2^{f_2} \cdots p_s^{f_s}}$ is $p_1^{f_1}$. Apply Lemma 2.30 to see that the order of $x^{p_1^{e_1}} y^{p_2^{f_2} \cdots p_s^{f_s}}$ is $p_1^{f_1} p_2^{e_2} \cdots p_s^{e_s}$. Thus we have manufactured an element in G which has order greater than the order of x. This is a contradiction. $\square$

We are now ready to prove

Corollary. 2.29 *If G is a finite Abelian group, then G is cyclic if and only if the order of G is equal to the exponent of G.*

Proof of Corollary 2.29. We need only prove that if the finite Abelian group G has the same order and exponent, then G is cyclic. Let x be an element of G of maximal order. Then

$$\begin{aligned} \text{the order of } x &= \text{the exponent of } G, && \text{by Lemma 2.31} \\ &= \text{the order of } G, && \text{by hypothesis.} \end{aligned}$$

Thus $G = \langle x \rangle$ and G is cyclic. $\square$

October 2, 2023
Due today HW3
Due Monday HW4
Exam Wed Oct 18
Are there questions?

Why do I want you to prove things from scratch, when you already know a big theorem that proves the statement instantly?

A partial proof of a cool corolary.
The arithmetic of cycles.
Quotient groups, normal subgroups, the isomorphism theorems
Last time we proved

Corollary. 2.29 *If G is a finite Abelian group, then G is cyclic if and only if the order of G is equal to the exponent of G.*

Corollary 2.40. *If F is a field, $F^* = (F \setminus \{0\}, \times)$ and G is a finite subgroup of F^*, then G is a cyclic group.*

My "proof" uses the fact that the polynomial ring $F[x]$ is a Unique Factorization Domain. We will eventually prove this fact. We will not have a real proof of Corollary 2.40 until we prove that $F[x]$ is a UFD.

"*Proof*" Let r be the exponent of G. It follows that $g^r = 1$ for all $g \in G$. The fact that $F[x]$ is a UFD guarantees that $x^r - 1$ has at most r roots in F. Thus,

$$\begin{aligned} \text{the exponent of } G &\le \text{the order of } G, && \text{by Lagrange's Theorem,}\\ &\le \text{the exponent of } G. && \text{We just showed this.}\end{aligned}$$

The group G is a finite Abelian group whose order is equal to its exponent. Apply Corollary 2.29 to conclude that G is a cyclic group. $\square$

Remarks.
- The cleanest statement of Corollary 2.40 is that the multiplicative group of a finite field is cyclic.
- Once we prove the theorem about the structure of finite Abelian groups and Gauss' Lemma (that $F[x]$ is a UFD), then Corollary 2.40 is fairly easy to prove.
- The question "Let F be a finite field and let $F^\times$ be the multiplicative group $F \setminus \{0\}$. Describe the structure of the finite Abelian group $F^\times$. Prove that your description is correct." appeared on the Qual.

2.F. **The arithmetic of cycles.** There are seven thoughts about S_n in this subsection.

(1) Every permutation in S_n is equal to a product of disjoint cycles.

Proof. Let σ be an element of S_n. Decompose $\{1, \dots, n\}$ into disjoint orbits under the action of σ. (If $k \in \{1, \dots, n\}$, then the orbit of k under σ is $\{\sigma^i(k) \mid i \in \mathbb{Z}\}$.) Observe that $\sigma|_{\text{any fixed orbit}}$ is a cycle. Observe that $\sigma = \prod_{\text{all orbits}} \sigma|_{\text{orbit}}$, and this is a product of cycles. $\square$

(2) Disjoint cycles in S_n commute.

Proof. If the cycles $(u_1, \dots, u_a)$ and $(v_1, \dots, v_b)$ are disjoint cycles in S_n, then the functions

$$(u_1, \dots, u_a)(v_1, \dots, v_b) \quad \text{and} \quad (v_1, \dots, v_b)(u_1, \dots, u_a)$$

are equal. □

(3) The order of a k-cycle is k. If $\sigma_1, \dots, \sigma_\ell$ are disjoint cycles, then the order of $\sigma_1 \cdots \sigma_\ell$ is the least common multiple of the

$$\{\text{order of } \sigma_1, \text{ order of } \sigma_2, \dots, \text{ order of } \sigma_\ell\}.$$

(See Lemma 2.30.)

(4) Every permutation in S_n is equal to a product of transpositions[17].

Proof. Observe that

$$(1, 2, 3, \dots, r) = (1, r)(1, r-1) \cdots (1, 4)(1, 3)(1, 2).$$

□

(5) The notion of even and odd permutation makes sense.

Observation 2.41. *Suppose that permutation σ in S_n is a product of a transpositions and also is a product of b transpositions. We claim that a and b are both even or a and b are both odd.*

Proof. It suffices to show that $(-1)^a = (-1)^b$. Observe that S_n acts on $\mathbb{Z}[x_1, \dots, x_n]$ by $\sigma(x_i) = x_{\sigma(i)}$. Let $\Delta = \prod_{i<j}(x_j - x_i)$.

Claim 2.42. *If (k, ℓ) in S_n, then $(k, \ell)\Delta = -\Delta$.*

Proof of claim. It does no harm to assume that $k < \ell$. Observe that

$$\Delta = \Bigg(\prod_{\substack{i<j \\ \{i,j\}\cap\{k,\ell\}=\emptyset}} (x_j - x_i) \Bigg) \Bigg(\prod_{i<k} (x_k - x_i)(x_\ell - x_i) \Bigg) \Bigg(\prod_{k<i<\ell} (x_i - x_k)(x_\ell - x_i) \Bigg) \Bigg(\prod_{\ell<i} (x_i - x_\ell)(x_i - x_k) \Bigg) (x_\ell - x_k).$$

$$(k, \ell)(\Delta) = \Bigg(\prod_{\substack{i<j \\ \{i,j\}\cap\{k,\ell\}=\emptyset}} (x_j - x_i) \Bigg) \Bigg(\prod_{i<k} (x_\ell - x_i)(x_k - x_i) \Bigg) \Bigg(\prod_{k<i<\ell} (x_i - x_\ell)(x_k - x_i) \Bigg) \Bigg(\prod_{\ell<i} (x_i - x_k)(x_i - x_\ell) \Bigg) (x_\ell - x_k).$$

The four factors inside $\Big(\ \Big)$ remain unchanged. The factor $(x_\ell - x_k)$ has changed to $(x_k - x_\ell) = -(x_\ell - x_k)$. The claim is established. □

The observation follows readily, because $\sigma(\Delta) = (-1)^a\Delta$ and $\sigma(\Delta) = (-1)^b\Delta$. The polynomial Δ in the domain $\mathbb{Z}[x_1, \dots, x_n]$ is not identically zero; hence $(-1)^a = (-1)^b$, as desired. □

[17] A transposition is a 2-cycle.

Definition 2.43. If the element σ of S_n is equal to the product of an even number of transpositions, then σ is called an even permutation and if σ is equal to the product of an odd number of transpositions, then σ is called an odd permutation.

(6) Define the Alternating group and calculate its order.

Definition 2.44. The alternating group A_n is the following subgroup of S_n:

$$A_n = \{\sigma \in S_n | \sigma \text{ is an even permutation}\}.$$

Observation 2.45. *If $2 \le n$, then A_n has order $\frac{n!}{2}$.*

Proof. All of the odd permutations of S_n are in the coset $(1,2)A_n$. Indeed, S_n is the disjoint union of the cosets $(1)A_n \cup (1,2)A_n$. We saw, when we proved Lagrange's Theorem that all cosets of A_n in S_n have the same number of elements. It follows that the order of A_n is $\frac{1}{2}$ the order of S_n. (Of course, S_n has $n!$ elements.) □

(7) Calculate $\sigma(a_1, \dots, a_r)\sigma^{-1}$ and observe that the Klein 4-group is a normal subgroup of S_4.

Observation 2.46. *If σ and $(a_1, \dots, a_r)$ are permutations in S_n, then*

$$\sigma(a_1, \dots, a_r)\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_r)).$$

Proof. Observe that $\sigma(a_1, \dots, a_r)\sigma^{-1}$ and $(\sigma(a_1), \dots, \sigma(a_r))$ are the exact same function. Each one sends $\sigma(a_i)$ to $\sigma(a_{i+1})$ for $1 \le i \le r-1$, $\sigma(a_r)$ to $\sigma(a_1)$, and leaves

$$\{1, \dots, n\} \setminus \{\sigma(a_1), \dots, \sigma(a_r)\}$$

completely alone. □

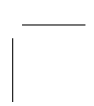
Example 2.47. The subgroup $V_4 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ of S_4 is closed under conjugation. In other words, if $\sigma \in S_4$ and $\tau \in V_4$, then $\sigma\tau\sigma^{-1}$ is in V_4. We learn in the next section that a subgroup which is closed under conjugation is called a normal subgroup. Felix Klein thought about this group V_4 and named it the Vierergruppe.

2.G. **Quotient groups, normal subgroups, the isomorphism theorems.**

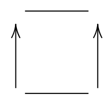
Make identifications to create new objects. Example 1. Surfaces.

One major technique that distinguishes Mathematics from many other disciplines is that in Mathematics one can take a perfectly good thing and one can pretend one part of the original thing is equal to some other part of the original thing and thereby create a brand new perfectly good thing.

The first example that comes to mind is the study of surfaces. One can start with a rectangular surface

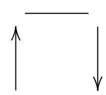


and pretend that each point on the left side is the same as the corresponding point in the right side.



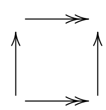
Now one has a cylinder.

Or one can start with a rectangular surface and pretend that each point on the left side is the same as the corresponding point in the right side measured in the opposite direction.



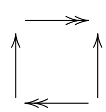
Now one has a Möbius bond.

One can make identifications on a rectangular surface



and create a torus.

One can make identifications on a rectangular surface



and create a Klein bottle.

The cylinder, the Möbius band, and the torus can all be built in 3-space. The Klein bottle can not be built in 3-space but it makes just as much sense to a Mathematician as the other three surfaces.

Oct. 4, 2023
HW4 is due on Monday.
HW5 will be posted soon. It is due on Monday, Oct. 16.
Exam 1 is Wednesday, Oct. 18.

Are there any questions?

Last time we took a topological space, made identifications, and produced a new topological space.

Make identifications to create new objects. Example 2. Groups.

Start with a group G. Pick out two elements g_1 and g_2. Our goal is to create a new group $\bar{G}$ which is as much like G as possible, but in which the image of g_1 in $\bar{G}$ is equal to the image of g_2 in $\bar{G}$. Lets write $\bar{g}_1$ in place of "the image of g_1 in $\bar{G}$".

Notice first that we are putting a relation $\sim$ on G and saying that $\bar{g}_1 = \bar{g}_2$ in $\bar{G}$ if and only if $g_1 \sim g_2$ in G. What kind of relations $\sim$ in G will give rise to groups $\bar{G}$?

(1) The relation $\sim$ better be an equivalence relation because $=$ in $\bar{G}$ is an equivalence relation. (See the footnote 12 on page 21 for the definition of an equivalence relation, if necessary.)
(2) If g_1, g_2, and g_3 are elements of G with $g_1 \sim g_2$, then one must have $g_1g_3 \sim g_2g_3$.
(3) In particular, $g_1 \sim g_2$ if and only if $g_1g_2^{-1} \sim e$ where e is the identity element of G.
(4) Hence, it suffices to figure out which elements g in G satisfy $g \sim e$. Let $N = \{g \in G \mid g \sim e\}$.
(5) Observe that N must be a subgroup.
(6) Observe that if $n \in N$ and g is an arbitrary element of G, then $gng^{-1} \sim geg^{-1} = e$; hence gng^{-1} must be in N.

Definition 2.48. If N is a subgroup of G and $gng^{-1} \in N$ for all $n \in N$ and $g \in G$, then G is called a normal subgroup of G.[18]

Remark. Sometimes it is easier to make sense of words than symbols. Here is Definition 2.48 expressed in words. A subgroup N of the group G is a normal subgroup if N is closed under conjugation by elements of G.

Definition 2.49. If N is a normal subgroup of G, then consider the set

$$\frac{G}{N} = \{\bar{g} \mid g \in G \text{ and } \bar{g}_1 = \bar{g}_2 \iff g_1g_2^{-1} \in N\}.$$

Remark. Here are two other ways two other ways to think of the set $\frac{G}{N}$.

- The set $\frac{G}{N}$ is the set of equivalence classes in G, where $g_1 \sim g_2$ if and only if $g_1g_2^{-1} \in N$.
- The set $\frac{G}{N}$ is the set of left cosets of N in G.

Theorem 2.50. *If N is a normal subgroup of the group G, then $\frac{G}{N}$ is a group with operation*

$$\bar{g}_1\bar{g}_2 = \overline{g_1g_2}.$$

Furthermore, the identity element of $\frac{G}{N}$ is $\bar{e}$, where e is the identity element of G and if g is an element of G, then the inverse of $\bar{g}$ is $\overline{g^{-1}}$.

Proof. **We must show that the proposed operation in $\frac{G}{N}$ makes sense.** In other words, suppose $\bar{g}_i = \bar{h}_i$ for $i \in \{1, 2\}$ and $g_1, g_2, h_1, h_2 \in G$. We must show that $\overline{g_1g_2} = \overline{h_1h_2}$.

Well, if $i \in \{1, 2\}$, then $g_i = h_in_i$ for some n_1, n_2 in N. Thus

$$g_1g_2 = h_1n_1h_2n_2 = h_1h_2(h_2^{-1}n_1h_2)n_2.$$

The subgroup N of G is normal so $h_2^{-1}n_1h_2 \in N$ and and $(h_2^{-1}n_1h_2)n_2 \in N$. Thus, $\overline{g_1g_2} = \overline{h_1h_2}$.

It is now completely trivial to show that $\frac{G}{N}$ satisfies all of the group axioms. □

Examples 2.51. (a) If G is an Abelian group, then every subgroup of G is normal.
(b) If n is a positive integer, then $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is the cyclic group of order n.

[18] The symbols "$N \lhd G$" mean "N is a normal subgroup of G".

(c) The subgroup $\langle(1,2)\rangle$ of S_3 is not normal because

$$(1,2,3)(1,2)(1,2,3)^{-1} = (2,3) \notin \langle(1,2)\rangle.$$

(d) The subgroup $\{(1),(1,2)(1,3),(1,3)(2,4),(1,4)(2,3)\}$ is a normal subgroup of S_4, A_4, and D_4. (See Example 2.47.)

(e) Every subgroup of index 2 is normal.

Proof. Let N be a subgroup of G of index two. Notice that if g is an element of G which is not in N, then

(2.51.1) G is the disjoint union of the left cosets $N \cup gN$.

We show that N is a normal subgroup of G. Take $n \in N$ and $g \in G$. If $g \in N$, then it is obvious that $gng^{-1} \in N$. Henceforth, $g \notin N$. We assume that $gng^{-1} \notin N$. We will reach a contradiction. If $gng^{-1} \notin N$, then by (2.51.1) $gng^{-1} \in gN$; hence $ng^{-1} \in N$ and $g^{-1} \in N$, which is impossible. □

(f) Consider the group Q_8, which is the eight element group generated by a, b with $a^4 = e$, $b^2 = a^2$, and $ba = a^3 b$. The only element of Q_4 of order 2 is a^2. Observe that $\langle a^2\rangle$ is a normal subgroup of Q_8 (because conjugation preserves order. That is, if g, h are elements of a group, then g and hgh^{-1} have the same order.)

There is also another way to see that $\langle a^2\rangle \lhd Q_8$. If G is a group, then the <u>center</u> of G is

$$Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}.$$

It is true (and easy to see) that

$$Z(G) \lhd G$$

for all groups G. Furthermore, one can verify that $Z(Q_8) = \langle a^2\rangle$.

(g) Let $\phi : G \to G'$ be a group homomorphism and let

$$\ker\phi = \{g \in G \mid \phi(g) \text{ is equal to the identity element of } G'\}.$$

Then $\ker\phi$ is a normal subgroup of G.

Proof. Check that $\ker\phi$ is closed under the operation of G. Check that if $g \in \ker\phi$, then $g^{-1} \in \ker\phi$. Check that $\ker\phi$ is closed under conjugation. □

Theorem 2.52. [The First Isomorphism Theorem.] *Let $\phi : G \to G'$ be a group homomorphism.*

(a) *If N is a normal subgroup of G and $N \subseteq \ker\phi$, then ϕ induces a group homomorphism $\bar\phi : \frac{G}{N} \to G'$, with*

$$\bar\phi(\bar g) = \phi(g).$$

(b) *The homomorphism*

$$\bar\phi : \frac{G}{\ker\phi} \to \operatorname{im}\phi$$

is an isomorphism.

Remark 2.53. It is very difficult to produce homomorphisms from random groups. To create such a homomorphism, I usually view the random group as a quotient of a well-understood group, I create a homomorphism from the well understood group, and then I apply the First Isomorphism Theorem.

• Here is my first example of this philosophy. When we proved that all cyclic groups of order n are isomorphic, we gave an unpleasant argument. The "correct" argument is to show that any group of order n is isomorphic to $\frac{\mathbb{Z}}{n\mathbb{Z}}$:

Let G be a cyclic group of order n with generator g. (Call the operation in G "times".) Define $\phi : \mathbb{Z} \to G$ with $\phi(r) = g^r$. This is a homomorphism. Apply the First Isomorphism Theorem to conclude that $\bar{\phi} : \frac{\mathbb{Z}}{n\mathbb{Z}} \to G$ is an isomorphism.

• Here is a second example of this philosophy. The last time I taught the course, I put

Suppose that G is a group with 16 elements and $g^2 = \text{id}$ for all $g \in G$, where id is the identity element of G.

(a) **Prove that G is Abelian.**

(b) **Prove that G is isomorphic to $C_2 \oplus C_2 \oplus C_2 \oplus C_2$, where C_2 is equal to the group of complex numbers $\{1, -1\}$ under multiplication.**

as one of the questions on the exam.

I was horrified how many students defined their isomorphism "the wrong way". The "right way" to define the isomorphism is **from $C_2 \oplus C_2 \oplus C_2 \oplus C_2$**.

Proof of the First Isomorphism Theorem, Theorem 2.52.

We must show that $\bar{\phi}$ of (a) **is a legitimate function.** Once we do that, then everything else is obvious.

Suppose that g_1 and g_2 are elements of G with $\bar{g}_1 = \bar{g}_2$ in $\frac{G}{N}$. We must show that $\phi(g_1) = \phi(g_2)$.

The hypothesis $\bar{g}_1 = \bar{g}_2$ in $\frac{G}{N}$ guarantees that

$$g_1 g_2^{-1} \in N \subseteq \ker \phi.$$

It follows that $\phi(g_1 g_2^{-1})$ is the identity element of G'; and therefore, $\phi(g_1) = \phi(g_2)$. ☐

Example 2.54. The groups $\frac{\mathbb{R}}{\mathbb{Z}}$ and U are isomorphic.

Proof. Consider the homomorphism $\phi : \mathbb{R} \to U$, which is given by $\phi(\theta) = e^{2\pi i\theta}$. Apply the First Isomorphism Theorem. ☐

Example 2.55. The groups $\frac{U}{U_2}$ and U are isomorphic.

Proof. Consider the homomorphism $\phi : U \to U$, which is given by $\phi(u) = u^2$. Apply the First Isomorphism Theorem. ☐

Example 2.56. The groups $\frac{U}{U_n}$ and U are isomorphic.

Proof. Consider the homomorphism $\phi : U \to U$, which is given by $\phi(u) = u^n$. Apply the First Isomorphism Theorem. □

Example 2.57. The groups $\frac{S_4}{V_4}$ and S_3 are isomorphic.

Proof. This one is sneaky. I do not know any homomorphisms from $S_4 \to S_3$. Instead, I propose that we consider $\phi : S_3 \to \frac{S_4}{V_4}$ to be the composition of the following two homomorphisms[19]:

$$S_3 \xrightarrow{\text{inclusion}} S_4 \xrightarrow{\text{natural quotient map}} \frac{S_4}{V_4}.$$

So, ϕ is automatically a homomorphism.

Observe that the kernel of ϕ is (1) because (1) is the only element of

$$V_4 \cap S_3.$$

Thus ϕ is an injection.[20]

An injective function from a six element set to a six element set is necessarily surjective. □

Example 2.58. The groups $\frac{S_n}{A_n}$ and U_2 are isomorphic.

Proof. Define $\phi : S_n \to U_2$ by

$$\phi(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Verify that ϕ is a homomorphism. Apply the First Isomorphism Theorem. □

Example 2.59. The groups $\frac{O_n(\mathbb{R})}{\mathrm{SO}_n(\mathbb{R})}$ and U_2 are isomorphic.

Proof. Define $\phi : O_n(\mathbb{R}) \to U_2$ by $\phi(M) = \det M$ for $M \in O_2(\mathbb{R})$. Apply the First Isomorphism Theorem. □

Example 2.60. If r and s are relatively prime integers[21], then

$$\frac{\mathbb{Z}}{rs\mathbb{Z}} \cong \frac{\mathbb{Z}}{r\mathbb{Z}} \oplus \frac{\mathbb{Z}}{s\mathbb{Z}}.$$

This assertion is usually called the Chinese Remainder Theorem.

Lemma 2.60.1. *If r and s are integers with greatest common divisor d[22], then there exist integers a and b with $ar + bs = d$.*

[19]If N is a normal subgroup of the group G, then the function $\phi : G \to \frac{G}{N}$, which is given by $\phi(g) = \bar{g}$, for all $g \in G$, is a group homomorphism. This homomorphism is called the natural quotient map.

[20]Have I ever said out loud that the homomorphism ϕ is an injection if and only if the kernel of ϕ consists of the identity element? At any rate, it is true, easy to prove, and very useful.

[21]We have established Theorem 2.33; so we have complete understanding of the phrase "relatively prime". In particular, "r and s are relatively prime" means that the only integers that divide both r and s are 1 and -1.

[22]Again, we have established Theorem 2.33 so we have complete understanding of the phrase "greatest common divisor". In particular, the greatest integer that divides both r and s is the greatest common divisor of r and s.

Proof. We proved in Proposition 2.24 that the smallest subgroup of $\mathbb{Z}$ that contains r and s, denoted $\langle r, s\rangle$, is cyclic. Let t be the name of the generator; so $\langle r, s\rangle = \langle t\rangle$. The integer $-t$ also generates $\langle r, s\rangle$. So change t to negative t, if necessary. We may assume that t is positive and $\langle r, s\rangle = \langle t\rangle$. The fact that $t \in \langle r, s\rangle$ ensures that $t = ar + bs$ for some integers a and b. We need only show that t is the greatest common divisor of a and b. The fact that $\langle r, s\rangle \subseteq \langle t\rangle$ ensures that t is a common factor of r and s. On the other hand, the equation $t = ar + bs$ guarantees that every common factor of r and s also divides t. □

Now prove the assertion of (2.60). Define $\phi : \mathbb{Z} \to \frac{\mathbb{Z}}{r\mathbb{Z}} \oplus \frac{\mathbb{Z}}{s\mathbb{Z}}$ by $\phi(n) = (\bar{n}, \bar{n})$. Observe that ϕ is a homomorphism.

We prove that ϕ is surjective. We know from Lemma 2.60.1 that there are integers a and b with $ra + bs = 1$. Observe that $\phi(1 - ar) = (\bar{1}, \bar{0})$ and $\phi(1 - bs) = (\bar{0}, \bar{1})$. Every element in the target can be written in terms of $(\bar{1}, \bar{0})$ and $(\bar{0}, \bar{1})$. We conclude that ϕ is surjective.

Observe that $\langle rs\rangle \subseteq \ker \phi$. Apply the first part of the First Isomorphism Theorem to conclude that

$$\bar{\phi} : \frac{\mathbb{Z}}{\langle rs\rangle} \to \frac{\mathbb{Z}}{r\mathbb{Z}} \oplus \frac{\mathbb{Z}}{s\mathbb{Z}}$$

is a group homomorphism. A surjective function from a set with rs elements to a set with rs elements is necessarily injective.

Example 2.61. Recall the group $D_n = \langle \sigma, \rho\rangle$, where σ is reflection across the x-axis and ρ is rotation (ccw) by $\frac{2\pi}{n}$. We know from Theorem 2.11.1 that D_n has $2n$ elements. We also know that $\sigma^2 = \mathrm{id}$, $\rho^n = \mathrm{id}$, and $(\rho\sigma)^2 = \mathrm{id}$. How does one construct a homomorphism from D_n?

Theorem 2.61.1. *Let $\langle x, y\rangle$ be the free group on x and y and let N be the smallest*[23] *normal subgroup of $\langle x, y\rangle$ which contains x^2, y^n, and $(xy)^2$. Then the following statements hold.*

(a) *The groups D_n and $\frac{\langle x,y\rangle}{N}$ are isomorphic.*
(b) *If G is a group and g_1 and g_2 are elements of G with $g_1^2 = \mathrm{id}$, $g_2^n = \mathrm{id}$, and $(g_1 g_2)^2 = \mathrm{id}$, then there exists a group homomorphism $\Phi : D_n \to G$ with $\Phi(\sigma) = g_1$ and $\Phi(\rho) = g_2$.*

Proof. We first prove (a). Start with the homomorphism[24] $\phi : \langle x, y\rangle \to D_n$, given by $\phi(x) = \sigma$ and $\phi(y) = \rho$. Observe that x^2, y^n, and $(xy)^2$ are in $\ker \phi$ (which is a normal subgroup of $\langle x, y\rangle$). It follows that N (which is the smallest normal subgroup of $\langle x, y\rangle$ that contains x^2, y^n, and $(xy)^2$) is contained in $\ker \phi$. The First Isomorphism Theorem guarantees that there exists a homomorphism

$$\bar{\phi} : \frac{\langle x, y\rangle}{N} \to D_n,$$

with $\bar{\phi}(\bar{x}) = \sigma$ and $\bar{\phi}(\bar{y}) = \rho$. Observe that $\bar{\phi}$ is surjective and that the domain of $\bar{\phi}$ has at most $2n$ elements. Conclude that $\frac{\langle x,y\rangle}{N}$ has exactly $2n$ elements and $\bar{\phi}$ is an isomorphism.

[23] There does exist a smallest normal subgroup of $\langle x, y\rangle$ which contains x^2, y^2, and $(xy)^2$. Indeed, the set of normal subgroups of $\langle x, y\rangle$ which contains x^2, y^2, and $(xy)^2$ is not empty, because $\langle x, y\rangle$ is one such group. Thus, $N = \cap H$ as H roams over all normal subgroups of $\langle x, y\rangle$ which contains x^2, y^2, and $(xy)^2$.

[24] The group $\langle x, y\rangle$ is a free group, we are free to map the generators anywhere we want.

(b) The group $\langle x, y\rangle$ is a free group; so there exists a homomorphism $\psi : \langle x, y\rangle \to G$ with $\psi(x) = g_1$ and $\psi(y) = g_2$. Observe that $N \subseteq \ker \psi$. The First Isomorphism Theorem guarantees that there exists a homomorphism $\bar\psi : \frac{F}{N} \to G$ with $\bar\psi(\bar x) = g_1$ and $\bar\psi(\bar y) = g_2$. Let $\Phi : D_n \to G$ be the composition

$$D_n \xrightarrow{\bar\phi^{-1}} \frac{F}{N} \xrightarrow{\bar\psi} G.$$

Observe that $\Phi(\sigma) = g_1$ and $\Phi(\tau) = g_2$. □

Example 2.62. How does one construct a group homomorphism from the group Q_8? Recall that Q_8 is an eight element group with distinct elements of the form $a^i b^j$, with $0 \le i \le 3$ and $0 \le j \le 1$ whose elements satisfy $a^4 = 1$, $b^2 = a^2$, $ba = a^3 b$.

Exercise 2.62.1. [25] *Let $\langle x, y\rangle$ be the free group on x and y and let N be the smallest normal subgroup of $\langle x, y\rangle$ which contains x^4, x^2y^{-2}, and $yxy^{-1}x^{-3}$. Then the following statements hold.*

(a) *The groups Q_8 and $\frac{\langle x,y\rangle}{N}$ are isomorphic.*
(b) *If G is a group and g_1 and g_2 are elements of G with $g_1^4 = \mathrm{id}$, $g_2^2 = g_1^2$, and $g_2g_1 = g_1^3g_2$, then there exists a group homomorphism $\Phi : Q_8 \to G$ with $\Phi(\sigma) = g_1$ and $\Phi(\rho) = g_2$.*

Theorem 2.63. [The Second Isomorphism Theorem.] *If K is a normal subgroup of the group G, then the following statements hold.*

(a) *There is a one-to-one correspondence between the subgroups of G which contain K and the subgroups of $\frac{G}{K}$. If H is a subgroup of G which contains K, then the corresponding subgroup of $\frac{G}{K}$ is $\frac{H}{K}$. If $\mathscr{H}$ is a subgroup of $\frac{G}{K}$, then the corresponding subgroup of G is*
$$\widehat{\mathscr{H}} = \{h \in G \mid \bar h \in \mathscr{H}\}.$$
(b) *If H is a subgroup of G with K a subgroup of H, then H is a normal subgroup of G if and only if $\frac{H}{K}$ is a normal subgroup of $\frac{G}{K}$.*
(c) *If H is a normal subgroup of G with K a subgroup of H, then*
$$\frac{\frac{G}{K}}{\frac{H}{K}} \cong \frac{G}{H}.$$

Proof. We prove (a).

- Let H be a subgroup of G containing K. Verify that $\frac{H}{K}$ is a subgroup of $\frac{G}{K}$.
- Let $\mathscr{H}$ be a subgroup of $\frac{G}{K}$. Verify that $\widehat{\mathscr{H}}$ is a subgroup of G which contains K.
- Let H be a subgroup of G containing K. verify that
$$\widehat{\frac{H}{K}} = H.$$
- Let $\mathscr{H}$ be a subgroup of $\frac{G}{K}$. Verify that
$$\frac{\widehat{\mathscr{H}}}{K} = \mathscr{H}.$$

[25] If the statement is true, then prove it. If the statement is false, then fix it and prove it.

We prove (b).

$H \lhd G \Rightarrow \frac{H}{K} \lhd \frac{G}{K}$:

If $\bar{h} \in \frac{H}{K}$ and $\bar{g} \in \frac{G}{K}$, then

$$\bar{g}\bar{h}\bar{g}^{-1} = \overline{ghg^{-1}} \in \frac{H}{K}.$$

$H \lhd G \Leftarrow \frac{H}{K} \lhd \frac{G}{K}$:

Take $h \in H$ and $g \in G$. Then $\bar{h} \in \frac{H}{K}$ and $\bar{g} \in \frac{G}{K}$. Thus, $\bar{g}\bar{h}\bar{g}^{-1} \in \frac{H}{K}$; but

$$\bar{g}\bar{h}\bar{g}^{-1} = \overline{ghg^{-1}}.$$

Thus $\overline{ghg^{-1}} \in \frac{H}{K}$ and $ghg^{-1} \in H$.

We prove (c). Consider the natural quotient map

$$G \xrightarrow{\theta} \frac{G}{H}.$$

Observe that $K \subseteq \ker \theta$. Apply the First Isomorphism Theorem to see that

$$\bar{\theta} : \frac{G}{K} \to \frac{G}{H},$$

given by $\bar{\theta}(gK) = gH$ is a well-defined group homomorphism. Apply the other part of the First Isomorphism Theorem to see that

$$\frac{\frac{G}{K}}{\ker \bar{\theta}} \cong \operatorname{im} \bar{\theta}.$$

Observe that $\bar{\theta}$ is surjective and $\ker \bar{\theta} = \frac{H}{K}$. Conclude that

$$\frac{\frac{G}{K}}{\frac{H}{K}} \cong \frac{G}{H}.$$

□

Example 2.64. What are the subgroups of $\frac{S_4}{V_4}$?

We know that the composition

$$S_3 \xrightarrow{inclusion} S_4 \xrightarrow{natural quotient map} \frac{S_4}{V_4}$$

is an isomorphism. We also know that the subgroups of S_3 are

$$\langle \mathrm{id} \rangle, \quad \langle (1,2) \rangle, \quad \langle (1,3) \rangle, \quad \langle (2,3) \rangle, \quad A_3, \quad \text{and} \quad S_3.$$

So the subgroups of $\frac{S_4}{V_4}$ are

$$\frac{V_4}{V_4}, \quad \frac{\langle (1,2) \rangle V_4}{V_4}, \quad \frac{\langle (1,3) \rangle V_4}{V_4}, \quad \frac{\langle (2,3) \rangle V_4}{V_4}, \quad \frac{A_3 V_4}{V_4}, \quad \text{and} \quad \frac{S_3 V_4}{V_4}.$$

Notice that if H is a subgroup of a group G and N is a normal subgroup of G, then

$$HN = \{hn \mid h \in H \text{ and } n \in N\}$$

is a subgroup of G and of course is the smallest subgroup of G which contains H and N. Observe that the above set HN is closed. If $h_1, h_2 \in H$ and $n_1, n_2 \in N$, then

$$(h_1 n_1)(h_2 n_2) = h_1 h_2 (h_2^{-1} n_1 h_2) n_2$$

with $h_1 h_2$ in H because H is a subgroup of G and $(h_2^{-1} n_1 h_2) n_2$ in N because N is a normal subgroup of G. A different way to write the subgroups of S_4 which contain V_4 is

$$V_4, \quad \langle (1,2), V_4 \rangle, \quad \langle (1,3), V_4 \rangle, \quad \langle (2,3), V_4 \rangle, \quad A_4, \quad \text{and} \quad S_4.$$

Theorem 2.65. [The Third Isomorphism Theorem.] *Let G be a group, N be a normal subgroup of G, and K be a subgroup of G. Then $K \cap N$ is a normal subgroup of K and*

$$\frac{KN}{N} \cong \frac{K}{K \cap N}.$$

Proof. There exists a homomorphism $\theta : K \to \frac{KN}{N}$, which is given by $\theta(k) = \bar{k}$. (This map is inclusion followed by the natural quotient map.) It is clear that θ is surjective and that the kernel of θ is $K \cap N$. □

2.H. **Groups acting on sets.**

Definition 2.66. The group G acts on the set S if there is a function

$$G \times S \to S,$$

written as

$$(g, s) \mapsto gs,$$

which satisfies:

(a) $\mathrm{id}(s) = s$ for all $s \in S$, and
(b) $g(hs) = (gh)s$ for all $g, h \in G$ and $s \in S$.

Examples 2.67. (1) The group S_n acts on the set $\{1, 2, \dots, n\}$.
(2) The group $\mathrm{GL}_n(\mathbb{R})$ acts on the set $\mathbb{R}^n$.
(3) Every group G acts on itself by left translation.
(4) Every group G acts on itself by conjugation.
(5) If H is a subgroup of G, then G acts on the set of left cosets of H in G by left translation.
(6) If $K \triangleleft G$, then G acts on K by conjugation.

Some Ideas 2.68. Let the group G act on the set S.

(1) If $x \in S$, then the orbit of x is $\{gx | g \in G\}$.
(2) The group G partitions the set S into a collection of disjoint orbits. For example, when $\mathrm{SO}_2(\mathbb{R})$ acts on $\mathbb{R}^2$, then the action partitions xy-plane into the set of circles with center $(0, 0)$.
(3) If $x \in S$, then the <u>stabilizer</u> of x is $\operatorname{stab} x = \{g \in G \mid gx = x\}$.

(4) Observe that if $x \in S$, then the orbit of x is equal to

$$\{gx | \text{where we take one representative from each left coset of } \operatorname{stab} x \text{ in } G\}.$$

Thus[26], $|\text{orbit } x| = [G : \operatorname{stab} x]$.

Conclusion 2.69. *If G is a group which acts on a finite set S, then*

$$|S| = \sum_x [G : \operatorname{stab} x],$$

where the sum is taken over one element x from each orbit.

Application 2.70. *Let G be a finite group and let G act on itself by conjugation. The orbits of this action are the set of conjugacy classes of G.*[27] *If $g \in G$, then*

$$\operatorname{stab} g = \{h \in G \mid hgh^{-1} = g\}.$$

This set is called the centralizer of g in G. One obtains the equation

$$|G| = \sum_{x_i} [G : C(x_i)],$$

where one x_i is taken from each conjugacy class of G. It is often useful to separate the conjugacy classes which have exactly one element.

Theorem 2.71. [The Class Equation] *If G is a finite group with center*[28] *C, then*

$$|G| = |C| + \sum_{x_i} [G : C(x_i)],$$

where one x_i is taken from each conjugacy class of G which contains more than element.

Corollary 2.72. *Let p be a prime integer and n be a positive integer. If G is a group of order p^n, then G has a non-trivial center.*

Remark. The assertion of Corollary 2.72 is that the center of G is larger than merely the identity element of G.

Proof. The Class equation gives that

$$|G| = |C| + \sum_{x_i} [G : C(x_i)],$$

where one x_i is taken from each conjugacy class of G which contains more than element. Observe that $1 \le |C|$, p divides $|G|$, and p divides each $[G : C(x_i)]$ that appears. Thus $1 < |C|$. □

Theorem. *If G is a group of order p^n for some n with $1 \le n$, then G has a non-trivial center.*

[26] I am writing $[G : H]$ for the number of left cosets of H in G. I used a slightly different notation in Homework problem 8. This number is called the index of H in G.

[27] If $g \in G$, then the conjugacy class of g in G is $\{hgh^{-1} \mid h \in G\}$.

[28] The center of the group G is the set of elements of G that commute with every element of G.

Proof. Let G act on G by conjugation. Then

$$\underbrace{|G|}_{p \text{ divides this}} = \overbrace{\underbrace{|\{g \in G | \{g\} = \text{orbit}(g)\}|}_{\text{This number is not zero}}}^{\text{the center of } G} + \sum_{g} \underbrace{\underbrace{|\,\text{orbit}(g)|}_{[G\,:\,\text{stab}\,g]}}_{p \text{ divides this}},$$

where the sum is taken over the orbits of size larger than one and exactly one g is taken from each orbit. ☐

Corollary 2.73. *If G is a group of order p^2, where p is a prime integer, then G is Abelian.*

Proof. Let C be the center of G. Apply Corollary 2.72 to see that $1 < |C|$. Apply Lagrange's Theorem to see that $|C|$ is equal to p or p^2.

It suffices to prove that $p \neq |C|$. Assume $|C| = p$. We will reach a contradiction. It is clear that $C \lhd G$. Thus, $|\frac{G}{C}| = p$. Apply Lagrange's Theorem to see that $\frac{G}{C}$ is a cyclic group. It follows that there is an element $g \in G$ such that every element of G has the form $g^i c$ for some i and some $c \in C$. It is clear that $g^i c$ and $g^j c'$ commute for all integers i and j and all elements c and c' in C. We have proven that G is an Abelian group and this is absurd because, the center of G is a proper subgroup of G. ☐

Corollary 2.74. *If p is a prime integer, then every group of order p^2 is isomorphic to $\frac{\mathbb{Z}}{p^2\mathbb{Z}}$ or $\frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p\mathbb{Z}}$.*

Proof. Let G be a non-cyclic group of order p^2. By Lagrange's Theorem every non-identity element of G has order p. Let a be one of these elements. Take $b \in G \setminus \langle a \rangle$. Observe that $\langle b \rangle \cap \langle a \rangle = \{\text{id}\}$. Otherwise, there exists i with b^i equal to a non-identity element of $\langle a \rangle$. Every non-identity element of $\langle a \rangle$ generates $\langle a \rangle$. In this case,

$$\langle a \rangle \subsetneq \langle b \rangle$$

and each group has order p. This of course, is absurd.

Use the First Isomorphism Theorem to see that there are group homomorphisms $\frac{\mathbb{Z}}{p\mathbb{Z}} \to G$ given by

$$\bar{n} \mapsto a^n \quad \text{and} \quad \bar{m} \mapsto b^m.$$

We proved in Corollary 2.73 that G is Abelian, so we may apply the Universal Mapping Property for direct sum of Abelian groups to see that there exists a homomorphism

$$\phi : \frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p\mathbb{Z}} \to G$$

with

$$\phi((\bar{n}, \bar{m})) = a^n b^m.$$

The image of ϕ is a subgroup of G of order greater than p (because $\langle a \rangle$ has order p and $b \notin \langle a \rangle$. The only subgroup of G which has order larger than p is G itself. Thus, ϕ is surjective. Every surjective function from a set of size p^2 to a set of size p^2 is necessarily injective. Thus, ϕ is an isomorphism. ☐

2.I. **The Sylow Theorems.**

Definition 2.75. Let G be a finite group and p be a prime integer which divides the order of G. If p^r divides the order of G and p^{r+1} does not divide the order of G, then any subgroup of G of order p^r is called a Sylow p-subgroup of G.

Theorem 2.76. *Let G be a finite group and p be a prime integer which divides the order of G. Then the following statements hold.*

(a) *If p^r divides the order of G, then G has a subgroup of order p^r.*
(b) *Every subgroup of G of order p^r is contained in a Sylow p-subgroup of G.*
(c) *Any two Sylow p-subgroups of G are conjugate. (In other words, if H_1 and H_2 are Sylow p-subgroups of G, then there is an element $g \in G$ such that $gH_1g^{-1} = H_2$.)*
(d) *If n is the number of Sylow p-subgroups then*
    (i) *n divides the index $[G : \text{a Sylow } p\text{-subgroup}]$ and*
    (ii) $n \equiv 1 \mod p$.

The First Step 2.77. (Cauchy's Theorem) *Let G be a finite group and p be a prime integer which divides the order of G. Then G has an element of order p.*

Warm Up. Think about $p = 2$. Pair every element up with its inverse. Some of these pairings have size 2; the pairing that goes with id has size 1. The group has even size; thus there must be some non-identity element which is its own inverse.

We want to generalize this approach to work for all p. I propose that we think of the set of tuples of length 2 so that the product of the two elements is the identity. Let $\mathbb{Z}/2\mathbb{Z}$ act on this set by cyclic permutation. The set of such tuples decomposes into disjoint orbits. We want to count the number of orbits which have size 1.

Proof. Let
$$S = \{(a_1, \dots, a_p) \mid a_i \in G \text{ and } a_1 \cdots a_p = \text{id}\}.$$
Observe that $|S| = |G|^{p-1}$. Indeed, one can pick $a_1, \dots, a_{p-1}$ at random and then one is forced to choose $a_p = (a_1 \cdots a_{p-1})^{-1}$. Let $\frac{\mathbb{Z}}{p\mathbb{Z}}$ act on S by cyclic permutation:
$$k(a_1, \dots a_p) = (a_{k+1}, \dots, a_p, a_1, \dots, a_k).$$
This is an action because
$$0(a_1, \dots a_p) = (a_1, \dots a_p)$$
and
$$k'(k((a_1, \dots a_p)) = (k' + k)(a_1, \dots a_p).$$
Thus,
$$|S| = |\{s \in S \mid |\text{orbit of s}| = 1\}| + \sum |\text{orbit of } s|,$$
where the sum is taken over one s from each orbit with at least two elements. We know that p divides $|S|$. If the orbit of s has more than one element, then
$$|\text{the orbit of s}| = [\tfrac{\mathbb{Z}}{p\mathbb{Z}} : \text{stab}\, s]$$

and this number is divisible by p. Thus, p divides $|\{s \in S \mid |\text{orbit of s}| = 1\}|$ and there is an element x in G, with x not the identity element and $x^p = \text{id}$. $\square$

The Next Step 2.78. *We prove assertions* (a) *and* (b) *of Theorem* 2.76.

Let G be a finite group. Suppose p is a prime integer and p divides the order of G. The following statements hold.

(a) If p^n divides the order of G, then G has a subgroup of order p^n.
(b) Every subgroup of G of order p^n is contained in some Sylow p-subgroup of G.

Proof. The proof is by induction. Suppose p^r divides the order of G and p^{r+1} does not divide the order of G. Suppose that H is a subgroup of G of order p^n for some n with $1 \le n \le r-1$. We prove that there exists a subgroup H_1 of G with $H \subseteq H_1$ and $|H_1| = p^{n+1}$.

Let H act on the left cosets of H in G by left translation.

Let S be the set of left cosets of H in G. We see that

$$|S| = |\{s \in S|\text{ the orbit of } s \text{ has one element}\}| + \sum |\text{the orbit of } s|,$$

where the sum is taken over one s from each large orbit.

Observe that $|S| = [G : H]$. The hypothesis ensures that p divides this number.

If the orbit of s has more than one element, then $|\text{orbit of } s| = [H : \text{stab}\, s]$. We arranged that $[H : \text{stab}\, s] \neq 1$. Thus p divides $[H : \text{stab}\, s]$. It follows that

$$p \text{ divides } |\{s \in S|\text{ the orbit of } s \text{ has one element}\}|.$$

Thus,

$$p \text{ divides } |\{xH | hxH = xH \text{ for all } h \in H\}| \textit{ and}$$

$$p \text{ divides } |\{xH | x^{-1}hx \in H \text{ for all } h \in H\}|.$$

Observe that $\{x \in G | x^{-1}hx \in H \text{ for all } h \in H\}$ is a subgroup of G. This subgroup is called the normalizer of H in G. It might be denoted as $N(H)$ or $N_G(H)$. At any rate $H \lhd N(H)$. Thus,

$$\frac{N(H)}{H}$$

is a legitimate group and we have shown that p divides the order of this group. Apply 2.77 to see that

$$\frac{N(H)}{H}$$

has an element of order p. In other words, $N(H)$ has a subgroup of order p^{n+1} and this subgroup contains H. $\square$

The Next Step 2.79. *We prove assertion* (c) *of Theorem* 2.76.

Proof. Let P and H both be Sylow subgroups of G.

Let H act on the set of left cosets of P in G.

Then

$$|S| = |\{s | \text{orbit of } s \text{ has size } 1\}| + \sum_s |\text{the orbit of } s|,$$

where the sum includes exactly one s from each orbit of size more than one.

Of course S is the set of left cosets of P in G; hence $|S| = [G : P]$ and p does not divide this number. If the orbit of s has more than one element, then

$$|\text{the orbit of } s| = [H : \operatorname{stab} s]$$

and p does divide this number. Thus, p does not divide

$$|\{s | \text{orbit of } s \text{ has size } 1\}|.$$

In particular,

$$|\{s | \text{orbit of } s \text{ has size } 1\}| \neq 0.$$

Hence, there is a left coset xP of P in G with the property that $hxP = xP$ for all $h \in H$. Thus, $x^{-1}hx \in P$ for all h in H for some $x \in G$. Thus, $x^{-1}Hx \subseteq P$. Both sets have the same size. We conclude that $x^{-1}Hx = P$. □

The Next Step 2.80. *We prove assertion* (di) *of Theorem* 2.76.

Proof. **Let G act on the set of Sylow p-subgroups of G by conjugation.** In light of (c) there is only one orbit; thus,

$$\text{the number of Sylow } p\text{-subgroups of } G = [G : \operatorname{stab} P],$$

where P is any fixed Sylow p-subgroups of G. Observe that

$$\operatorname{stab} P = \{x \in G \mid xPx^{-1} = P\} = N(P).$$

Thus,

$$\text{the number of Sylow } p\text{-subgroups of } G = [G : N(P)],$$

and this number divides $[G : P]$ because

$$[G : P] = [G : N(P)][N(P) : P].$$

See HW8. □

The Next Step 2.81. *We prove assertion* (dii) *of Theorem* 2.76.

Proof. Let P be a Sylow p-subgroup of G.

Let P act on the set of Sylow p-subgroups of G by conjugation.

Obtain

$$\text{the number of Sylow } p\text{-subgroups of } G = |\{s | \text{the orbit of } s \text{ has one element}\}| + \sum_s |\text{the orbit of } s|$$

where the sum is taken over the set of orbits of size more than 1 and exactly one s is taken from each such orbit.

If the orbit of s has size more than 1 then the orbit of s has $[P : \operatorname{stab} s]$ elements. This number is divisible by p.

It is clear that P is an element of S with orbit size 1. We complete the proof by showing that P is the only Sylow p-subgroup with orbit size 1.

Suppose that Q has orbit size 1. Then $xQx^{-1} = Q$ for all $x \in P$. Thus, $P \subseteq N(Q)$. The groups P and Q are both Sylow p-subgroups of $N(Q)$. According to (c), P and Q are conjugate in $N(Q)$. On the other hand Q is a normal subgroup of $N(Q)$. So, $P = gQg^{-1} = Q$ for some $g \in N(Q)$. The equality on the left holds because P and Q are conjugate in $N(Q)$; the equality on the right holds because, $Q \lhd N(Q)$. □

2.I.1. *First Application of the Sylow Theorems.*

Observation 2.82. *If G is a group of order pq, where $q < p$ are prime integers and q does not divide $p-1$, then G is cyclic.*

Example. Every group of order 15 is cyclic.

Proof. We show

(1) G has an element a of order p and an element b of order q;
(2) the subgroups $\langle a\rangle$ and $\langle b\rangle$ are normal subgroups of G;
(3) $\langle a\rangle \cap \langle b\rangle = \{\mathrm{id}\}$;
(4) $ab = ba$;
(5) ab has order pq.

(1) This assertion is an immediate application of the Sylow Theorems.

(2) The number of Sylow p-subgroups of G (denoted n_p) is congruent to 1 mod p and divides q. Thus $n_p = 1$. The number of Sylow q-subgroups of G (denoted n_q) is congruent to 1 mod q and divides p. (If $(aq+1)|p$, with a positive, then $aq+1 = p$ and $aq = p-1$, which has been ruled out by hypothesis.) Thus, n_q is also 1. It follows that $\langle a\rangle$ and $\langle b\rangle$ both are normal subgroups of G.

(3) Every non-identity element in $\langle a\rangle \cap \langle b\rangle$ has order p and also has order q. Of course, this makes no sense. Thus, $\langle a\rangle \cap \langle b\rangle = \{\mathrm{id}\}$.

(4) Observe that

$$(aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in \langle a\rangle \cap \langle b\rangle = \{\mathrm{id}\},$$

because $\langle a\rangle$ and $\langle b\rangle$ both are normal subgroups of G. Thus, $ab = ba$.

(5) Apply Lemma 2.30 or just notice that ab does not have order 1, p, or q. □

2.I.2. *Second Application of the Sylow Theorems.* In this section we classify the non-Abelian groups of order 12. (We classify all finite Abelian groups in the next section. There is no need to do another special case of that classification here.) We use Lemma 2.83 in our classification. The easiest way to describe one of the groups of order 12 is by using "semidirect product". This technique is introduced in Observation 2.84. You might find Keith Conrad's notes [3] about this classification to be interesting.

Lemma 2.83. *The only subgroup of S_n of index two is A_n.*

Proof. [29] Let H be a subgroup of S_n of index two. Thus, H is a normal subgroup of S_n and S_n/H is isomorphic to U_2. Let $\phi : S_n \to U_2$ be a surjective homomorphism with kernel H. Observe that all transpositions in S_n are conjugate. Thus, ϕ carries every transposition of S_n to the same value in the Abelian group U_2. The transpositions generate S_n; hence $\phi(\sigma)$ generates U_2 as σ roams over the transpositions of S_n. It follows that $\phi(\sigma) = -1$ for each transposition σ of S_n and the kernel of S_n is necessarily equal to A_n. We have shown $H = \ker \phi = A_n$. □

Recall that if N is a group, then $\mathrm{Aut}(N)$ is the set of group isomorphisms $N \to N$. Recall also that $\mathrm{Aut}(N)$ is a group in its own right with the operation composition. Let N and H be groups and $\phi : H \to \mathrm{Aut}(N)$ be a group homomorphism. We form a new group $N \rtimes_\phi H$, called the semidirect product of N and H. The elements of $N \rtimes_\phi H$ are

$$\{(n,h) \mid n \in N \text{ and } h \in H\}$$

The operation is

$$(n_1,h_1)\cdot(n_2,h_2) = (n_1\phi(h_1)|_{n_2}, h_1h_2).$$

Observation 2.84. *If N and H are groups and $\phi : H \to \mathrm{Aut}(N)$ is a group homomorphism, then $N \rtimes_\phi H$ is a group. The identity element of $N \rtimes_\phi H$ is $(\mathrm{id}_N, \mathrm{id}_H)$. The inverse of (n,h) is $(\phi(h^{-1})|_{n^{-1}}, h^{-1})$. The set $\{(n,\mathrm{id}_H) \mid n \in N\}$ is a normal subgroup of $N \rtimes_\phi H$.*

Proof. **identity element**

$$(n,h)\cdot(\mathrm{id}_N,\mathrm{id}_H) = (n\phi(h)|_{\mathrm{id}_N}, h\,\mathrm{id}_H)$$

Every homomorphism (in particular $\phi(h)$) carries the identity element (in particular id_N in N) to the identity element (in this case id_N in N).

$$= (n,h).$$

$$(\mathrm{id}_N,\mathrm{id}_H)\cdot(n,h) = (\mathrm{id}_N\,\phi(\mathrm{id}_H)|_n, \mathrm{id}_H\,h)$$

Every homomorphism (in this case ϕ) carries the identity element (in this case, id_H in H) to the identity element (in this case, the Automorphism of N which sends each element to itself).

$$= (\mathrm{id}_N\,n, \mathrm{id}_H\,h) = (n,h).$$

inverse

$$(n,h)\cdot(\phi(h^{-1})|_{n^{-1}}, h^{-1}) = (n\underbrace{\phi(h)|_{\phi(h^{-1})|_{n^{-1}}}}_{\left(\underbrace{\phi(h)\circ\phi(h^{-1})}_{\phi(hh^{-1})}\right)\Big|_{n^{-1}}}, hh^{-1}) = (nn^{-1}, hh^{-1}) = (\mathrm{id}_N, \mathrm{id}_H)$$

[29] I found this proof at https://math.stackexchange.com/questions/27024/a-n-is-the-only-subgroup-of-s-n-of-index-2

$$(\phi(h^{-1})|_{n^{-1}}, h^{-1}) \cdot (n,h) = (\underbrace{\phi(h^{-1})|_{n^{-1}}\phi(h^{-1})|_n}_{\phi(h^{-1})|_{n^{-1}n}}, h^{-1}h) = (\phi(h^{-1})|_{\mathrm{id}_N}, \mathrm{id}_H) = (\mathrm{id}_N, \mathrm{id}_H).$$

The assertion that the inverse of the inverse of (n,h) is (n,h) is true and the proof is interesting.

associativity On the one hand,

$$\begin{aligned}&\Big((n_1,h_1)\cdot(n_2,h_2)\Big)\cdot(n_3,h_3)\\ =&\Big(n_1\phi(h_1)|_{n_2}, h_1h_2\Big)\cdot(n_3,h_3)\\ =&\Big(n_1\phi(h_1)|_{n_2}\phi(h_1h_2)|_{n_3}, (h_1h_2)h_3\Big).\end{aligned}$$

On the other hand,

$$\begin{aligned}&(n_1,h_1)\cdot\Big((n_2,h_2)\cdot(n_3,h_3)\Big)\\ =&(n_1,h_1)\cdot\Big((n_2\phi(h_2)|_{n_3}, h_2h_3)\Big)\\ =&(n_1\phi(h_1)|_{(n_2\phi(h_2)|_{n_3}}, h_1(h_2h_3)).\end{aligned}$$

These are equal.

The set $\{(n,\mathrm{id}_H) \mid n\in N\}$ is a normal subgroup of $N\rtimes_\phi H$.

Let (n_1,h_1) be an arbitrary element of $N\rtimes_\phi H$. Observe that

$$\begin{aligned}&(\phi(h_1^{-1})|_{n_1^{-1}}, h_1^{-1})(n,\mathrm{id})(n_1,h_1)\\ =&(\phi(h_1^{-1})|_{n_1^{-1}}\phi(h_1^{-1})|_n, h_1^{-1})(n_1,h_1)\\ =&(\text{an element of } N, h_1^{-1}h_1)\checkmark\end{aligned}$$

□

Example 2.85. If H and N are subgroups of a group G with N a normal subgroup of G and $NH=G$, then define $\phi : H\to \operatorname{Aut} N$ by $\phi(h)$ is the homomorphism $\phi(h) : N\to N$ which sends n to $\phi(h)|_n = hnh^{-1}$. Observe that G is isomorphic to $N\rtimes_\phi H$. The details are left to you.

Example 2.86. If H and N are groups and $\phi : H\to\operatorname{Aut} N$ is the homomorphism $\phi(h)$ is the identity function $N\to N$ for all h in H. Then $N\rtimes_\phi H$ is the direct product $N\times H$.

Example 2.87. Let $\phi : \mathbb{Z}/4\mathbb{Z}\to\operatorname{Aut}(\mathbb{Z}/3\mathbb{Z})$ be the homomorphism with

$$\phi(\bar b)|_{\bar c} = (-1)^b\bar c,$$

for all $\bar b\in\mathbb{Z}/4\mathbb{Z}$ and $\bar c\in\mathbb{Z}/3\mathbb{Z}$. (We say this a little more slowly: ϕ is a homomorphism from $\mathbb{Z}/4\mathbb{Z}$ to $\operatorname{Aut}(\mathbb{Z}/3\mathbb{Z})$. If $\bar b$ is in $\mathbb{Z}/4\mathbb{Z}$, then $\phi(\bar b)$ is an automorphism of $\mathbb{Z}/3\mathbb{Z}$. If $\bar b$ is in $\mathbb{Z}/4\mathbb{Z}$ and $\bar c\in\mathbb{Z}/3\mathbb{Z}$, then $\phi(\bar b)$ sends $\bar c$ to $(-1)^b\bar c$.)[30] The group $(\mathbb{Z}/3\mathbb{Z})\rtimes_\phi(\mathbb{Z}/4\mathbb{Z})$ is called the <u>dicyclic group</u>. Then

(1) the dicyclic group has 12 elements,

[30] If n and a are integers, we write $\bar a$ for the class of a in $\mathbb{Z}/n\mathbb{Z}$.

(2)
- the dicyclic group has 2 elements of order 6,
- the dicyclic group has 6 elements of order 4,
- the dicyclic group has 2 elements of order 3,
- the dicyclic group has 1 element of order 2, and
- the dicyclic group has 1 element of order 1, and

(3) there are elements x, y in the dicyclic group such that the dicyclic group is equal to $\langle x, y\rangle$, $x^6 = \mathrm{id}$, $y^2 = x^3$, $yxy^{-1} = x^5$.

(4) Furthermore, if F is the free group on X, Y, and N is the smallest normal subgroup of F which contains X^6, Y^2X^4, and $YXY^{-1}X$, then F/N is isomorphic to the dicyclic group.

(5) If G is a group with 12 elements $G = \langle \xi, \psi\rangle$, $\xi^6 = \mathrm{id}$, $\psi^2 = \xi^3$, and $\psi\xi\psi^{-1} = \xi^{-1}$, then G is isomorphic to the dicyclic group.

You will establish most of these assertions for homework.

Theorem 2.88. *If G is a non-Abelian group of order 12, then G is isomorphic to exactly one of the following groups:*

$$A_4, \quad D_6, \quad \textit{or} \quad \textit{the dicyclic group}.$$

Proof. No two of the three listed groups are isomorphic:

- A_4 has 3 elements of order 2 and 8 elements of order 3;
- D_6 has 7 elements of order 2, 2 elements of order 3, and 2 elements of order 6;
- and the dicyclic group has 1 element of order 2, 2 elements of order 3, 6 elements of order 4, and 2 elements of order 6.

Observe that G has at least one Sylow 3-subgroup; call it P. Let G act on the set of cosets of P in G by left translation. This action is equivalent to a group homomorphism $\phi : G \to S_4$. Observe that the kernel of ϕ is contained in P. Indeed, if $g \in \ker\phi$, then in particular $gP = P$; hence $g \in P$. There are two choices: either $\ker\phi$ is equal to $\{\mathrm{id}\}$ or $\ker\phi = P$. If $\ker\phi = \{\mathrm{id}\}$, then G is isomorphic to a twelve element subgroup of S_4. Apply Lemma 2.83 to conclude that G is isomorphic to A_4.

Henceforth, $\ker\phi = P$. It follows, in particular, that $P \lhd G$; and therefore, P is the only Sylow 3-subgroup of G. It follows that G has exactly 2 elements of order 3. Let c be one of the elements of G of order 3. Every element of the conjugacy class of c, which is $\{gcg^{-1} | g \in G\}$, has order 3. Thus the conjugacy class of c has one or two elements. Of course, the size of the conjugacy class of c is $[G : \operatorname{stab} c]$. Thus $\operatorname{stab} c$ has either 6 or 12 elements. Recall that $\operatorname{stab} c$ is called the centralizer of c and this group is equal to $\{g \in G | gc = cg\}$. The centralizer of c is a group whose order is divisible 2. Cauchy's Theorem ensures that there is an element d of order 2 which commutes with c. The element $a = cd$ has order 6. (See Lemma 2.30, if necessary.) The subgroup $\langle a\rangle$ of G has index 2; consequently, $\langle a\rangle$ is a normal subgroup of G. Take $b \in G \setminus \langle a\rangle$. It follows that $b^2 \in \langle a\rangle$ and $bab^{-1} \in \langle a\rangle$. But we know much more. The element bab^{-1} must have order 6; so the only choices for bab^{-1} are a and a^5. Furthermore, bab^{-1} can not equal a because the group G is not Abelian. In a similar manner, we observe that b^2 can not equal a or a^5, because in either of these cases $\langle a\rangle$ would be a proper subgroup of $\langle b\rangle$:

$$6 = |\langle a\rangle| < |\langle b\rangle| \le 12.$$

Lagrange's Theorem would force $G = \langle b\rangle$, which is not possible because G is not Abelian. If $b^2 = a^2$, then

$$a^4 = a^5a^5 = (bab^{-1})(bab^{-1}) = ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2;$$

and this contradicts the fact that a has order 6. Similarly, if $b^2 = a^4$, then

$$a^2 = (a^5)^4 = (bab^{-1})^4 = ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4,$$

which is still impossible. Thus, $b^2 = \mathrm{id}$ and G is D_6; or $b^2 = a^3$ and G is the dicyclic group. □

2.I.3. *A list of groups of small order.* Every group of order n is isomorphic to exactly one of the groups in the second column.

order	the groups	explanation
1	$\{\mathrm{id}\}$	
2	$\frac{\mathbb{Z}}{2\mathbb{Z}}$	Use Lagrange's Theorem.
3	$\frac{\mathbb{Z}}{3\mathbb{Z}}$	Use Lagrange's Theorem.
4	$\frac{\mathbb{Z}}{4\mathbb{Z}}, \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$	See Corollary 2.74.
5	$\frac{\mathbb{Z}}{5\mathbb{Z}}$	Use Lagrange's Theorem.
6	$\frac{\mathbb{Z}}{6\mathbb{Z}}, S_3$	See Homework problem 15.
7	$\frac{\mathbb{Z}}{7\mathbb{Z}}$	Use Lagrange's Theorem.
8	$\frac{\mathbb{Z}}{8\mathbb{Z}}, \frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}, \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}, D_4, Q_8$	See Homework problem 20 and Theorem 2.96.
9	$\frac{\mathbb{Z}}{9\mathbb{Z}}, \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$	See Corollary 2.74.
10	$\frac{\mathbb{Z}}{10\mathbb{Z}}, D_5$	See Homework problem 15.
11	$\frac{\mathbb{Z}}{11\mathbb{Z}}$	Use Lagrange's Theorem.
12	$\frac{\mathbb{Z}}{12\mathbb{Z}}, \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}, D_6, A_4$, the dicyclic group	See Theorems 2.88 and 2.96.
13	$\frac{\mathbb{Z}}{13\mathbb{Z}}$	Use Lagrange's Theorem.
14	$\frac{\mathbb{Z}}{14\mathbb{Z}}, D_7$	See Homework problem 15.
15	$\frac{\mathbb{Z}}{15\mathbb{Z}}$	See Observation 2.82
16	There are 14 groups of order 16.	See [11].
17	$\frac{\mathbb{Z}}{17\mathbb{Z}}$	Use Lagrange's Theorem.
18	There are 5 groups of order 18.	See Theorem 2.89
19	$\frac{\mathbb{Z}}{19\mathbb{Z}}$	Use Lagrange's Theorem.

Theorem 2.89. *If G is a group of order 18, then G is isomorphic to exactly one of the groups $\frac{\mathbb{Z}}{18\mathbb{Z}}$, $\frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$, D_9, $S_3 \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$, or $\left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \rtimes_\theta \frac{\mathbb{Z}}{2\mathbb{Z}}$, where $\theta : \frac{\mathbb{Z}}{2\mathbb{Z}} \to \operatorname{Aut}\left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right)$ sends $\bar{1}$ from $\frac{\mathbb{Z}}{2\mathbb{Z}}$ to the automorphism of $\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$ which sends each element to its inverse.*

Proof. Let G be a group of order 18. If G is Abelian, then G is isomorphic to either $\frac{\mathbb{Z}}{18\mathbb{Z}}$ or $\frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$. (Either make a direct proof or appeal to the structure theorem.) Henceforth, assume that G is not Abelian. The Sylow Theorem guarantees that G has a subgroup N of order 9. This subgroup has index 2 in G; so it is a normal subgroup of G. Every group of order p^2 is Abelian, so N is Abelian.

Let Z be the center of G.

Claim 2.89.1. *The order of Z is 3 or 1.*

Proof of Claim 2.89.1. If b is any element of G not in N, then $G = N \cup bN$. If b were in Z, then G would be Abelian. Thus, $b \notin Z$ and $Z \subseteq N$. The group Z can not be all of N; or else, once again, G would be Abelian. It follows that Z is a proper subgroup of N. Claim 2.89.1 is established.

Claim 2.89.2. *If $|Z| = 3$, then $G \cong S_3 \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$.*

Proof of Claim 2.89.2. In this case $\frac{G}{Z}$ is isomorphic to $\frac{\mathbb{Z}}{6\mathbb{Z}}$ or S_3. However, if $\frac{G}{Z}$ were isomorphic to $\frac{\mathbb{Z}}{6\mathbb{Z}}$, then G would be Abelian and this case has been ruled out of consideration. So, $\frac{G}{Z}$ must be isomorphic to S_3. Thus, there exist a and b in G with $a^3 \in Z$, $b^2 \in Z$, $abab \in Z$, and G is generated by a, b, and Z.

Observe that there exist A and B in G so that $A^3 = \mathrm{id}$, $B^2 = \mathrm{id}$, $ABAB = \mathrm{id}$, and G is generated by A, B, and Z. Indeed, if $b^2 = c \in Z$, then take $B = bc$. Observe that $B^2 = bcbc = bbcc = c^3 = \mathrm{id}$. If $(aB)^2 = c' \in Z$, then take $A = c'a$. Observe that $ABAB = c'aBc'aB = c'c'(aB)^2 = c'c'c' = \mathrm{id}$. Observe that A^3 must equal id. Indeed, let us suppose $A^3 = z \in Z$. We already showed that $BAB^{-1} = A^{-1}$; hence,

$$z = BzB^{-1} = BA^3B^{-1} = A^{-3} = z^{-1}.$$

The only element of Z which is its own inverse is id.

Observe that the inclusion maps induce an isomorphism

$$Z \oplus \langle A, B \rangle \to G,$$

and Claim 2.89.2 is established.

Claim 2.89.3. *If $|Z| = 1$ and x is any element of G with $x \notin N$, then $x^2 = \mathrm{id}$.*

Proof of Claim 2.89.3. The group $\frac{G}{N}$ is cyclic of order 2; so, $x^2 \in N$. Thus, x^2 commutes with x and also with every element of N. It follows that $x^2 \in Z = \{\mathrm{id}\}$. The proof of Claim 2.89.3 is complete.

Claim 2.89.4. *If $|Z| = 1$ and N is cyclic, then $G \cong D_9$.*

Proof of Claim 2.89.4. Fix a generator a for N and any element $b \in G \setminus N$. Observe that G is a group of 18 elements generated by a, b with $a^9 = \text{id}$, $b^2 = \text{id}$ (take $x = b$ in Claim 2.89.3) and $(ab)^2 = \text{id}$ (take $x = ab$ in Claim 2.89.3). Thus, G is isomorphic D_9 by Theorem 2.61.1 and the proof of Claim 2.89.4 is complete.

Claim 2.89.5. *If $|Z| = 1$ and $N \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$, then G is isomorphic to $\left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \rtimes_\theta \frac{\mathbb{Z}}{2\mathbb{Z}}$ as described above.*

Proof of Claim 2.89.5. Fix generators a, b for N. Pick $c \in G \setminus N$. Observe that G is generated by a, b, c. Observe also that $a^3 = b^3 = \text{id}$ and $ab = ba$. Apply Claim 2.89.3 three times to see that $c^2 = (ca)^2 = (cb)^2 = \text{id}$. Consider the free group $F = \langle X, Y, Z\rangle$. Let N be the smallest normal subgroup of F which contains $X^3, Y^3, Z^2, (ZX)^2, (ZY)^2, XYX^2Y^2$. It is clear that $\frac{F}{N}$ has at most 18 elements. If $\frac{F}{N}$ has at least 18 elements then there is a surjective homomorphism $\frac{F}{N} \to G$ which sends the class of X to a, the class of Y to b and the class of Z to c and $G \cong \frac{F}{N}$.

We finish the proof by exhibiting a surjection from $\frac{F}{N}$ onto a group with 18 elements that is known to exist. This surjection shows that $|\frac{F}{N}| \geq 18$; and therefore, the calculation of the previous paragraph may be made. Of course, $\left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \rtimes_\theta \frac{\mathbb{Z}}{2\mathbb{Z}}$ is an honest group with 18 elements. Take $a = ((1, 0), 0)$, $b = ((0, 1), 0)$, $c = ((0, 0), 1)$. There is no difficulty observing that $a^3 = b^3 = c^2 = ((0, 0), 0)$;

$$\begin{aligned} ca &= ((0,0),1)((1,0),0) = ((-1,0),1),\\ cb &= ((0,0),1)((0,1),0) = ((0,-1),1),\\ (ca)^2 &= ((-1,0),1)((-1,0),1) = ((0,0),0) = (cb)^2 \end{aligned}$$

and $ab = ba$. The proof of Claim 2.89.5 is complete.

We have shown that if G is a non-Abelian group of order 18, then G is isomorphic to D_9, $S_3 \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$, or $\left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \rtimes_\theta \frac{\mathbb{Z}}{2\mathbb{Z}}$, where $\theta : \frac{\mathbb{Z}}{2\mathbb{Z}} \to \text{Aut}\left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right)$ sends $\bar{1}$ from $\frac{\mathbb{Z}}{2\mathbb{Z}}$ to the automorphism of $\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$ which sends each element to its inverse. It is clear that none of these three groups isomorphic to any other group from the list. The center of $S_3 \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$ has 3 elements; the centers of $S_3 \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$ and $\left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \rtimes_\theta \frac{\mathbb{Z}}{2\mathbb{Z}}$ each have 1 element. The Sylow 3-subgroup of D_9 is cyclic; but the Sylow 3-subgroup of $\left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \rtimes_\theta \frac{\mathbb{Z}}{2\mathbb{Z}}$ is not cyclic. □

2.J. **Finitely generated Abelian groups.** The ultimate theorem (Theorem 2.96) is obtained from Theorem 2.90 by way of multiple uses of the Chinese Remainder Theorem (Example 2.60). Indeed, Theorem 2.90 is the main result; Theorem 2.96 is merely Theorem 2.90 with decorations painted on it.

Recall that the Abelian group G is finitely generated if there exist an integer n and a surjective group homomorphism $\phi : \mathbb{Z}^n \to G$.

Theorem 2.90. *Every finitely generated Abelian group is isomorphic to the direct sum of cyclic groups.*

Theorem 2.90 is a consequence of the following five results.

Lemma 2.91. *Every subgroup of $\mathbb{Z}^n$ is generated by n or fewer generators.*

Corollary 2.92. *If G is a finitely generated Abelian group then there exist non-negative integers m and n and an $n \times m$ matrix of integers M such that*

$$\frac{\mathbb{Z}^n}{\text{the subgroup of } \mathbb{Z}^n \text{ generated by the columns of } M} \cong G. \tag{2.92.1}$$

Remark 2.92.2. The Abelian group on the left side of (2.92.1) is usually called the cokernel of M and denoted $\operatorname{coker} M$.

Lemma 2.93. *If $M_{n\times m}$, $N_{n\times n}$, and $P_{m\times m}$ are matrices of integers with N and P invertible over $\mathbb{Z}$, then* $\operatorname{coker} M \cong \operatorname{coker}(NMP)$.

Lemma 2.94. *If $M_{n\times m}$ is a matrix of integers, then there exist matrices $N_{n\times n}$ and $P_{m\times m}$, which are invertible over $\mathbb{Z}$, such that*

$$NMP = \left[\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right],$$

where D equal to the diagonal matrix

$$D = \begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_r \end{bmatrix},$$

with $d_i \neq 0$.

Lemma 2.95. *If*

$$M' = \left[\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right],$$

with D equal to the diagonal matrix

$$D = \begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_r \end{bmatrix},$$

is an $n \times m$ matrix of integers, then

$$\operatorname{coker} M' = \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}} \oplus \mathbb{Z}^{n-r}.$$

Lemma. 2.91. *Every subgroup of $\mathbb{Z}^n$ is generated by n or fewer generators.*

Remark. This is a special case of the result "every finitely generated module over a Noetherian ring is Noetherian".

Proof. The proof is by induction on n. We already proved that every subgroup of $\mathbb{Z}$ is cyclic; see Proposition 2.24.

Let G be a subgroup of $\mathbb{Z}^n$. Let

$$G_1 = \left\{ r \in \mathbb{Z} \,\middle|\, \exists b \in \mathbb{Z}^{n-1} \text{ with } \begin{bmatrix} r \\ b \end{bmatrix} \in G \right\}$$

and

$$G_2 = \left\{ b \in \mathbb{Z}^{n-1} \,\middle|\, \begin{bmatrix} 0 \\ b \end{bmatrix} \in G \right\}.$$

Observe that G_1 is a subgroup of $\mathbb{Z}$ and G_2 is a subgroup of $\mathbb{Z}^{n-1}$. Thus, G_1 is a cyclic group, and, by induction G_2 can be generated by $n-1$ elements. Let $b_2, \dots, b_n$ be a generating set for G_2 and r_1 be a generator of G_1. There exists $b_1 \in \mathbb{Z}^{n-1}$ with $\begin{bmatrix} r_1 \\ b_1 \end{bmatrix} \in G$. Observe that

$$\begin{bmatrix} r_1 \\ b_1 \end{bmatrix}, \begin{bmatrix} 0 \\ b_2 \end{bmatrix}, \dots, \begin{bmatrix} 0 \\ b_n \end{bmatrix}$$

generates G. □

Corollary. 2.92. *If G is a finitely generated Abelian group, then there exist non-negative integers m and n and an $n \times m$ matrix of integers M such that*

$$\frac{\mathbb{Z}^n}{\textit{the subgroup of } \mathbb{Z}^n \textit{ generated by the columns of } M} \cong G.$$

Proof. The hypothesis that G is a finitely generated Abelian group guarantees that there is a surjective homomorphism

$$\mathbb{Z}^n \xrightarrow{\pi} G.$$

The First Isomorphism Theorem yields that

$$G \cong \frac{\mathbb{Z}^n}{\ker \pi}.$$

Apply Lemma 2.91 to see that $\ker \pi$ is a finitely generated subgroup of $\mathbb{Z}^n$. Take a generating set for $\ker \pi$ and arrange this generating set to be the columns of a matrix. □

Lemma. 2.93. *If $M_{n\times m}$, $N_{n\times n}$, and $P_{m\times m}$ are matrices of integers with N and P invertible over $\mathbb{Z}$, then* $\operatorname{coker} M \cong \operatorname{coker}(NMP)$.

Proof. Consider the following commutative diagram of homomorphisms of Abelian groups

$$\begin{tikzcd}
\mathbb{Z}^m \arrow[r, "M"] \arrow[d, "P^{-1}"', "\cong"] & \mathbb{Z}^n \arrow[r, "q"] \arrow[d, "N", "\cong"'] & \operatorname{coker} M \arrow[r] & 0 \\
\mathbb{Z}^m \arrow[r, "NMP"] & \mathbb{Z}^n \arrow[r, "q'"] & \operatorname{coker}(NMP) \arrow[r] & 0,
\end{tikzcd}$$

where q and q' are the natural quotient maps. The composition $q' \circ N$ is a surjective group homomorphism $\mathbb{Z}^n \to \operatorname{coker}(NMP)$. Apply the First Isomorphism Theorem to see that $q' \circ N$ induces an isomorphism

$$\overline{(q' \circ N)} : \frac{\mathbb{Z}^n}{\ker(q' \circ N)} \longrightarrow \operatorname{coker}(NMP).$$

We show that

$$\ker(q' \circ N) = \operatorname{im} M.$$

Of course, that completes the proof since

$$\frac{\mathbb{Z}^n}{\operatorname{im} M} = \operatorname{coker} M.$$

The inclusion $\operatorname{im} M \subseteq \ker(q' \circ N)$ is obvious because

$$q' \circ N \circ M = q' \circ (NMP) \circ P^{-1}$$

and the kernel of q' is equal to the image of NMP.

Now we prove $\ker(q' \circ N) \subseteq \operatorname{im} M$. Let $x \in \ker(q' \circ N)$. It follows that

$$Nx \in \ker q' = \operatorname{im}(NMP).$$

Thus, there exists an element $y \in \mathbb{Z}^m$ with $Nx = NMPy$. The matrix N is invertible; hence $x = MPy \in \operatorname{im} M$. □

Lemma. 2.94. *If $M_{n\times m}$ is a matrix of integers, then there exist matrices $N_{n\times n}$ and $P_{m\times m}$, which are invertible over $\mathbb{Z}$, such that*

$$NMP = \left[\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right],$$

where D equal to the diagonal matrix

$$D = \begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_r \end{bmatrix},$$

with $d_i \neq 0$.

Proof. We apply a sequence of elementary row and column operations, which are invertible over $\mathbb{Z}$, to M in order to produce a matrix whose only non-zero entries live on the main diagonal. Notice that there are six elementary row and column operations which are invertible over $\mathbb{Z}$, namely:

(1) we may exchange two rows,
(2) we may exchange two columns,
(3) we may add an integer multiple of one row to a different row,
(4) we may add an integer multiple of one column to a different column,
(5) we may multiply any row by -1, and
(6) we may multiply any column by -1.

The proof is by induction. We will apply elementary operations, as described above, until we obtain a matrix with every entry in row one and column one, except possibly the entry in position $(1, 1)$, equal to zero. Then we are finished by induction.

Step A. If every entry in row 1 and column 1 is zero, then we are finished.

Step B. If some entry in row 1 or column 1 is non-zero then we apply elementary operations in order to make the $(1, 1)$ entry be positive.

Step C. If the $(1,1)$ entry divides every entry in row 1 and column 1, then we apply elementary row and column operations and turn all of the entries in row 1 and column 1 other than the (1,1) entry into zero. We are finished.

Step D. The only remaining possibility is that the $(1,1)$ entry $x_{1,1}$ does not divide $x_{1,j}$ for some j (or $x_{i,1}$ for some i). In this case, we use the division algorithm for integers. The integer $x_{1,1}$ is positive; consequently, there exist integers q and r with

$$x_{1,j} = qx_{1,1} + r \quad \text{or} \quad x_{i,1} = qx_{1,1} + r$$

and $1 \le r \le x_{1,1} - 1$. We apply two elementary operations in order to put a smaller positive entry in position $(1,1)$. That is, we replace column j with column j minus q times column 1 and then we exchange column 1 and column j. (Or we replace row i with row i minus q times row 1 and then we exchange row 1 and row j.) Return to Step C.

The process stops after a finite number of iterations. □

Lemma. 2.95. *If*

$$M' = \left[\begin{array}{c|c} D & 0 \\ \hline 0 & 0 \end{array}\right],$$

with D equal to the diagonal matrix

$$D = \begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_r \end{bmatrix},$$

is an $n \times m$ matrix of integers, then

$$\operatorname{coker} M' = \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}} \oplus \mathbb{Z}^{n-r}.$$

Proof. Consider the group homomorphism

$$\phi : \mathbb{Z}^n \to \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}} \oplus \mathbb{Z}^{n-r},$$

which is given by

$$\phi\left(\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}\right) = \left(\bar{a}_1, \dots, \bar{a}_r, \begin{bmatrix} a_{r+1} \\ \vdots \\ a_n \end{bmatrix}\right).$$

Apply the First Isomorphism Theorem:

$$\frac{\mathbb{Z}^n}{\ker \phi} \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}} \oplus \mathbb{Z}^{n-r}.$$

Observe that $\ker \phi$ is generated by

$$\begin{bmatrix} d_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ d_2 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} 0 \\ \vdots \\ 0 \\ d_r \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

(In the vector on the right, d_r appears in row r.) □

Theorem 2.96. *Let G be a finite Abelian group. Then the following statements hold.*

(a) *There exist positive prime integers p_i and positive integers e_i such that*

$$G \cong \bigoplus_i \frac{\mathbb{Z}}{p_i^{e_i}\mathbb{Z}}. \tag{2.96.1}$$

Furthermore, the decomposition of (2.96.1) *is unique in the sense that if q_j are positive prime integers and f_j are positive integers with*

$$G \cong \bigoplus_j \frac{\mathbb{Z}}{q_j^{f_j}\mathbb{Z}},$$

then each decomposition has the same number of factors and, after renumbering, $p_i = q_i$ and $e_i = f_i$, for all i.

(b) *There exist positive integers $\lambda_1, \dots \lambda_r$ such that*

$$G \cong \frac{\mathbb{Z}}{\lambda_1\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{\lambda_r\mathbb{Z}} \quad \text{and} \quad \lambda_1|\lambda_2|\cdots|\lambda_r. \tag{2.96.2}$$

Furthermore, this decomposition is completely unique; if $\mu_1, \dots, \mu_s$ are positive integers with

$$G \cong \frac{\mathbb{Z}}{\mu_1\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{\mu_s\mathbb{Z}} \quad \text{and} \quad \mu_1|\mu_2|\cdots|\mu_s,$$

then $r = s$ and $\lambda_i = \mu_i$ for all i.

Proof.

The existence of decomposition (2.96.1). The decomposition of (2.96.1) is obtained by applying the Chinese Remainder Theorem (Example 2.60) to the decomposition of Theorem 2.90:

$$G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}}.$$

If $d = p_1^{e_1} \cdots p_\ell^{e_\ell}$, where the p_i are distinct positive prime integers and the e_i are prime integers, then

$$\frac{\mathbb{Z}}{d\mathbb{Z}} = \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{p_\ell^{e_\ell}\mathbb{Z}}.$$

The existence of decomposition (2.96.2). Begin with the decomposition of (2.96.1). Arrange the summands of G by using "right justification". That is, identify the positive prime integers $p_1, \dots, p_s$ which contribute a summand to G. For each p_i identify the corresponding exponents

$$0 \le e_{i,1} \le e_{i,2} \le \cdots \le e_{i,r} \tag{2.96.3}$$

Notice that in (2.96.3) all strings of exponents have the same length. We accomplished this but putting zeros in front of each short exponent string. Notice that $\frac{\mathbb{Z}}{p_i^0\mathbb{Z}}$ is the group $\{0\}$. It does no harm to include zero as a direct summand.

$$G = \begin{cases} \frac{\mathbb{Z}}{p_1^{e_{11}}\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p_1^{e_{12}}\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{p_1^{e_{1r}}\mathbb{Z}} \\ \oplus \frac{\mathbb{Z}}{p_2^{e_{21}}\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p_2^{e_{22}}\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{p_2^{e_{2r}}\mathbb{Z}} \\ \vdots \\ \oplus \frac{\mathbb{Z}}{p_s^{e_{s1}}\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p_s^{e_{s2}}\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{p_s^{e_{sr}}\mathbb{Z}} \end{cases}$$

Let $\lambda_j = \prod_i p_i^{e_{ij}}$. (So λ_j is the product of the generator of the denominators that appear in column j.) Apply the Chinese Remainder Theorem to see that

$$G \cong \frac{\mathbb{Z}}{\lambda_1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{\lambda_2\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{\lambda_r\mathbb{Z}}.$$

It is clear from the construction that $\lambda_1|\lambda_2|\dots|\lambda_r$.

Now we show that the p-primary decomposition is unique. This argument consists of a few steps.

Observation 2.97. *Let G_1 and G_2 be finite Abelian groups and n_1 and n_2 be non-negative integers. If*

$$G_1 \oplus \mathbb{Z}^{n_1} \quad \textit{and} \quad G_2 \oplus \mathbb{Z}^{n_2}$$

are isomorphic Abelian groups, then $G_1 \cong G_2$ and $n_1 = n_2$.

Proof. If G is an Abelian then the torsion subgroup of G is

$$\tau(G) = \{g \in G \mid \text{ there exists a positive integer } N \text{ with } Ng = 0\}.$$

Notice that if

$$G_1 \oplus \mathbb{Z}^{n_1} \cong G_2 \oplus \mathbb{Z}^{n_2},$$

then $\tau(\text{LHS}) \cong \tau(\text{RHS})$ (hence $G_1 \cong G_2$) and any isomorphism $\phi : \text{LHS} \to \text{RHS}$ satisfies

$$\phi(\tau(\text{LHS})) = \tau(\text{RHS}).$$

Apply the First Isomorphism Theorem to

$$\phi : \text{LHS} \to \frac{\text{RHS}}{\tau(\text{RHS})}$$

to conclude

$$\frac{\text{LHS}}{\tau(\text{LHS})} \cong \frac{\text{RHS}}{\tau(\text{RHS})};$$

hence,

$$\mathbb{Z}^{n_1} \cong \mathbb{Z}^{n_2};$$
$$\frac{\mathbb{Z}^{n_1}}{2\mathbb{Z}^{n_1}} \cong \frac{\mathbb{Z}^{n_2}}{2\mathbb{Z}^{n_2}};$$

and

$$\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{n_1} \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{n_2}.$$

Count the number of elements to conclude $n_1 = n_2$. □

The uniqueness of decomposition (2.96.1). Suppose the p_i and q_j are distinct positive prime integers, the e_i and f_j are positive integers, and

$$\bigoplus_i \frac{\mathbb{Z}}{p_i^{e_i}\mathbb{Z}} \cong \bigoplus_j \frac{\mathbb{Z}}{q_j^{f_j}\mathbb{Z}}. \tag{2.97.1}$$

We want to prove that both decompositions have the same number of factors and that, after renumbering, $p_i = q_i$ and $e_i = f_i$. Let p be a prime integer. The p-primary subgroup of G is the

$$\{g \in G \mid p^N g = 0 \text{ for some positive integer } N\}.$$

Observe that if p and q are positive prime integers then the p-primary subgroup of

$$\frac{\mathbb{Z}}{q^f\mathbb{Z}} = \begin{cases} 0 & \text{if } p \neq q, \\ \frac{\mathbb{Z}}{q^f\mathbb{Z}} & \text{if } p = q. \end{cases}$$

Indeed, it is clear that $p^N \frac{\mathbb{Z}}{p^f\mathbb{Z}} = 0$ for all $f \leq N$. It is also clear that p^N acts like a unit on $\frac{\mathbb{Z}}{q^f\mathbb{Z}}$ if $p \neq q$ because there exist integers[31] a and b with $ap^N + bq^f = 1$; so ap^N acts like $1 - bq^f$ on $\frac{\mathbb{Z}}{q^f\mathbb{Z}}$ and a acts like the inverse of p^N on $\frac{\mathbb{Z}}{q^f\mathbb{Z}}$.

Consider the p-primary component of (2.97.1) for each positive prime integer p. It suffices to prove that if

$$\frac{\mathbb{Z}}{p^{e_1}\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{p^{e_r}\mathbb{Z}} \cong \frac{\mathbb{Z}}{p^{f_1}\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{p^{f_s}\mathbb{Z}} \tag{2.97.2}$$

with

$$1 \leq e_1 \leq \cdots \leq e_r \quad \text{and} \quad 1 \leq f_1 \leq \cdots \leq f_s,$$

then $r = s$ and $e_i = f_i$ for all i. We use two tricks to finish the argument.

Trick one. If G is an Abelian group and p is an integer, then let

$$\{0\} :_G p = \{g \in G | pg \in \{0\}\}.$$

Observe that

$$|\{0\} :_{\text{LHS}} p| = p^r \quad \text{and} \quad |\{0\} :_{\text{RHS}} p| = p^s$$

because the subgroup of $\frac{\mathbb{Z}}{p^e\mathbb{Z}}$ of elements of order p or less is generated by $\overline{p^{e-1}}$. There are p elements in this subgroup:

$$\overline{p^{e-1}},\ \overline{2p^{e-1}},\ \overline{3p^{e-1}},\ \dots,\ \overline{(p-1)p^{e-1}}.$$

So, $\boxed{r = s}$ and "we continue in this manner to finish the argument".

Trick two. One way to "continue in this manner" is to "throw away" all of the summands of the form $\frac{\mathbb{Z}}{p\mathbb{Z}}$. One very clean way to do this is to look at the subgroup pG of G. Of course,

$$pG = \{\underbrace{g + \cdots + g}_{p} | g \in G\}.$$

[31] Use Lemma 2.60.1, if necessary.

Notice that if $G = \frac{\mathbb{Z}}{p^e\mathbb{Z}}$, then

$$\begin{cases} pG = \{0\} & \text{if } e = 1 \\ pG \cong \frac{\mathbb{Z}}{p^{e-1}\mathbb{Z}} & \text{if } 2 \leq e. \end{cases}$$

The assertion when $e = 1$ is obvious. Use the First Isomorphism Theorem to prove the assertion when $2 \leq e$. Indeed, if $(G, +)$ is any Abelian group, then there is a surjective homomorphism

$$\phi : G \to pG$$

given by $\phi(g) = \underbrace{g + \cdots + g}_{p}$. Observe that $\ker\phi = \{0\} :_G p$. Apply the First Isomorphism Theorem to

$$\phi : \frac{\mathbb{Z}}{p^e\mathbb{Z}} \to p\frac{\mathbb{Z}}{p^e\mathbb{Z}},$$

given by $\phi(g) = pg$, to obtain

$$\frac{\frac{\mathbb{Z}}{p^e\mathbb{Z}}}{\ker\phi} \cong p\frac{\mathbb{Z}}{p^e\mathbb{Z}}.$$

Recall that we already observed that

$$\ker\phi = \{0\} :_G p,$$

and, if $G = \frac{\mathbb{Z}}{p^e\mathbb{Z}}$, then $\{0\} :_G p = p^{e-1}\frac{\mathbb{Z}}{p^e\mathbb{Z}}$. Conclude

$$\frac{\frac{\mathbb{Z}}{p^e\mathbb{Z}}}{p^{e-1}\frac{\mathbb{Z}}{p^e\mathbb{Z}}} \cong p\frac{\mathbb{Z}}{p^e\mathbb{Z}}.$$

Use the second isomorphism theorem to see that the group on the left is

$$\frac{\frac{\mathbb{Z}}{p^e\mathbb{Z}}}{\frac{p^{e-1}\mathbb{Z}}{p^e\mathbb{Z}}} \cong \frac{\mathbb{Z}}{p^{e-1}\mathbb{Z}}.$$

Multiply both sides of (2.97.2) by p and calculate $|\{0\} :_{\square} p|$ to see that

$$|0 :_{p\text{LHS}} p| = |0 :_{p\text{RHS}} p|;$$

hence

$$p^{|\{i|2\leq e_i\}|} = p^{|\{i|2\leq f_i\}|}.$$

Thus,

$$|\{i|2 \leq e_i\}| = |\{i|2 \leq f_i\}|$$

and

$$\boxed{|\{i|1 = e_i\}| = |\{i|1 = f_i\}|}$$

and the proof is completed by induction (or by iteration).

The uniqueness of the decomposition (2.96.1) implies the uniqueness of the decomposition (2.96.2).

$\square$

3. RINGS

3.A. The basics.

Definition 3.1. The set R with two operations $+$ and $\cdot$ is a ring if

(a) $(R, +, 0)$ is an Abelian group,
(b) $r \cdot r' \in R$,
(c) there exists $1 \in R$ with $1 \cdot r = r = r \cdot 1$,
(d) $r \cdot (r' \cdot r'') = (r \cdot r') \cdot r''$,
(e) $r(s + s') = rs + rs'$, and
(f) $(s + s')r = sr + s'r$ for all r, r', r'', s, s' in R.

Examples 3.2.

- The set of integers $\mathbb{Z}$ under addition and multiplication is a ring.
- Every field is a ring.
- If R is a ring, then $R[x]$ (the set of polynomials in one variable with coefficients in R) is a ring.
- If R is a ring, then $R[[x]]$ (the set of formal power series in one variable with coefficients in R) is a ring.
- If $R \subseteq S$ are rings and $s_1, \dots$ are elements of S, then $R[s_1, \dots]$ is the smallest subring of S that contains R and $s_1, \dots$, (For example $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$, and $\mathbb{Q}[\pi]$ are subrings of $\mathbb{C}$.)
- If R is a ring, then $\mathrm{Mat}_{n\times n}(R)$ (the set of $n \times n$ matrices with entries from R) is a ring.
- The set of continuous functions from $[0, 1]$ to $\mathbb{R}$ is a ring.

Words 3.3.

- The ring R is commutative if $rr' = r'r$ for all $r, r' \in R$.
- The ring R is a domain if R is commutative, $1 \neq 0$, and
$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0.$$
- The ring R is a field if R is a commutative ring, $1 \neq 0$, and every non-zero element of R has a multiplicative inverse. (That is, if $r \in R \setminus \{0\}$, then there exists $r' \in R$ with $rr' = 1 = r'r$.)
- A division ring or skew field is a non-commutative ring R with $1 \neq 0$ and every non-zero element has a multiplicative inverse.

November 15, 2023

- characteristic
- module
- Examples of Division Rings
- Group rings
- check that R/I is a legitimate ring when I is a (two-sided) ideal of the ring R
- examples of ideals

Characteristic

Definition 3.4. If R is a ring then there is a ring homomorphism $\phi : \mathbb{Z} \to R$ with $\phi(1) = 1$. The kernel of ϕ is generated by a non-negative integer c. This c is called the characteristic of R.

Examples 3.5. Every ring that contains $\mathbb{Z}$ has characteristic zero. Our undergraduate students like characteristic p because if a and b are elements of a ring of characteristic p, then

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \dots \binom{p}{p-1} ab^{p-1} + b^p = a^p + b^p.$$

So, in particular, the function $\phi : R \to R$, which is given by $\phi(r) = r^p$ is a ring homomorphism.[32]

Modules

Definition 3.6. Let R be a ring and M be an Abelian group. If there is a function $R \times M \to M$, which sends the ordered pair (r, m), with $r \in R$ and $m \in M$, to an element rm in M which satisfies

- $r(m_1 + m_2) = rm_1 + rm_2$,
- $(r_1 + r_2)m = r_1m + r_3m$,
- $(r_1r_2)m = r_1(r_2m)$,
- $1(m) = m$,

then M is a left R-module.

Examples 3.7. Let R be a ring.

- R is a left R-module.
- If M_i is a left R-module for all $i \in I$, then $\bigoplus_{i\in I} M_i$ is a left R-modules. In particular, $\bigoplus_{i\in I} R$ is a left R-module (called a free R-module).
- Every left ideal of R is a left R-module.
- If $N \subseteq M$ are left R-modules then the (well understood) Abelian group M/N is a left R-module, with scalar multiplication r times $m + N$ is equal to $rm + N$. (I guess we better check that this makes sense.)

[32] A ring homomorphism is a function ϕ from the ring R to the ring S for which $\phi(r + r') = \phi(r) + \phi(r')$, $\phi(rr') = \phi(r)\phi(r')$, and $\phi(1) = 1$ for all r and r' in R.

3.B. **Ideals, Quotient rings, and the First Isomorphism Theorem.**

Definition 3.8. Let R be a ring.

- The subset I of R is a left ideal is a subgroup of the Abelian group $(R,+,0)$ which is closed under left multiplication by elements of R.
- The subset I of R is a right ideal is a subgroup of the Abelian group $(R,+,0)$ which is closed under right multiplication by elements of R.
- The subset I of R is a two-sided ideal or ideal if I is both a left ideal and a right ideal of R.

Remark. If R is a commutative ring, then the concepts "left ideal", "right ideal", "two-sided ideal", and "ideal" are identical. Any subset of R which is one of these concepts is all of the concepts.

Examples of Division Rings.[33]

The Quaternions Let K be a subfield of $\mathbb{R}$ and let

$$\mathbb{H} = K \oplus Ki \oplus Kj \oplus Kk.$$

Define multiplication on $\mathbb{H}$ by

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j.$$

Now we see why every non-zero element of $\mathbb{H}$ has an inverse. Observe that

$$(a + bi + cj + dk)(a - bi - cj - dk)$$
$$= \begin{cases} \ (a^2 + b^2 + c^2 + d^2) \\ +(-ab + ab - cd + dc)i \\ +(-ac + bd + ca - db)j \\ +(-ad + bd - cb + da)k. \end{cases}$$

If $x = a + bi + cj + dk$ is not equal to zero then $a^2 + b^2 + c^2 + d^2$ is not zero (because $K \subseteq \mathbb{R}$) and x^{-1} is equal to

$$\frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk).$$

Here are other similar Division rings. Let p be a prime integer which is congruent to 3 mod 4. Consider $H = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$. Define $i^2 = -1,\ j^2 = p,\ ij = -ji = k$. The inverse of $a + bi + cj + dk$ is

$$\frac{1}{a^2 + b^2 - pc^2 - pd^2}(a - bi - cj - dk).$$

Some Number Theory tricks guarantee that $a^2 + b^2 - pc^2 - pd^2 \neq 0$.

Endomorphism rings If M is a simple left module over the ring R, then $\mathrm{End}_R(M)$ is a division ring.

A simple module is a module M with no submodules other than 0 and M.

An R-module Endomorphism of M is an R-module homomorphism from M to M.

If M and N are R-modules, then an R-module homomorphism from M to N is a homomorphism of Abelian groups $\phi : M \to N$ which "respects" scalar multiplication in the sense that $\phi(rm) = r\phi(m)$ for all $r \in R$ and $m \in M$.

Of course, the image of an R-module homomorphism is an R-module. If the target is a simple module, then the homomorphism is either the zero map or is surjective.

Similarly, the kernel of an R-module homomorphism is an R-module. If the domain is a simple module, then the homomorphism is either the zero map or is injective.

It is now clear that every non-zero R-module homomorphism from a simple R-module M to itself is an isomorphism and therefore, $\mathrm{End}_R(M)$ is a division ring.

[33]I found this information at
https://ysharifi.wordpress.com/2022/03/25/examples-of-division-rings/

Example 3.9. If $\mathfrak{m}$ is a maximal left ideal in the ring R, then $R/\mathfrak{m}$ is a simple left R-module and $\mathrm{End}_R(R/\mathfrak{m})$ is a division ring.

In particular, if R is the ring of $n \times n$ matrices with entries from the field $\boldsymbol{k}$ and $\mathfrak{m}$ is the subset of R with every entry in column n equal to zero, then $\mathfrak{m}$ is a maximal left ideal of R. So $\mathrm{End}_R(R/\mathfrak{m})$ is a Division ring.

Total ring of fractions

Example 3.10. Let R be a Noetherian ring with no zero divisors. Let Q be the set

$$\{\tfrac{r}{s} \mid r \in R \text{ and } s \in R \setminus \{0\}\}.$$

Define $+, -, \times, \div$ in the obvious manner. (We will do this procedure slowly when R is commutative.) Then Q is a Division ring. (I skipped over something here. If you really care, check the details carefully.)

November 27, 2023

The Final exam is Friday Dec. 15, 4:00-6:30 in our usual class room.

The Final is comprehensive.

Questions 2, 3, 4 from Exam 2 were old Qual questions.

The question about 72 is hard; but now you have a new tool.

The question about $\frac{HN}{N}$ is easy.

The question about p^6 and p^7 is very standard. It can also be asked about Jordan canonical forms. The point is that to count the number of Abelian groups of order p^n with certain properties or to describe the set of JCF of $n \times n$ matrices with certain properties is equivalent to counting partitions of n with certain properties.

With respect to problem 1, Part (a) is a silly question. We have been thinking about the direct sum of Abelian groups. In an "Abelian category" direct sum is equivalent to has a "splitting map". This explains (c). The "category of groups" is not an "Abelian category". This explains (b).

When we last had class, we were listing examples of Division rings. We had $\mathbb{H}$ (and some twists), $\operatorname{End}_R(M)$ where M is a simple left R-module, and every Noetherian ring without zero divisors is naturally embedded in a smallest Division ring.

I want to give one more example.

Formal Laurent series.

If R is a ring, then the set of formal power series

$$R[[x]] = \{\sum_{i=0}^{\infty} r_i x^i \mid r_i \in R\}.$$

over R is another ring. If r_0 is a unit, then $\sum_{i=0}^{\infty} r_i x^i$ is also a unit. Indeed, the inverse of $1 - xp(x)$ is

$$\sum_{i=0}^{\infty} (xp(x))^i.$$

If R is a division ring, then every element of $R[[x]]$ has the form x^iunit for some i. We do not have to do much to turn $R[[x]]$ into a division ring; we only have to invert x. At any rate, the ring of Formal Laurent series

$$D((x)) = \left\{ \sum_{n \le i} d_i x^i \mid n \in \mathbb{Z} \text{ and } d_i \in D \right\}$$

is a division ring whenever D is a division ring.

Group rings

Definition 3.11. If R is a ring and G is a group, then the group ring $R[G]$ is a free R-module

$$\bigoplus_{g \in G} Rg.$$

The multiplication involving the g's is the multiplication from G.

Remark. The Quaternion ring $\mathbb{H}$ is inspired by the Quaternion group Q_8 but is NOT a group ring. (In fact, I suspect that $\mathbb{H} \cong \frac{K[Q_8]}{(a^2+1)}$, where Q_8 is the eight element group with elements $a^i b^j$, $0 \le i \le 3$,

$0 \le j \le 1$, $a^4 = \mathrm{id}$, $a^2 = b^2$, and $ba = a^3b$. At any rate, $a^2 + 1$ is in the center of $K[Q_8]$; therefore, $a^2 + 1$ generates a two-sided ideal.)

Indeed, if G is a finite group then group rings $K[G]$ tends to have zero divisors. Indeed, if g is an element of G of order n, then

$$(1-g)(1+g+\cdots+g^{n-1}) = 1-g^n = 0.$$

Many rings and modules studied in Commutative Algebra or Algebraic Geometry are symmetric in the variables or are invariant under change of basis. If there are n variables involved then these rings and modules become $K[S_n]$-modules or $K[\mathrm{GL}_n]$-modules. The really nice thing about $K[S_n]$-modules or $K[\mathrm{GL}_n]$-modules is that Maschke's Theorem applies and every finietly generated module over these rings is the direct sum of simple modules. The simple modules over $K[S_n]$ or $K[\mathrm{GL}_n]$ were identified by Young and are described using Young Tableau, which are boxes arranged in a stack, corresponding to a partition of n, and filled in with numbers according to some rules. The numbers are usually strictly ascending in one direction and weakly ascending in the other direction.

We return to the regularly scheduled material (before we started thinking about Division rings). We had just defined left ideals, right ideals, and ideals in a ring.

Examples 3.12.

(a) If R is $\mathbb{Z}$ or $F[x]$, where F is a field, then every ideal is principal.[34] Of course, the zero ideal is principal. If I is a non-zero ideal, then let n be the smallest positive element of $\mathbb{Z}$ in I (or f be a non-zero element of I of least degree). If m is an arbitrary element of I, then $m = qn + r$ for integers q and r with $0 \le r \le n-1$. (If $g \in I$, then $g = qf + r$ for polynomials q and r in $F[x]$, where $\deg r < \deg f$.) The fact that r is in I, in each case, forces r to be zero. Thus, $I = (n)$ or $I = (f)$.

(b) The ideals (x, y) of $F[x, y]$, where F is a field and $(2, x)$ of $\mathbb{Z}[x]$ are not principal.

Proof. We focus on the ideal in $F[x, y]$. One can modify our argument to deal with the ideal in $\mathbb{Z}[x]$. First of all, notice that the units of $F[x, y]$ are the non-zero elements of F. (Recall that the element r in the commutative ring R is a unit if there is an element r' in R with $rr' = 1$.) Indeed, if $1 = (\sum_{i=0}^{a} f_i(x)y^i)(\sum_{j=0}^{b} g_j(x)y^j)$, with f_a and g_b non-zero, then $a = b = 0$, etc.) Observe that x and y are irreducible[35] elements if $F[x, y]$. The argument starts the same way, if

$$x = \left(\sum_{i=0}^{a} f_i(x)y^i\right)\left(\sum_{j=0}^{b} g_j(x)y^j\right),$$

[34]An ideal of the commutative ring R of the form $\{r_0 r \mid r \in R\}$ for any fixed r_0 in R is called principal and is denoted by r_0R or (r_0). Similarly, if T is any set of elements of the ring R, then (T) or $(T)R$ is the smallest ideal of R which contains T.

[35]The non-zero, non-unit element r of the commutative domain R is irreducible if whenever $r = r_1r_2$ with r_1 and r_2 in R, then r_1 or r_2 is a unit in R.

with f_a and g_b non-zero, then $a+b=0$, $x = f_0(x)g_0(x)$. The rest of the calculation takes place in $F[x]$. The constant terms of f_0 and g_0 must multiply to zero and the degrees of f_0 and g_0 must add to one. The rest is easy. etc.

Suppose $(x, y) = (f)$ for some $f \in F[x, y]$. We produce a contradiction. The elements x and y are irreducible in $F[x, y]$ and f divides x. Thus, f is either a unit or a unit times x. A unit times x can not divide y but f divides y; hence, f must be a unit of $F[x, y]$. Even this is impossible because, $(x, y) \subsetneq F[x, y]$. $\square$

(c) Let R be a ring and i be a fixed integer. The set

$$\{M \in \mathrm{Mat}_{n\times n}(R) | \text{ every entry of column } i \text{ of } M \text{ is zero}\}$$

is I is a left ideal of $\mathrm{Mat}_{n\times n}(R)$. The set

$$\{M \in \mathrm{Mat}_{n\times n}(R) | \text{ every entry of row } i \text{ of } M \text{ is zero}\}$$

is a right ideal of $\mathrm{Mat}_{n\times n}(R)$.

(d) The only two-sided ideals of $\mathrm{Mat}_{n\times n}(F)$, where F is a field, are $\{0\}$ and $\mathrm{Mat}_{n\times n}(F)$. (You can see this easily. If M is a non-zero matrix in an ideal I of $\mathrm{Mat}_{n\times n}(F)$, then by multiplying on the left and on the right you can produce a matrix with exactly one non-zero entry and that entry is 1. Then you can produce matrices in I with 1 in position (i, j) and zero everywhere else for all (i, j), for all (i, j). Then you can conclude $I = \mathrm{Mat}_{n\times n}(F)$.

Observation 3.13. *If I is a two-sided ideal of the ring R, then $\frac{R}{I}$ is a ring with multiplication $\bar{r}\bar{s} = \overline{rs}$ for $r, s \in R$.*

Proof. The quotient $\frac{R}{I}$ is automatically an Abelian group. It is necessary to check that the multiplication is well-defined. If r, r_1, s, s_1 are in R with $\bar{r} = \bar{r}_1$ and $\bar{s} = \bar{s}_1$ in $\frac{R}{I}$, then $r_1 = r + i_1$ and $s_1 = s_i + i_2$ for i_1 and i_2 in I. It follows that

$$r_1 s_1 = (r + i_1)(s + i_2) = rs + \underbrace{i_1 s + r i_2 + i_1 i_2}_{\in I};$$

hence, $\overline{r_1 s_1} = \overline{rs}$ in $\frac{R}{I}$. $\square$

Definition 3.14. If R and S are rings, then the function $\phi : R \to S$ is a <u>ring homomorphism</u> if

$$\begin{aligned} \phi(r + r') =& \phi(r) + \phi(r') \\ \phi(1) =& 1 \\ \phi(rr') =& \phi(r)\phi(r'). \end{aligned}$$

Theorem 3.15. [First Isomorphism Theorem] *Let $\phi : R \to S$ be a ring homomorphism. Then the following statements hold.*

(a) *The kernel of ϕ is an ideal of R.*

(b) *If I is an ideal of R with $I \subseteq \ker \phi$, then ϕ induces a ring homomorphism $\bar{\phi} : \frac{R}{I} \to S$ with $\bar{\phi}(\bar{r}) = \phi r$.*

(c) *The induced homomorphism $\bar{\phi} : \frac{R}{\ker \phi} \to \mathrm{im}\, \phi$ is a ring isomorphism.*

Proof. (a) The kernel of ϕ is an Abelian group. We check that $\ker\phi$ is closed under scalar multiplication. If $x \in \ker\phi$ and $r \in R$, then $\phi(rx) = \phi(r)\phi(x) = \phi(r)0 = 0$.

(b) and (c) We verify that $\bar{\phi}$ is a function. If r and r_1 are in R with $\bar{r} = \bar{r}_1$ in $\frac{R}{I}$, then $r - r_1 \in I \subseteq \ker\phi$ and

$$\phi(r) - \phi(r_1) = \phi(r - r_1) = 0.$$

Everything else is automatic. □

Examples 3.16.

(a) The rings $\frac{\mathbb{Z}[x]}{(x^2+1)}$ and $\mathbb{Z}[i]$ are isomorphic.

Proof. Define the ring homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}[i]$ by $\phi(g(x)) = g(i)$. Observe that ϕ is surjective and x^2+1 is in $\ker\phi$. Observe further, that if $f(x)$ is in $\ker\phi$, then $f(x) = q(x^2+1)+r$ where q and r are polynomials in $\mathbb{Z}[x]$ and $r = ax + b$ for some integers a and b.[36] It follows that r is also in $\ker\phi$. The number i is not a rational number; consequently, $ai + b = 0$, with $a, b \in \mathbb{Z}$ only if $a = b = 0$. Thus, $r = 0$ and every element of $\ker\phi$ is in the ideal $(x^2 + 1)$ of $\mathbb{Z}[x]$. Apply the First Isomorphism Theorem to conclude that ϕ induces an isomorphism $\bar{\phi} : \frac{\mathbb{Z}[x]}{(x^2+1)} \to \mathbb{Z}[i]$. □

(b) Let α be a complex number which is algebraic over $\mathbb{Q}$.[37] Let $f(x) \in \mathbb{Q}[x]$ be a non-zero polynomial of least degree with $f(\alpha) = 0$. Define the ring homomorphism

$$\phi : \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$$

by $\phi(g(x)) = g(\alpha)$. Observe that $\ker\phi = (f)$. (Indeed, if $g \in \ker\phi$, then $g = qf + r$ where $q, r \in \mathbb{Q}[x]$ and $\deg r < \deg f$. One sees that $r \in \ker\phi$. The choice of f forces r to be zero.) Conclude that

$$\frac{\mathbb{Q}[x]}{(f)} \cong \mathbb{Q}[\alpha].$$

Definition 3.17. Let R be a commutative ring.

(1) The proper ideal I of R is a maximal ideal if whenever J is an ideal of R with $I \subseteq J \subseteq R$, then $J = I$ or $J = R$.
(2) The proper ideal I of R is a prime ideal if whenever r_1 and r_2 are elements of R, with $r_1 r_2 \in I$, then $r_1 \in I$ or $r_2 \in I$.

Proposition 3.18. *Let I be an ideal of the commutative ring R. Then the following statements hold*:

(a) *I is a prime ideal if and only if R/I is a domain,*
(b) *I is a maximal ideal if and only if R/I is a field, and*
(c) *if I is a maximal ideal, then I is a prime ideal.*

---

[36] We can use the division algorithm at this point because $x^2 + 1$ is a monic polynomial. A monic polynomial is a polynomial whose leading coefficient is 1.

[37] This means that there exists some non-zero polynomial with coefficients from $\mathbb{Q}$ that α satisfies.

Proof. (a) ($\Leftarrow$) Suppose I is a prime ideal of R. Let r_1, r_2 be elements of R with $\bar{r}_1\bar{r}_2 = \bar{0}$ in $\bar{R} = R/I$. Of course, $\bar{r}_1\bar{r}_2 = \bar{0}$ means $r_1r_2 \in I$. The ideal I is prime; so $r_1 \in I$ or $r_2 \in I$; thus, $\bar{r}_1 = \bar{0}$ or $\bar{r}_2 = \bar{0}$ in $\bar{R}$.

(a) ($\Rightarrow$) Suppose $\bar{R} = R/I$ is a domain. Let r_1, r_2 be elements of R with $r_1r_2 \in I$. It follows that $\bar{r}_1$ and $\bar{r}_2$ are elements of $\bar{R}$ with $\overline{r_1r_2}$, which is equal to $\bar{r}_1\bar{r}_2$, equal to $\bar{0}$. But $\bar{R}$ is a domain; so, $\bar{r}_1 = \bar{0}$ or $\bar{r}_2 = \bar{0}$. In other words, $r_1 \in I$ or $r_2 \in I$.

(b) ($\Leftarrow$) Suppose I is a maximal ideal of R. Let r be an element of R with $\bar{r} \neq \bar{0}$ in $\bar{R} = R/I$. In particular $r \notin I$ and (I, r) is an ideal of R which properly contains the maximal ideal I. It follows that $(I, r) = R$ and there exists $r' \in R$ and $i \in I$ with $i + rr' = 1$ and $\bar{r}\overline{r'} = \bar{1}$.

(b) ($\Rightarrow$) Suppose $\bar{R} = R/I$ is a field. Let r be an element of $R \setminus I$. We show that $(I, r) = R$. The fact that $r \notin I$ ensures that $\bar{r}$ is a unit in $\bar{R}$ so there exists r' in R with $\bar{r}\overline{r'} = \bar{1}$ in $\bar{R}$. In other words, $rr' - 1 \in I$. Thus $1 \in (r, I)$.

(c) If I is a maximal ideal, then R/I is a field. Every field is a domain. Thus, R/I is a domain and therefore I is a prime ideal. □

Examples 3.19.

(a) The ideal (0) is a prime ideal of $\mathbb{Z}$ which is not a maximal ideal. Let n be a non-zero integer. Observe that the following statements are equivalent:
   (i) the ideal (n) of $\mathbb{Z}$ is a prime ideal,
   (ii) the integer n is irreducible,[38]
   (iii) the ideal (n) is a maximal ideal.

   Proof.
   (ai) $\Rightarrow$ (aii) We prove that if n is a reducible integer, then (n) is not a prime ideal. Of course, this is clear. If $n = n_1n_2$ with n_1, n_2 non-unit integers, then $n_1n_2 \in (n)$ with neither n_1 nor n_2 in (n); thus (n) is not a prime ideal.

   (aii) $\Rightarrow$ (aiii) Suppose n is an irreducible integer. We prove that (n) is a maximal ideal. Let J be an ideal of $\mathbb{Z}$ with $(n) \subsetneq J$. The ideal J is principal; so $J = (r)$ for some integer r and $r \notin (n)$. On the other hand $n \in (r)$; so $n = rr'$ for some $r' \in \mathbb{Z}$. The integer n is irreducible; hence either r or r' is a unit times n. We have set things up so that r is not a unit times n; thus, r' is a unit times n and r is in fact a unit. At any rate, (n) is a maximal ideal.

   (aiii) $\Rightarrow$ (aii) Apply Proposition 3.18.(c) □

(b) Let $R = F[x]$ be a polynomial ring in one variable over the field F. The ideal (0) is a prime ideal of R which is not a maximal ideal. Let f be a non-zero polynomial in R. Observe that the following statements are equivalent:
   (i) the ideal (f) of $F[x]$ is a prime ideal,

[38] Recall that we proved a little unit about the factorization of integers which starts with Definition 2.32.

(ii) the polynomial f is irreducible,[39]
(iii) the ideal (f) is a maximal ideal.

Proof. Use the same proof as was given in (a). □

(c) Observe that $(0) \subsetneq (2) \subsetneq (2, x)$ is a chain of prime ideals in $\mathbb{Z}[x]$. In this chain, only $(2, x)$ is a maximal ideal.
(d) Observe that

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq (x_1, x_2, x_3, x_4) \subsetneq (x_1, x_2, x_3, x_4, x_5)$$

is a chain of prime ideals in the polynomial $F[x_1, x_2, x_3, x_4, x_5]$ over the field F. The only maximal ideal in this chain is $(x_1, x_2, x_3, x_4, x_5)$.

Corollary 3.20. *If $\alpha \in \mathbb{C}$ and α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}[\alpha]$ is a field.*

Proof. We saw in Example 3.16.b that

$$\mathbb{Q}[\alpha] \cong \frac{\mathbb{Q}[x]}{(f)},$$

where f is a non-zero polynomial of $\mathbb{Q}[x]$ of least degree with $f(\alpha) = 0$. The ring $\mathbb{Q}[\alpha]$ is a subring of $\mathbb{C}$; so $\mathbb{Q}[\alpha]$ is a domain. Thus, (f) is a non-zero prime ideal of $\mathbb{Q}[x]$. Every non-zero prime ideal of $\mathbb{Q}[x]$ is a maximal ideal, by Example 3.19.(b). Thus, (f) is a maximal ideal of $\mathbb{Q}[x]$ and $\mathbb{Q}[x]/(f)$ is a field by Proposition 3.18. □

Corollary 3.21. *Let $\alpha, \beta \in \mathbb{C}$ with α and β algebraic over $\mathbb{Q}$. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. (Thus, $f \in \mathbb{Q}[x]$ is a non-zero polynomial of least degree with $f(\alpha) = 0$.) Suppose $f(\beta) = 0$. Then the rings $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\beta]$ are isomorphic.*

Proof. Apply Example 3.16.(b) to see that $\mathbb{Q}[\alpha] \cong \frac{\mathbb{Q}[x]}{(f)}$. The ring $\mathbb{Q}[\alpha]$ is a domain; so (f) is a prime ideal and f is an irreducible polynomial. Let $g \in Q[x]$ be the minimal polynomial of β. It follows that $(g) = \{h \in \mathbb{Q}[x] \mid h(\beta) = 0\}$. The hypothesis that $f(\beta) = 0$ guarantees that $f \in (g)$ and $f = g'g$ for some $g' \in \mathbb{Q}[x]$. The polynomial f is irreducible and g is not a unit; hence, f is a unit times g and f is also a minimal polynomial of β. Thus, $\mathbb{Q}[\beta] \cong \frac{\mathbb{Q}[x]}{(f)}$ and the proof is complete. □

Observation 3.22. [The second isomorphism Theorem] *If I is an ideal of the ring R, then the following statements hold.*
(a) *Every ideal of $\frac{R}{I}$ has the form $\frac{J}{I} = \{\bar{j} \mid j \in J\}$, where J is an ideal of R with $I \subseteq J$.*
(b) *There exists a one-to-one correspondence between the ideals of R which contain I and the ideals of $\frac{R}{I}$.*

[39] The factorization of polynomials in $F[x]$ works just like the factorization in $\mathbb{Z}$. Re-write the little factorization unit which starts with Definition 2.32 to be about ideals in a Principal Ideal Domain rather than about subgroups of $\mathbb{Z}$. (Of course a Principal Ideal Domain, is a domain in which every ideal is principal.) Recall from Example 3.12.(a) that $F[x]$ is a Principal Ideal Domain.

(c) *If J is an ideal of R which contains I, then*

$$\frac{\frac{R}{I}}{\frac{J}{I}} \cong \frac{R}{J}.$$

Proof. The arguments for (a) and (b) are straightforward. We prove (c). Apply the First Isomorphism Theorem to the natural quotient map

$$\phi : R \to R/J.$$

Observe that $I \subseteq \ker \phi$, so ϕ induces a ring homomorphism $\bar{\phi} : R/I \to R/J$ with $\bar{\phi}(\bar{r}) = \phi(r) = \bar{r}$. Of course, $\bar{r}$ on the left is an element of R/I and $\bar{r}$ on the right is an element of R/J. Apply the First Isomorphism Theorem again to the ring homomorphism $\bar{\phi} : R/I \to R/J$ to see that

$$\frac{R/I}{\ker \bar{\phi}} \cong R/J.$$

There is no difficulty in computing that $\ker \bar{\phi} = J/I$. □

3.C. **The quotient field of a domain.** The basic thought is that every domain sits inside a field. Indeed, every domain sits inside a "smallest field". There is no well-defined ordering on the set of fields which contain a given domain; so we can not just intersect over all of the fields containing the domain. Instead, we use a Universal Mapping Property.

Definition 3.23. Let D be a domain, F be a field, and $i : D \to F$ be an injective ring homomorphism. Then F is the quotient field of D (and $i : D \to F$ is a quotient field map) if $i : D \to F$ satisfies the following Universal Mapping Property: Whenever $\Phi : D \to K$ is an injective ring homomorphism to a field, then there exists a unique ring homomorphism $\phi : F \to K$, so that the following diagram commutes

$$\begin{tikzcd} D \arrow[rr, hook, "i"] \arrow[dr, hook, "\Phi"'] & & F \arrow[dl, dashed, "\exists!\phi"] \\ & K. & \end{tikzcd}$$

Observation 3.24. *Let D be a domain. If D has a quotient field, then this quotient field is unique.*

Proof. Suppose that $i_j : D \to F_j$ both satisfy the UMP for quotient field, for $1 \le j \le 2$.

$$\begin{tikzcd} D \arrow[rr, hook, "i_1"] \arrow[dr, "i_2"] \arrow[dd, hook, "i_1"'] & & F_1 \arrow[dl, dashed, "\exists!\phi_1"] \\ & F_2 \arrow[dl, dashed, "\exists!\phi_2"] & \\ F_1. & & \end{tikzcd}$$

The hypothesis that $i_1 : D \to F_1$ is a quotient field map ensures that there exists a unique ring homomorphism $\phi_1 : F_1 \to F_2$ such that $\phi_1 \circ i_1 = i_2$. Similarly, the hypothesis that $i_2 : D \to F_2$ is a quotient field map ensures that there exists a unique ring homomorphism $\phi_2 : F_2 \to F_1$ such that $\phi_2 \circ i_2 = i_1$. We now have two maps $F_1 \to F_1$ which cause

$$\begin{tikzcd} D \arrow[r, hook, "i_1"] \arrow[d, hook, "i_1"'] & F_1 \arrow[dl, dashed, "\exists!"] \\ F_1 & \end{tikzcd}$$

to commute; namely id_{F_1} and $\phi_2 \circ \phi_1$. We conclude that $\phi_2 \circ \phi_1 = \mathrm{id}_{F_1}$. Thus, ϕ_1 is injective and ϕ_2 is surjective. Reverse the roles of F_1 and F_2 to conclude that ϕ_2 is injective and ϕ_2 is surjective. We conclude that $\phi_1 : F_1 \to F_2$ is an isomorphism and

$$\begin{tikzcd} D \arrow[r, hook, "i_1"] \arrow[d, hook, "i_2"'] & F_1 \arrow[dl, "\phi_1"] \\ F_2 & \end{tikzcd}$$

commutes. $\square$

Example 3.25. If F is a field then the identity map $\mathrm{id} : F \to F$ is a quotient field map.

Proof. If $\Phi : F \to K$ is any injective ring homomorphism into a field, then there does indeed exist a unique ring homomorphism $F \to K$ such that the diagram

$$\begin{tikzcd} F \arrow[r, hook, "\mathrm{id}"] \arrow[d, hook, "\Phi"'] & F \arrow[dl, dashed, "\exists!"] \\ K & \end{tikzcd}$$

commutes; namely Φ. $\square$

Observation 3.26. *The inclusion map $i : \mathbb{Z} \to \mathbb{Q}$ is a quotient field map.*

Proof. Suppose $\mathbb{Z} \xhookrightarrow{\Phi} K$ is an injection into a field. We must prove that there exists a unique ring homomorphism $\phi : \mathbb{Q} \to K$ such that $\phi \circ i = \Phi$.

We first show that there is only one candidate for ϕ. Let b be a non-zero integer. If $\phi : \mathbb{Q} \to K$ is a ring homomorphism with $\phi \circ i = \Phi$, then

$$\phi(\tfrac{a}{b}) = \phi(a)\phi(\tfrac{1}{b}) = (\phi \circ i)(a)\phi(\tfrac{1}{b}) = \Phi(a)\phi(\tfrac{1}{b}).$$

Furthermore,

$$1 = \Phi(1) = \phi(i(1)) = \phi(1) = \phi(\tfrac{b}{b}) = \phi(b)\phi(\tfrac{1}{b}) = (\phi \circ i)(b)\phi(\tfrac{1}{b}) = \Phi(b)\phi(\tfrac{1}{b}).$$

The hypothesis ensures that $\Phi(b) \neq 0$. Thus $\Phi(b)$ has an inverse in K. We conclude that

$$(\Phi(b))^{-1} = \phi(\tfrac{1}{b}) \quad \text{and} \quad \phi(\tfrac{a}{b}) = \Phi(a)(\Phi(b))^{-1}.$$

Now we show that $\phi : \mathbb{Q} \to K$, with $\phi(\frac{a}{b}) = \Phi(a)(\Phi(b))^{-1}$, for $a, b \in \mathbb{Z}$ and $b \neq 0$, is a function.

Suppose a, b, c, d are integers with $b \neq 0$, $d \neq 0$, and $\frac{a}{b} = \frac{c}{d}$ in $\mathbb{Q}$. We show that

$$\Phi(a)(\Phi(b))^{-1} = \Phi(c)(\Phi(d))^{-1}$$

in K. Well,

$$ad = bc$$

in $\mathbb{Q}$ and also in $\mathbb{Z}$; thus

$$\Phi(a)\Phi(d) = \Phi(ad) = \Phi(bc) = \Phi(b)\Phi(c). \tag{3.26.1}$$

The homomorphism Φ is injective and b and d are non-zero integers; hence, $\Phi(b)$ and $\Phi(d)$ are non-zero elements of the field K. In particular, $\Phi(b)$ and $\Phi(d)$ have inverses in K. Multiply both sides of (3.26.1) by $\Phi(b)^{-1}\Phi(d)^{-1}$ and use the hypothesis that multiplication in K commutes to see that

$$\Phi(a)(\Phi(b))^{-1} = \Phi(c)(\Phi(d))^{-1}$$

as desired.

Now we show that the function $\phi : \mathbb{Q} \to K$, with $\phi(\frac{a}{b}) = \Phi(a)(\Phi(b))^{-1}$, for $a, b \in \mathbb{Z}$ and $b \neq 0$, is a ring homomorphism.

If a, b, c, d are integers with b and d not zero, then

$$\phi(\tfrac{a}{b} + \tfrac{c}{d}) = \phi(\tfrac{ad+bc}{cd}) = \Phi(ad + bc)(\Phi(bd))^{-1} = \Phi(a)(\Phi(b))^{-1} + \Phi(c))(\Phi(d))^{-1} = \phi(\tfrac{a}{b}) + \phi(\tfrac{c}{d}),$$

$$\phi(\tfrac{a}{b}\tfrac{c}{d}) = \phi(\tfrac{ac}{bd}) = \Phi(ac)(\Phi(bd))^{-1} = \phi(\tfrac{a}{b})\phi(\tfrac{c}{d}),$$

and

$$\phi(1) = \Phi(1) = 1.$$

Finally, we record the fact that the function $\phi : \mathbb{Q} \to K$, with $\phi(\frac{a}{b}) = \Phi(a)(\Phi(b))^{-1}$, for $a, b \in \mathbb{Z}$ and $b \neq 0$, satisfies $\phi \circ i = \Phi$.

Of course, this is clear. Indeed, if $n \in \mathbb{Z}$, then

$$(\phi \circ i)(n) = \phi(\tfrac{n}{1}) = \Phi(n)(\Phi(1))^{-1} = \Phi(n).$$

$\square$

Proposition 3.27. *If D is a domain, then there exists a field F and a quotient field map $D \overset{i}{\hookrightarrow} F$.*

Proof. Consider the set

$$S = \{(a, b) \mid a, b \in D \text{ with } b \neq 0\}.$$

Consider the relation $\sim$ on S where if (a, b) and (c, d) are in S, then

$$(a, b) \sim (c, d) \iff ad = bc \in D.$$

Observe that $\sim$ is an equivalence relation. Let F be the set of equivalence classes $S/\sim$. In other words, the elements of F all have the form $\overline{(a, b)}$, where (a, b) is an element of S and if (a, b) and (c, d) are elements of S, then $\overline{(a, b)} = \overline{(c, d)}$ in F if and only if $(a, b) \sim (c, d)$. Observe that the following statements hold.

(1) The function $S \times S \to S$, which is given by $(a, b) + (c, d) = (ac + bd, bd)$, induces a well-defined function $F \times F \to F$.
(2) The function $S \times S \to S$, which is given by $(a, b) \cdot (c, d) = (ac, bd)$. induces a well-defined function $F \times F \to F$.

(3) The set F with operations $+$ and $\cdot$, described in (1) and (2), forms a field. The additive identity of F is $\overline{(0,1)}$; the multiplicative identity is $\overline{(1,1)}$.
(4) The function $i : D \to F$, given by $d \mapsto \overline{(d,1)}$, is a ring homomorphism.
(5) The ring homomorphism i of (4) satisfies the Universal Mapping Property of a quotient field homomorphism.

$\square$

Definition. 3.23 Let D be a domain, F be a field, and $i : D \to F$ be an injective ring homomorphism. Then F is the quotient field of D (and $i : D \to F$ is a quotient field map) if $i : D \to F$ satisfies the following Universal Mapping Property: Whenever $\Phi : D \to K$ is an injective ring homomorphism to a field, then there exists a unique ring homomorphism $\phi : F \to K$, so that the following diagram commutes

$$\begin{tikzcd} D \arrow[r, hook, "i"] \arrow[dr, "\Phi"'] & F \arrow[d, dashed, "\exists!\phi"] \\ & K. \end{tikzcd}$$

We proved that if the domain D has a quotient field, then that quotient field is unique. We proved that $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$.

Proposition 3.28. *If D is a domain, then there exists a field F and a quotient field map $D \xhookrightarrow{i} F$.*

Proof. Consider the set
$$S = \{(a,b) \mid a,b \in D \text{ with } b \neq 0\}.$$
Consider the relation $\sim$ on S where if (a,b) and (c,d) are in S, then
$$(a,b) \sim (c,d) \iff ad = bc \in D.$$
Observe that $\sim$ is an equivalence relation. Let F be the set of equivalence classes $S/\sim$. In other words, the elements of F all have the form $\overline{(a,b)}$, where (a,b) is an element of S and if (a,b) and (c,d) are elements of S, then $\overline{(a,b)} = \overline{(c,d)}$ in F if and only if $(a,b) \sim (c,d)$. Observe that the following statements hold.

(1) The function $S \times S \to S$, which is given by $(a,b)+(c,d) = (ac+bd, bd)$, induces a well-defined function $F \times F \to F$.
(2) The function $S \times S \to S$, which is given by $(a,b) \cdot (c,d) = (ac, bd)$. induces a well-defined function $F \times F \to F$.
(3) The set F with operations $+$ and $\cdot$, described in (1) and (2), forms a field. The additive identity of F is $\overline{(0,1)}$; the multiplicative identity is $\overline{(1,1)}$.
(4) The function $i : D \to F$, given by $d \mapsto \overline{(d,1)}$, is a ring homomorphism.
(5) The ring homomorphism i of (4) satisfies the Universal Mapping Property of a quotient field homomorphism.

$\square$

3.D. **Unique Factorization Domains.**

Definition 3.29. The domain D is a Unique Factorization Domain (UFD) if

(a) Every non-zero element of D which is not a unit is a finite product of irreducible elements.
(b) If $d = \prod_{i=1}^{r} p_i$ and $d = \prod_{i=1}^{s} q_i$ are two factorizations of the non-zero non-unit d into irreducible elements, then $r = s$ and after renumbering $p_i = \text{unit}_i q_i$ for all i.

Examples 3.30. (a) Every field is a UFD. (Indeed, every element of a field is zero or a unit.)
(b) Every PID is a UFD. (This is a Theorem. We have essentially proved it. We will tidy it up.) Just in case I neglected to define PID, I include: The domain R is a Principal Ideal Domain (PID) if every ideal of R has the form (r) for some r in R. The standard examples of PIDs are: every field is a PID; the ring of integers is a PID; if F is a field, then the polynomial ring $F[x]$ (in one variable!) is a PID.)
(c) If D is a UFD, then $D[x]$ is a UFD. (This is a Theorem. Essentially, it is due to Gauss.) In particular, if D is a PID (or a field), then $D[x_1, \dots, x_n]$ is a UFD.
(d) If P is a smooth point on an Algebraic variety X, then the ring of rational functions on X which are defined at P (usually denoted $\mathscr{O}_{X,P}$) is a UFD. This theorem is due to Auslander-Buchsbaum-Serre 1959. This Theorem made Algebraic Geometers pay attention to Homological Algebra.
(e) The ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. (This will likely be a homework problem.)
(f) The ring $R = F[x, y, z, w]/(xy - zw)$ is not a UFD, where F is a field. The elements x, y, z, w of R are all irreducible and none is a unit times another. But $xy = zw$ in R. If you care, R is the homogeneous coordinate ring of the image of the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ into $\mathbb{P}^3$. I can unpack that. Projective one space is

$$\frac{\{[x_0 : x_1] \mid (x_0, x_1) \in F^2 \setminus \{(0,0)\}\}}{[x_0 : x_1] \sim [tx_0 : tx_1] \text{ for } t \in F \setminus \{0\}}$$

So, $\mathbb{P}^1$ is ordinary affine one space $\{[1 : x_1]\}$ together with a point at infinity $[0 : 1]$. Projective space is nice because it is compact (in the Zariski topology) and all the points look alike. If you happen to be standing at $[0 : 1]$, then from your point of view $[1 : 0]$ is "infinity". One disadvantage to projective space is that the product of projective spaces is not a projective space. Ah, but one can embed a product of projective spaces in projective space. The Segre embedding of

$$\mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^3$$

is

$$([x_0 : x_1], [y_0 : y_1]) \mapsto [x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1].$$

(Be sure to notice that this function is well-defined.) If the coordinates of $\mathbb{P}^3$ are $[x : z : w : y]$, then the set of polynomials that vanish on the image of the above Segre embedding is the ideal $(xy - zw)$ in the polynomial ring $F[x, y, z, w]$. (One direction of this assertion is obvious. The other direction requires a little work, but not much.) Hence the homogeneous coordinate ring for the image of this Segre embedding is

$$\frac{F[x, y, z, w]}{(xy - zw)}.$$

(g) The ring $\mathbb{Z}[i]$ is a Euclidean Domain; hence a PID; hence a UFD. I will probably make this a homework problem.

History 3.31. Fermat's Last Theorem was conjectured in 1640. It states that $x^n + y^n = z^n$ has no positive integer solutions for $3 \le n$.

In the mid-1800's it was realized that in $\mathbb{Z}[\omega_p]$ every non-zero element which is not a unit can be factored into irreducible elements, where $\omega_p = e^{2\pi i/p}$. (In this discussion, p is a prime integer.) It was assumed that this factorization is unique. A famous false proof of FLT was given under the hypothesis that $\mathbb{Z}[\omega_p]$ is a UFD for all primes p. Dirichlet observed that $\mathbb{Z}[\omega_{23}]$ is not a UFD. Kummer invented "ideal theory". (He considered "idealized integers". These are the objects we call ideals.) The rings $\mathbb{Z}[\omega_p]$ and $\mathbb{Z}[\sqrt{-5}]$ are examples of "rings of algebraic integers" – each element in these rings satisfies a **monic** polynomial with integer coefficients. Every ring of algebraic integers is a Dedekind Domain. Kummer proved that in a Dedekind domain every ideal can be factored into a product of prime ideals in a unique manner. I have probably will assign a homework problem that asks you to exhibit a special case of Kummer's Theorem.

An aside: The fact that the factorization is unique is easy but requires a little more than you know. The argument goes something like this. Suppose $P_1, \dots P_a$ and $Q_1, \dots, Q_b$ are prime ideals in the Dedekind Domain R and

$$\prod P_i = \prod Q_j, \tag{3.31.1}$$

then $a = b$ and, after re-numbering $P_i = Q_i$. The fact that $\prod Q_j \subseteq P_1$ and P_1 is prime forces $Q_j \subseteq P_1$, for some j. (Renumber the Q's to get $Q_1 \subseteq P_1$.) In a Dedekind domain all non-zero primes ideals are maximal ideals. (You probably do not know this.) So $Q_1 = P_1$. The next thing you don't know is that each non-zero ideal I in a Dedekind Domain has an "inverse". This "inverse" is a finitely generated R-submodule I^{-1} of the quotient field K of R with $II^{-1} = R$. (In this context an R-submodule of K is an Abelian group which is a subgroup of $(K, +)$ and is closed under scalar multiplication by R.) Multiply both sides of equation (3.31.1) by P_1^{-1} and repeat or use induction.

Theorem 3.32. *If R is a PID, then R is a UFD.*

We have essentially established this very important Theorem.

Definition 3.33. The ring R is Noetherian if the ideals of R satisfy the Ascending Chain Condition (ACC). The ideals of R satisfy (ACC) if whenever

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

is an ascending chain of ideals of R, then there exists an integer n such that $I_n = I_{n+k}$ for all non-negative integers k.

Remark 3.34. I am thinking of R as a commutative ring; but it could just as well be non-commutative. If R is non-commutative one could say that R is left-Noetherian if the left ideals of R satisfy (ACC) or right-Noetherian if the right ideals of R satisfy (ACC).

Observation 3.35. *If R is a (commutative) ring, then R is Noetherian if and only if every ideal of R is finitely generated.*

Proof. Suppose every ideal of R is finitely generated and

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

is an ascending chain of ideals of R. Then $\cup_i I_i$ is an ideal. This ideal is finitely generated and all of the generators are in I_n for some n. It follows that $I_n = I_{n+k}$ for all non-negative k.

Suppose some ideal I is not finitely generated. Take $i_1 \in I$. Then $(i_1) \subsetneq I$. It follows that there is an element $i_2 \in I \setminus (i_1)$. Thus,

$$(i_1) \subsetneq (i_2) \subsetneq I.$$

Continue in this manner to build an ascending chain of ideals of R which never stabilizes. □

Observation 3.36. *If R is a Noetherian domain, and r is an element of R which is not zero and is not a unit, then r is a finite product of irreducible elements of R.*

Proof. Modify the proof given in Lemmas 2.36 and 2.37. In these results we proved that every integer is a finite product of irreducible integers. The only property about integers that we used is that the subgroups of the group $(\mathbb{Z}, +)$ satisfy the ascending chain condition. Notice that the subgroups of the group $(\mathbb{Z}, +)$ are exactly the same as the ideals of the ring $\mathbb{Z}$. □

Corollary 3.37. *If r is an element of the PID R and r is not zero and not a unit, then r is a finite product of irreducible elements.* □

Proposition 3.38. *If r is an element of the PID R and r is not zero and not a unit, then r is irreducible if and only if (r) is a prime ideal.*

Proof. In fact, the following three statements are equivalent because R is a PID:

(a) r is an irreducible element of R,
(b) (r) is a maximal ideal of R, and
(c) (r) is a prime ideal of R.

To prove this equivalence, modify Example 3.19 as needed. □

Proposition 3.39. *The domain R is a UFD if and only if every non-zero non-unit element of R is a finite product of irreducible elements and every irreducible element of R generates a prime ideal.*

Proof. If necessary, one should look at the proof of Theorem 2.33 on page 24. □

This completes the proof of Theorem 3.32.

I do want to prove the Hilbert Basis Theorem. If R is a Noetherian (commutative) ring, then $R[x]$ is a Noetherian ring. (Hence as a consequence,

$$\frac{R[x_1, \dots, x_n]}{I}$$

is a Noetherian ring for any non-negative integer n and any ideal I of $R[x_1, \dots, x_n]$.) So, you would have to work hard to find a domain R and an element r in R with r not zero, r not a unit, and r not equal to a finite product of irreducible elements. (I will probably ask you to do this as a homework problem.)

Theorem 3.40. [The Hilbert Basis Theorem] *If R is a (commutative) Noetherian ring, then $R[x]$ is also a Noetherian ring.*

Proof. Let J be an ideal of $R[x]$. For each integer n, let

$$I_n = \{r \in R | rx^n + \text{l.o.t.} \in J\}.$$

Observe that

$$I_0 \subseteq I_2 \subseteq \cdots$$

are ideals of R. Every ascending chain of ideals in R stabilizes; hence, there exists n_0 with

$$I_{n_0+k} = I_{n_0}$$

for all non-negative k. For each i with $0 \le i \le n_0$ pick polynomials $f_{i,1}, \dots, f_{i,N_i}$ in $R[x]$ such that each $f_{i,j}$ is in J and has degree i; furthermore the leading coefficients of $f_{i,1}, \dots, f_{i,N_i}$ generate I_i. I claim that

$$\bigcup_{i=0}^{n_0} \{f_{i,1}, \dots, f_{i,N_i}\}$$

generates J. It is clear that

$$\left(\bigcup_{i=0}^{n_0} \{f_{i,1}, \dots, f_{i,N_i}\} \right) \subseteq J.$$

We prove the other inclusion. Let f be an element of J. We prove that

$$f \in \left(\bigcup_{i=0}^{n_0} \{f_{i,1}, \dots, f_{i,N_i}\} \right)$$

by induction on the degree of f. It is clear that if $\deg f = 0$, then $f \in (f_{0,1}, \dots, f_{0,N_0})$. Suppose that $g \in J$ with $\deg g < \deg f$ implies that

$$g \in \left(\bigcup_{i=0}^{n_0} \{f_{i,1}, \dots, f_{i,N_i}\} \right)$$

Observe that f minus a linear combination of elements from

$$\bigcup_{i=0}^{n_0} \{f_{i,1}, \dots, f_{i,N_i}\}$$

is in J and has degree less than the degree of f. (This works for $\deg f \le n_0$ as well as $n_0 < \deg f$.) Hence the proof is complete by induction. □

Theorem 3.41. *If R is a* UFD*, then $R[x]$ is a* UFD.

The idea: The ring $R[x]$ sits between two UFDs:

$$R \subseteq R[x] \subseteq K[x]$$

where K is the quotient field of R. We will prove that the irreducible elements of $R[x]$ are the irreducible elements of R and the elements f of $R[x]$ such that the coefficients of f are relatively prime and f is irreducible in $K[x]$.

Definition 3.42. Let R be a UFD and $f \in R[x]$. If the coefficients of f are relatively prime, then f is called a primitive polynomial

Lemma 3.43. [Gauss' Lemma] *Let R be a* UFD. *If f and g are primitive polynomials in $R[x]$, then fg is primitive.*

Proof. Let $f = \sum_{i=0}^{s} f_i x^i$ and $g = \sum_{j=0}^{t} g_j x^j$, with f_i and g_j in R. Let p be an arbitrary irreducible element of R. Suppose that $p|f_i$ for $i < a$ and p does not divide f_a and $p|g_j$ for $j < b$ and p does not divide g_b. Observe that the coefficient of x^{a+b} in fg is

$$\underbrace{\cdots + f_{a-1}g_{b+1}}_{p|\text{ this}} + \underbrace{f_a g_b}_{p \text{ does not divide this}} + \underbrace{f_{a+1}g_{b-1} + \dots}_{p|\text{ this}}.$$

Thus, p does not divide the coefficient of x^{a+b} in fg. We conclude that fg is primitive. □

Corollary 3.44. *Let R be a UFD and f be a primitive polynomial in $R[x]$. Let K be the quotient field of R.*

(a) *Let $f = \prod_{i=1}^{s} g_i$ in $K[x]$ with $g_i = \frac{a_i}{b_i} h_i$ for a_i, b_i in R and h_i a primitive polynomial of $R[x]$. Then f is equal to $\prod_{i=1}^{s} h_i$ times a unit of R.*

(b) *The polynomial f is irreducible in $R[x]$ if and only if f is irreducible in $K[x]$.*

Proof. (a) Observe that $(\prod b_i)f = (\prod a_i)(\prod h_i)$. The polynomials f and $\prod h_i$ are both primitive in $R[x]$. (Use Gauss' Lemma for $\prod h_i$.) Hence $\prod a_i$ is equal to a unit of R times $\prod b_i$ in R.

(b) Suppose f is irreducible in $R[x]$ and $f = g_1 g_2$ in $K[x]$. Write $g_i = \frac{a_i}{b_i} h_i$ with a_i, b_i in R and h_i primitive in $R[x]$. Apply (a) to conclude that f is equal to $h_1 h_2$ times a unit of R in $R[x]$. The polynomial f is irreducible in $R[x]$; so h_1 or h_2 is a unit of $R[x]$; hence a unit of R. Thus, either g_1 or g_2 is a unit in $K[x]$ and f is irreducible in $R[x]$.

Suppose f is irreducible in $K[x]$. Suppose $f = g_1 g_2$ in $R[x]$. The hypothesis that f is irreducible in $K[x]$ ensures that either g_1 or g_2 is a unit of $K[x]$; hence, an element of K. But f is primitive in $R[x]$. Thus, g_1 or g_2 is a unit in R. We conclude that f is irreducible in $R[x]$. □

The proof of Theorem 3.41. Take $f \in R[x]$. Use Corollary 3.44.(a) to write $f = \prod r_i \prod f_j$ where the r_i are irreducible in R and the f_j are primitive in $R[x]$ and irreducible in $K[x]$. We have exhibited a factorization of f into irreducible elements of $R[x]$.

Suppose

$$\prod r_i \prod f_j = \prod s_k \prod g_\ell \tag{3.44.1}$$

with r_i and s_k irreducible in R and f_j and g_ℓ primitive in $R[x]$ and irreducible in $K[x]$. First look in $K[x]$ to see that there are exactly as many f_j's as there are g_ℓ's and after renumbering f_j is equal to a unit of K times g_j. The unit of K is a/b for a, b in R with b not zero. Multiply both sides by b: $bf_j = ag_j$. The polynomials f_j and g_j are primitive in $R[x]$; hence, b is equal to a unit of R times a. At any rate, we can cancel all of the f_j's and g_ℓ's from (3.44.1) at the expense of multiplying one of the sides by a unit of R. We are left with $\prod r_i$ is equal to a unit of R times $\prod s_k$, where the r_i and the s_k are irreducible elements of R. The hypothesis that R is a UFD ensures that the number of r_i is equal to the number of s_k and after re-numbering r_i is equal to a unit of R times s_i. $\square$

CONTENTS

REFERENCES

[1] Aluffi, Paolo, *Algebra: Chapter 0*, American Mathematical Society, Graduate Studies in Mathematics Volume 104 (2009) (Reprinted with corrections, 2016.) ISBN-10: 0-8218-4781-3 ISBN-13: 978-0-8218-4781-7.

[2] Artin, Michael, *Algebra*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991. ISBN: 0-13-004763-5.

[3] `https://kconrad.math.uconn.edu/blurbs/grouptheory/group12.pdf`

[4] Dummit, David S. and Foote, Richard M. *Abstract algebra. Third edition.* John Wiley & Sons, Inc., Hoboken, NJ, 2004. ISBN: 0-471-43334-9.

[5] Hungerford, Thomas W., *Algebra*, Reprint of the 1974 original. Graduate Texts in Mathematics, **73**. Springer-Verlag, New York-Berlin, 1980. ISBN: 0-387-90518-9.

[6] Jacobson, Nathan, *Basic algebra. I*, Second edition. W. H. Freeman and Company, New York, 1985. ISBN: 0-7167-1480-9

[7] O'Connor, J. and Robertson, E., *The development of Ring Theory*,
`https://www-history.mcs.st-andrews.ac.uk/HistTopics/Ring_theory.html`

[8] Rotman, Joseph J., *Advanced modern algebra. Part 1.* Third edition. Graduate Studies in Mathematics, **165**. American Mathematical Society, Providence, RI, 2015. ISBN: 978-1-4704-1554-9.
[9] `https://en.wikipedia.org/wiki/History_of_group_theory`
[10] `https://en.wikipedia.org/wiki/Field_(mathematics)`
[11] M. Wild, *The groups of order sixteen made easy* Amer. Math. Monthly **112** (2005), 20–31.