MATH 120 NOTES

ARUN DEBRAY

DECEMBER 8, 2012

These notes were taken in Stanford's Math 120 class in Fall 2012, taught by Professor Soren Galatius. I TEXed them up using `vim`, and as such there may be typos; please send questions, comments, complaints, and corrections to `adebray@stanford.edu`.

Contents

1. Overview of Groups: 9/24/12

This class will spend most of its time on groups, and the rest on rings.

Informally, a ring (something like $\mathbb{Z}$ or $\mathbb{R}$) has a sense of addition or multiplication that satisfies certain axioms. Elements of a ring are in some sense a generalization of numbers. Thus, rings show up in number theory (one question we will address is which integers n can be written as $n = a^2 + b^2$, $a, b \in \mathbb{Z}$. It turns out that for primes p, this is true iff $p = 4n + 1$ for some $n \in \mathbb{N}$.)

Groups, by contrast, are symmetries of things.

Example 1.1.

$$\mathrm{SO}(3) = \left\{ A \in M_3(\mathbb{R}) \;\middle|\; \begin{array}{l} \det A = 1 \\ A^\mathsf{T} A = I \end{array} \right\},$$

i.e. a subset of the set of 3×3 matrices. This group is the group of rotations of $\mathbb{R}^3$ (all of them, except for the identity, define some axis to rotate around). It is also called the group of symmetries of $\mathbb{R}^3$.

Example 1.2. Consider the unit cube $C = \{(x, y, z) \in \mathbb{R}^3 \mid x, y, z \in [-1, 1]\}$. The group consists of 90°-rotations that send the cube to the cube: $G = \{A \in \mathrm{SO}(3) \mid A\mathbf{v} = C \text{ for all } \mathbf{v} \in C\}$. Alternatively, one could also consider reflections, which would give another example.

Definition. A function $f : X \to Y$ is:

- injective if $a \neq b$ implies $f(a) \neq f(b)$,
- surjective if every $y \in Y$ has an $x \in X$ for which $f(x) = y$, and
- bijective if it is both injective and surjective.

Example 1.3. Let Ω be any set, and consider the group S_Ω be the set of bijections $\Omega \to \Omega$.

All of these groups have some composition-like operation that is associative, has some identity that does nothing, and has an inverse for every element. But the idea of abstract algebra is to consider these as axioms to start from, rather than promises that are satisfied.

Definition. A binary operation on a set G is a function $G \times G \to G$.[1]

Definition. A group is a pair $(G, *)$ where G is a set and $*$ is a binary operation that satisfies the following axioms:

i. $*$ is associative: if $a, b, c \in G$, then $a * (b * c) = (a * b) * c$.
ii. G has an identity element e such that for all $g \in G$, $g * e = e * g = g$.
iii. Every $g \in G$ has an inverse g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Sometimes the terminology "G is a group" is used, even though a group is technically a pair of a set and a binary operation. If the binary operation is known from context, then this is fine.

SO(3) is a group under matrix multiplication, and S_Ω under function composition (i.e. composition is the group operation $*$).

Definition. In the special case where $\Omega = \{1, \dots, n\}$, then S_Ω is written S_n and is called the symmetric group of order n.

Definition. A group G is abelian if it is commutative: for all $a, b \in G$, $a * b = b * a$.

Note that not all groups are abelian, and in fact none of the above examples are. The groups $(\mathbb{Z}, +)$ and $(\mathbb{R}, +)$, the integers and reals under addition, respectively, are abelian.

The pairs $(\mathbb{R}, \cdot)$ and $(\mathbb{R}, /)$ are not groups; the former lacks an inverse for 0, and in the latter / is not a binary operation, since $a/0$ is undefined.

Here are some immediate consequences of the group axioms:

1. The identity is unique: if e and e' are both identities (i.e. they both satisfy axiom ii), then $e * e' = e$, but $e * e' = e'$, so $e = e'$.

   This is sort of implicit in axion iii, since the definition of an inverse wouldn't quite work if identities weren't unique.
2. Inverses are also unique. By axiom iii, if g and g' are both inverses of f, then $(g * f) * g' = g * (f * g')$, so $e * g' = g * e$, so $g' = g$ by the uniqueness of the identity.

Another notational shortcut is to write the group operation as ab instead of $a * b$. Obviously, this won't be done if ab means something else (as in the group $(\mathbb{Z}, +)$). Additionally, due to associativity, any parentheses written in multiple applications of the group operation don't change the final value and tend to be omitted.

Another notational shortcut is to write $a^n = a * a * \cdots * a$ (where n copies of a are multiplied together). This can be extended to $a^0 = e$ and $a^{-n} = (a^{-1})^n$. Again, this is not done when it would cause a clash in notation.

Definition. The order of an element $a \in G$, denoted $|a|$, is the smallest $n \in \mathbb{N}$ such that $a^n = e$, and is infinite if no such n exists.

For example, in the group of symmetries of a square, a rotation by 90° has order 4.

The word order has another meaning: the order of a finite group is the number of elements it has. For example, the order of S_n, written $|S_n|$, is $n!$

[1] $A \times B = \{(a, b) : a \in A, b \in B\}$.

Definition. The dihedral group of order $2n$, written D_{2n},[2] is the set of symmetries of the regular n-gon in the plane. The n-gon's vertices can be defined in the complex plane as $\{e^{\frac{2\pi ik}{n}}, k \in \mathbb{Z}\}$ and are numbered 1 to n, so that $D_{2n} = \{f \in S_n :$ if $i, j \in \{1, \dots, n\}$ are adjacent, then so are $f(i)$ and $f(j)$.$\}$ (Here adjacent means 1 and 2, 7 and 6, etc., or 1 and n.)

Thus, any symmetry can be completely specified by describing where vertex 1 goes to, and then by adjacency there are only 2 places to put vertex 2 (and then the rest of the vertices are determined by adjacency). Thus, D_{2n} is finite and has $2n$ elements.

2. Meeting D_{2n} and S_n: 9/26/12

The dihedral group has 2 special elements: r is the clockwise rotation by $\frac{2\pi}{n}$, and s is the reflection about the real axis. Every other element of D_{2n} is a composition of these two transformations: each rotation is of the form $1, r, r^2, \dots, r^{n-1}$ (since $r^n = 1$ is a complete rotation back to the starting point), and the reflections are $sr, sr^2, \dots, sr^{n-1}$.

By counting, these are $2n$ distinct elements, and since $|D_{2n}| = 2n$, then these are all of its elements. Thus, $D_{2n} = \{r, r^2, \dots, r^{n-1}, sr, sr^2, \dots, sr^{n-1}\}$.

Notice that $rs \neq sr$; in fact, $rs = sr^{-1}$, and $srs = r^{-1} = r^{n-1}$. We also have $s^2 = r^n = 1$, and these rules completely describe D_{2n}, allowing the calculation of orders: $|r| = n$, $|s| = 2$, and $|r^2|$ is $n/2$ if n is even and n otherwise.

Similarly, it will be helpful to introduce some notation for S_n. There are three ways to specify an element of S_n. The first is to write the rule of the function explicitly, such as a $\sigma \in S_4$ given by $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 3$, and $\sigma(4) = 1$. This is sometimes nice, but is not economical for large n.

It is also possible to make a table of i and $\sigma(i)$, or draw arrows across said table. This is intiutive, but also cumbersome for large n.

Thus, cycle notation is a common solution.

Definition. A cycle $c \in S_n$, written $(a_1\ a_2\ \dots\ a_m)$ for $a_1, \dots, a_m \in \{1, \dots, n\}$, is the permutation that sends $a_j \xrightarrow{c} a_{j+1}$ when $j \leq m - 1$ and $a_m \xrightarrow{c} a_1$. If $x \notin \{a_1, \dots, a_m\}$, then $c(x) = x$.

A cycle is just a permutation obtained by pushing some subset of $\{1, \dots, n\}$ in a circle.

Definition. Two (or more) cycles are disjoint if they have no elements in common.

Disjoint cycles commute: if $\sigma, \tau \in S_n$ are disjoint, then $\sigma\tau = \tau\sigma$. This is because at most one of the disjoint cycles moves any given element, so the order they do it in is irrelevant.[3] However, cycles in general do not commute: $(1\ 2)(1\ 2\ 3) = (2\ 3)$, but $(1\ 2\ 3)(1\ 2) = (1\ 3)$.[4]

Not every permutation is a cycle: consider $\tau \in S_4$ such that $\tau(1) = 2$, $\tau(2) = 1$, $\tau(3) = 4$, and $\tau(4) = 3$. Then, $\tau = (1\ 2)(3\ 4)$.

Theorem 2.1 (The Cycle Decomposition Algorithm)**.** *Every element of S_n can be written as a product of disjoint cycles.*

This decomposition is in fact unique up to rearrangement, a fact which will be proven later.

Definition. The support of a permutation σ is $\mathrm{Supp}(\sigma) = \{i \mid \sigma(i) \neq i\} \subset \{1, \dots, n\}$. Thus, it is the set of elements that a permutation changes.

Proof of 2.1. Proof by induction on $|\mathrm{Supp}(\sigma)|$. First, suppose $|\mathrm{Supp}(\sigma)| = 0$. Then, $\sigma = 1$, which is the product of 0 distinct cycles, which satisfies the hypothesis.

In general, pick $i \in \mathrm{Supp}(\sigma)$ and consider the infinite sequence $i, \sigma(i), \sigma^2(i), \dots$ By the Pidgeonhole Principle, this sequence must repeat since S_n is finite, so pick the minimal s such that $\sigma^s(i) = i$ and let $c = (i\ \sigma(i) \dots \sigma^{s-1}(i)) \in S_n$. Then, c is a cycle for which $c(j) = \sigma(j)$ for $j \in \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{s-1}(i)\}$.

Consider $(\sigma c^{-1}) \in S_n$, for which $(\sigma c^{-1})(j) = j$ if $j \in \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{s-1}(i)\}$ and $(\sigma c^{-1})(j) = \sigma(j)$ otherwise.

Thus, $\mathrm{Supp}(\sigma c^{-1}) < \mathrm{Supp}(c)$, so taking the inductive leap, $\sigma c^{-1} = c_1 \dots c_j$ for disjoint cycles $c_1, \dots, c_j$. Thus c is also disjoint to the c_i, so $\sigma = c_1 \dots c_j c$ is a product of disjoint cycles. □

In order to calculate the composition of permutations, one can use this cycle decomposition: in order to calculate $\sigma\tau$, first calculate $\sigma\tau(1)$, then $\sigma\tau(\sigma\tau(1))$, and so on, in order to obtain a cycle. Then, repeat with the first remaining element, and so on, until all are accounted for. For example, in S_5, $(1\ 4\ 5)(2\ 1\ 3\ 4) = (1\ 3\ 5)(2\ 4)$.

[2] …sometimes. The notation D_n is sometimes seen to mean D_{2n}, so take care to check which group is actually being referred to.

[3] Of course, there is a straightforward way to formalize this proof.

[4] When multiplying cycles, start with the rightmost element, because permutations are functions and the operation is function composition, which is evaluated right to left.

Definition. A field is a set F with two binary operations $+$, $\cdot$, such that:

- $(F, +)$ and $(F \setminus \{0\}, \cdot)$ are abelian groups, and
- the distributive law holds: $a(b + c) = ab + ac$ for all $a, b, c \in F$.

Some more examples of groups which will be useful later:

Informally, $\mathbb{Z}/n\mathbb{Z}$ is the set of integers mod n, with group operation addition mod n. This is an abelian group.[5]

Definition. The quarternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}$.

This is a nonabelian group of order 8: $(\pm 1)a = a(\pm 1) = \pm a$ and $(\pm 1)^2 = (\pm i)^2 = (\pm j)^2 = (\pm k)^2 = 1$, but $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$.

Definition. If F is a field, then the general linear group of order n over F is $\mathrm{G}\ell_n(F) = \{A \in M_n(F) \mid \det A \neq 0\}$. These are the $n \times n$ matrices with elements in F and nonzero determinants, with group operation matrix multiplication.[6]

For example, $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Q}$ are fields, so $\mathrm{G}\ell_n(\mathbb{C})$, $\mathrm{G}\ell_n(\mathbb{R})$, and $\mathrm{G}\ell_n(\mathbb{Q})$ are all matrix groups. It is also possible to define these groups over finite fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ when p is prime, where addition and multiplication are mod p.

3. Homomorphisms and Isomorphisms: 9/28/12

Much of this discussion will be familiar to someone with experience in linear algebra, for whom one could set up an analogy of groups to vector spaces, subgroups to linear subspaces, group homomorphisms to linear maps, etc.

Definition. If G and H are groups, then a function $f : G \to H$ is a homomorphism if for all $x, y \in G$, $f(xy) = f(x)f(y)$.

This just means that multiplication preserves the group operation.

Example 3.1. Some examples of homomorphisms:

1. $\mathbb{Z} \xrightarrow{f} \mathbb{Z}$ given by $f(x) = 2x$.
2. $(\mathbb{C}, +) \xrightarrow{f} (\mathbb{C} \setminus \{0\}, \cdot)$ given by $f(z) = e^z$.
3. $G \xrightarrow{f} H$ where $f(x) = 1$ for any $x \in G$ (which is trivially a homomorphism).

The last example illustrates that homomorphisms don't mean groups are related, since one can be established between any given groups. But some more meaningful hommormorphisms are important:

Definition. An isomorphism is a homomorphism that is also a bijection.

Example 3.2. $(\mathbb{R}, +) \xrightarrow{f} (\mathbb{R}^+, \cdot)$, where $f(x) = e^x$. Because f has a nice inverse, this is a bijection.

Notice that the homomorphisms in Example 3.1 are not isomorphisms (unless $G = H = \{0\}$ for the trivial example).

Definition. Two groups G and H are isomorphic, written $G \cong H$, if there is some isomorphism $G \to H$.

Informally, isomorphic groups have the same properties related to group structure: propositions based on group structure are also isomorphic in some sense.[7] For example, if $G \cong H$ and G has an element of order n, then H does. An example of a more formal proof of such a property:

Claim. If $G \cong H$ and G is abelian, then H is also abelian.

Proof. Call the isomorphism $f : G \to H$. For any $a, b \in G$, $ab = ba$, so $f(a)f(b) = f(b)f(a)$ because f is a homomorphism. Then, since f is surjective, every element of H is $f(a)$ for some $a \in G$, so for all $c, d \in H$, $cd = dc$. Thus H is abelian. □

Related to isomorphisms is the classification problem: how does one determine if two groups are isomorphic? This leads to a goal of classifying groups up to isomorphism.

In the language of vector spaces, any two finite-dimensional vector spaces over the same field are isomorphic if they have the same dimension. But for groups, the general case is very difficult.

Theorem 3.1. *If $|G| = p$ for some prime p, then $G \cong \mathbb{Z}/n\mathbb{Z}$.*

This has a fairly straightforward proof that will be seen next week. The following is harder:

[5] Technically, $\mathbb{Z}/n\mathbb{Z}$ is constructed from equivalence classes of integers, defining $\bar{s} \in \mathbb{Z}/n\mathbb{Z}$ to be $\bar{s} = \{s + kn \mid k \in \mathbb{Z}\}$.

[6] $\mathrm{G}\ell_n(F)$ can be thought of as the support of the function $\det : M_n(F) \to F$, using the more common definition of support as the subset of the domain that does not map to zero. Thus, is it correct to say that $\mathrm{G}\ell_n(F)$ is a support group?

[7] Thinking once again of vector spaces, isomorphic vector spaces have the same dimension.

Theorem 3.2. *If $|G| = 6$, then $G \cong \mathbb{Z}/6\mathbb{Z}$ (if G is abelian) or $G \cong D_6$ (if it isn't).*

Some of these can be accomplished by brute-force checking: it is not terribly difficult, for example, to prove that all groups of order 2 are isomorphic to $\mathbb{Z}/2\mathbb{Z}$ simply because there aren't very many possibilities.

Definition. A subgroup of a group G is a nonempty subset $H \subseteq G$ closed under multiplication and taking inverses. In this case, one writes $H \leq G$; if $H \subsetneq G$, then $H < G$.

Thus, a subgroup is a group under the same group operation, since $1 \in H$ and associativity is already known.

Example 3.3. Some examples of isomorphisms:

(1) $\mathbb{Z} \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.
(2) $\{1, r, \ldots, r^{n-1}\} \leq D_{2n}$.
(3) $(\mathbb{R}^+, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot)$.

Definition. If G is a group and $x \in G$, then the group $\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ is called the subgroup generated by x.

This is an abelian group, since $x^m x^n = x^{m+n} = x^{n+m} = x^n x^m$, and the inverse of x^n is x^{-n}. Thus, any subgroup of G containing x must contain all of its powers in order to be closed, so $\langle x \rangle$ is the smallest subgroup of G that contains x.

For example, in D_{2n}, $\langle r \rangle = \{1, r, \ldots, r^{n-1}\}$.

Definition. A group G is cyclic if it is generated by some element x: $\langle x \rangle = G$.

For example, $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$, but D_{2n} is not cyclic (unless $n = 1$). In fact, every cyclic group is abelian (because powers of x commute, as above).

Theorem 3.3 (Classification of Cyclic Groups)**.** *If G and H are cyclic, then $|G| = |H|$ iff $G \cong H$.*

This theorem, the proof of which will be given in Section 4, is an extremely nice result — so nice as to be extremely rare.

Proposition 3.4. *If G is a group and $x \in G$, then $|x| = |\langle x \rangle|$.*

Proof. Case 1. Suppose $|x|$ is finite.

Clearly, $\{x^n, n \in \mathbb{Z}\} \supseteq \{1, x, \ldots, x^{|x|-1}\}$, since $\{0, 1, \ldots, |x| - 1\} \subset \mathbb{Z}$.

Additionally, if $x^n \in \langle x \rangle$, then $n = q|x| + r$ (division with remainder) for $q, r \in \mathbb{Z}$ and $0 \leq r < |x|$. Th, $x^n = x^{q|x|+r} = x^{q|x|}x^r = 1 \cdot x^r = x^r$, so $x^n \in \{1, x, \ldots, x^{|x|-1}\}$, since these are all the possible r.

Since all of $1, x, \ldots, x^{|x|-1}$ are distinct (see Exercise 3.1), then $\{x^n, n \in \mathbb{Z}\} \subseteq \{1, x, \ldots, x^{|x|-1}\}$, so the sets are equal, and $|x| = |\langle x \rangle|$. □

Exercise 3.1. Fill in the remaining part of the proof by showing that $1, x, \ldots, x^{|x|-1}$ are distinct.

4. The Structure of Cyclic Groups: 10/1/12

Since every element of a group is contained in a cyclic subgroup, then investigating and classiftying them will reveal a lot of things about groups in general.

Lemma 4.1. *Let G be a group, $x \in G$, and $n, m \in \mathbb{Z} \setminus \{0\}$. If $x^n = x^m = 1$, then $x^{(m,n)} = 1$.*[8]

Proof. Using the Euclidean algorithm, $(n, m) = an + bm$ for $a, b \in \mathbb{Z}$. Then,

$$x^{(n,m)} = x^{an+bm} = x^{an}x^{bm} = (x^a)^m(x^b)^m = 1.$$ □

Corollary 4.2. *If $x^m = 1$, then $|x| \mid m$.*

Proof. Set $n = |x|$ in Lemma 4.1, so that $x^{(n,m)} = 1$. But $(m, n) \leq n$, so $(m, n) = |x|$, because the order is minimal. □

This is another example of cyclic groups being particularly pretty, as this statement does not hold true for groups in general.

It will now be possible to prove the classification theorem for cyclic groups.

[8] The greatest common divisor of two integers, $\gcd(a, b)$, is also denoted (a, b) when there is no issue of confusion with open intervals or ordered pairs.

Proof of Theorem 3.3. Case 1. Assume $G \cong H$ and prove that $|G| = |H|$.

Clearly, if f is an isomorphism between G and H, then f is one-to-one, and so G and H have the same number of elements (and if either is infinite, then the other must be as well).

Case 2. Suppose $|G| = |H|$ for cyclic G, H, and prove that $G \cong H$.

Define $G \overset{\varphi}{\to} H$ by $\varphi(x^k) = y^k$ for $k \in \mathbb{Z}$. Since G is cyclic, then every element in G can be written as x^k for some $k \in \mathbb{Z}$.

It will be necessary to argue that φ is well-defined: if $x^k = x^\ell$, then $x^{k-\ell} = 1$, so by Lemma 4.1, $n \mid k - \ell$, so $k - \ell = nd$ for some $d \in \mathbb{Z}$. Then,

$$y^{k-\ell} = y^{nd} = (y^n)^d = 1 \implies y^k = y^\ell$$

by multiplying by y^ℓ on both sides. Thus, φ is well-defined.

It is now 'obvious' that φ is a homomorphism; it is easy to check that $\varphi(x^k x^\ell) = \varphi(x^k)\varphi(x^\ell)$, and it is also clear that it is a bijection: the map $\psi(y^k) = x^k$ is well-defined by the same argument that φ is, and composition shows that $\psi \circ \varphi = \varphi \circ \psi = \mathrm{Id}$. □

One again, the case where G and H have infinite order is left as an exercise.

One can also classify subgroups of cyclic groups, which once again is easier and nicer than the general case.

Proposition 4.3. *If G is a group, $x \in G$, and $a \in \mathbb{Z} \setminus \{0\}$, then:*

i. If $|x|$ is infinite, then $|x^a|$ is infinite.
ii. If $|x| = n$ (is finite), then $|x^a| = \frac{n}{(n,a)}$.
iii. If $|x| = n$ and $a \mid n$, then $|x^a| = \frac{n}{a}$. (This follows from ii, since $(n, a) = a$.)

Proof of ii. Let $r = \frac{n}{(n,a)}$, so that $(n, a)s = a$ for some s for which $(r, s) = 1$.

Since $|x^a|, r \in \mathbb{N}$, then showing their equality is equivalent to showing $|x^a|/r$ and $r/|x^a|$:

- if $(x^a)^r = 1$, then $|x^a| \mid r$, because $x^{\frac{an}{(n,a)}} = x^{ns} = 1$.
- $1 = (x^a)^k = x^{ak}$, so since $|x| = n$, then $n \mid ak$, so $(n, a)r \mid (n, a)sk$, so $r \mid sk$ and therefore $r \mid k$, since $r \nmid s$. □

Corollary 4.4. *If G is finite and $G = \langle x \rangle$, then $G = \langle x^k \rangle$ iff $(k, |x|) = 1$.*

Corollary 4.5. *If $a \mid n$, then $\langle x^a \rangle \leq G$ has order $\frac{n}{a}$.*

In some sense, there is a well-defined bijection from the divisors of n to the subgroups of a cyclic group of order n. That this is even a bijection is surprising and important, allowing the subgroups to be classified.

Theorem 4.6. *If G is cyclic and $G = \langle x \rangle$, then:*

i. All subgroups of G are cyclic and in fact if $H \leq G$ then $H = \langle x^a \rangle$, where

$$a = \begin{cases} \min\{n \in \mathbb{N} \mid x^n \in H\}, & H \neq \{0\} \\ 0, & H = \{0\}. \end{cases}$$

ii. For any $a \mid |G|$, there is a unique $H \leq G$ given by $H = \langle x^{\frac{n}{a}} \rangle$ such that $|H| = a$, if G is finite.

If G is finite, then i implies $|H| = |x^a| = \frac{n}{(n,a)} \mid n$ (which is akin to a surjection, and ii establishes that it is an injection). Additionally, this is yet another nice result that is only true for cyclic groups: for $G = D_8$, $|r^2| = 2$ and $|s| = 2$, but $\langle r^2 \rangle \neq \langle s \rangle$.

Proof of Theorem 4.6. Part i: Given $H \leq G = \langle x \rangle$, let $a = \min\{n \in \mathbb{N} \mid x^n \in H\}$. Since $x^a \in H$, then $\langle x^a \rangle \subseteq H$.

Conversely, if $y \in H \leq G$, then $y = x^n$ for some $n \in \mathbb{Z}$ because G is cyclic. Thus, $n = qa + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < a$, so $x^r = x^n x^{-qa} = x^n (x^a)^{-q} \in H$ (because $x^n, x^a \in H$).

This means that $r = 0$, so $n = qa$, so $y = x^n = (x^a)^q \in \langle x^a \rangle$, so $H \subseteq \langle x^a \rangle$, and every subgroup of a cyclic group is cyclic.

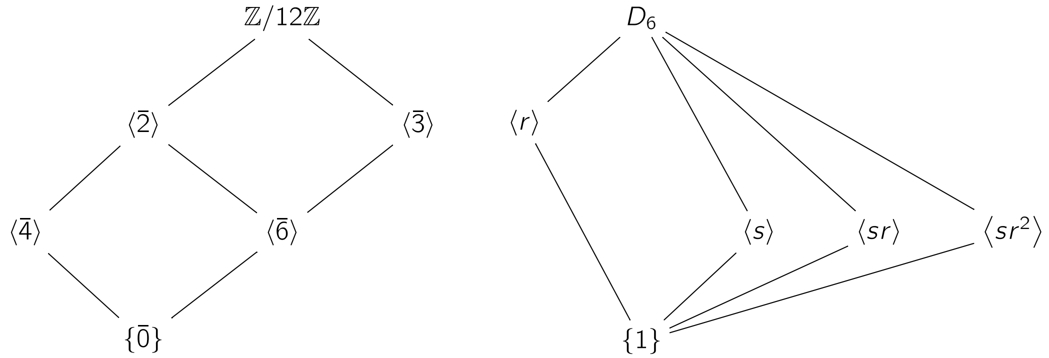
Part ii: Suppose $H = \langle x^b \rangle \leq G = \langle x \rangle$ (this is just the finite case; see the book for the infinite one).

$(n, b) \mid b$, so $x^b \in \langle x^{(n,b)} \rangle$. Thus $\langle x^b \rangle \subseteq \langle x^{(n,b)} \rangle$. But $(n, b) \mid n$, so they have the same order (i.e. $\frac{n}{(n,b)}$). Thus, $\langle x^b \rangle = \langle x^{(n,b)} \rangle$ (since if A, B are finite sets, $|A| = |B|$, and $A \subseteq B$, then $A = B$). Thus, each subgroup is uniquely determined from a prime factor of n. □

5. Quotient Groups: 10/3/12

In some sense, there is more than just a set of subgroups; they have a lattice-like structure.

Example 5.1.



Here, if A is above B and connected by a vertical line, then $B < A$.

So far, all the subgroups mentioned are cyclic. But this is not true in general; $\{1, r^2, s, sr^2\} \leq D_8$, for example. Thus, some new notation is introduced.

Definition. If G is a group with $x_1, \dots, x_n \in G$, then $\langle x_1, \dots, x_n\rangle$ is the smallest subgroup containing them. This can be formalized in two ways:

$$\langle x_1, \dots, x_n\rangle = \bigcap_{\substack{H\leq G\\ x_1,\dots,x_n\in H}} H = \left\{\prod_{j=1}^{n} x_j^{k_j} \mid k_1, \dots, k_n \in \mathbb{Z}\right\}.$$

Similarly, if $A \subseteq G$, then the smallest subgroup containing A is

$$\langle A\rangle = \bigcap_{\substack{H\leq G\\ A\subseteq H}} H = \left\{\prod_{a\in A} a^{k_a} \mid k_a \in \mathbb{Z}\right\}.$$

Definition. The kernel of a homomorphism $\varphi : G \to H$ is $\operatorname{Ker}(\varphi) = \{g \in G \mid \varphi(g) = 1\}$.

Lemma 5.1. *$\operatorname{Ker}(\varphi) \leq G$.*

Proof.

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1) \implies 1 = \varphi(1),$$

so $1 \in \operatorname{Ker}(\varphi)$.

$\varphi(x) = 1 \implies \varphi(x^{-1}) = \varphi(x)^{-1} = 1^{-1} = 1$, and if $\varphi(x) = \varphi(y) = 1$, then $\varphi(xy) = \varphi(x)\varphi(y) = 1$. □

The motivating question behind quotient groups is, given a $K \leq G$, to find a quotient group G/H and some surjective homomorphism $\pi : G \to H$ such that $\operatorname{Ker}(\pi) = K$.[9] The terminology and notation comes from dividing numbers; the two processes have much in common.

It is possible to show the uniqueness of such a surjection, even though we don't yet know it exists!

Proposition 5.2. *If $\varphi : G \to H$ and $\varphi' : G \to H'$ are surjective homomorphisms with kernels $K = \operatorname{Ker}(\varphi) = \operatorname{Ker}(\varphi')$, then there is a unique isomorphism $\psi : H \to H'$ such that $\psi(\varphi(g)) = \varphi'(g)$.*

Proof. For any $H \in H$, choose a $g \in G$ such that $h = \varphi(g)$ (since φ is surjective). However, g might not be unique.

Then, let $\psi(h) = \varphi'(g)$. ψ is well-defined, because if $h = \varphi(g_1) = \varphi(g_2)$, then $1 = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1g_2^{-1})$, so $g_1g_2^{-1} \in K$, so $1 = \varphi;(g_1g_2^{-1}$, since $K = \operatorname{Ker}(\varphi')$ as well. In the same manner, one can show $\varphi'(g_1) = \varphi'(g_2)$.

ψ is a bijection because H, H' are equivalent; one can create a well-defined map in the other directon in the same manner, so ψ has an inverse.

ψ is also a homomorphism: if $h_1, h_2 \in H$, then pick g_1, g_2 such that $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$. Then,

$$\psi(h_1)\psi(h_2) = \varphi'(h_1)\varphi'(h_2) = \varphi'(h_1h_2) = \psi(h_1h_2).$$

Since φ is a homomorphism, then $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = h_1h_2$.

Thus, ψ is an isomorphism. □

[9] I actually disagree; though this was the motivation given in lecture, it seems somewhat clunky. It seems more interesting to approach from the angle of equivalence classes. But your mileage may vary.

It turns out there is a necessary condition for $k \leq G$ to be the kernel of a homomorphism $\varphi : G \to H$: if $K = \mathrm{Ker}(\varphi)$, then for any $k \in K$, $g \in G$, then

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = 1$$

because $k \in \mathrm{Ker}(\varphi)$. Thus, $gkg^{-1} \in K$. For example, $H = \{1, s\} \leq D_{2n}$ is not the kernel of any homomorphism, because $rsr^{-1} = sr^{-2} \notin H$ when $n \neq 2$.

Definition. A subgroup $H \leq G$ is normal, written $H \trianglelefteq G$, if $ghg^{-1} \in H$ for any $h \in H$, $g \in G$.

This is not just a necessary condition for the existence of a homomorphism with H as its kernel, but also a sufficient one.

Definition. If $H \trianglelefteq G$, then there is an equivalence relation on G where $g_1 \sim g_2$ if $g_1h = g_2$ for some $h \in H$. Each of these equivalence classes is called a left coset.

It's straightforward to show that $\sim$ is an equivalence relation. $g \sim g$ since $1 \in H$, and if $g_1 = hg_2$ then $g_2 = h^{-1}g_1$. If $g - 1 = h_1g_2$ and $g_2 = h_2g_3$, then $h_1h_2 \in H$ and $g_1 = (h - 1h_2)g_3$.

Notationally, the equivalence class of G is the left coset $gH = \{gh \mid h \in H\}$.

Definition. If $H \leq G$, the quotient G/H is the set of left cosets of G under H.[10]

Theorem 5.3. *If $H \trianglelefteq G$, then there is a unique group structure on G/H such that the surjection $\pi : G \to H$ given by $\pi : g \mapsto gH$ is a homomorphism.*

The natural choice for a group operation is well-defined (i.e. multiplication within equivalence classes), but it will be necessary to check this. Formally, the operation will be $(g_1H)(g_2H) = (g_1g_2)H$, which is the only way to make π a homomorphism.

6. More Quotient Groups: 10/5/12

Left cosets are either equal or disjoint. Thus, one can write several equivalences:

$$g_1 \sim g_2 \iff g_1g_2^{-1} \in H \iff g_1 \in g_2H \iff g_1H = g_2H.$$

One can also think of G/H, the set of left cosets of G, as a subset of the power set of G.

Example 6.1. In $\langle s \rangle \leq D_6$, the cosets are $1\langle s \rangle = s\langle s \rangle = \langle s \rangle$, $r\langle s \rangle = sr^2\langle s \rangle = \{r, sr^2\}$, and $r^2\langle s \rangle = sr\langle s \rangle = \{r^2, sr\}$.

Thus, $D_6/\langle s \rangle = \{\langle s \rangle, r\langle s \rangle, r^2\langle s \rangle\}$.

Proof of Theorem 5.3. Since $\pi(g_1g_2) = \pi(g_1)\pi(g_2)$, then the only possible definition for the group operation is $g_1H)(g_2H) = (g_1g_2)H$.

But since there are multiple ways to write a given left coset, it will be necessary to check well-definedness.

Suppose $g_1H = \bar{g}_1H$ and $g_2H = \bar{g}_2H$. Then, $g_1^{-1}\bar{g}_1 \in H$ and $g_2^{-1}\bar{g}_2H$.

Since H is normal then

$$(g_1g_2)^{-1}(\bar{g}_1\bar{g}_2) = g_2^{-1}(g_1^{-1}\bar{g}_1)\bar{g}_2 = g_2^{-1}(g_1^{-1}\bar{g}_1)(g_2^{-1})^{-1}(g_2^{-1}\bar{g}_2).$$

Since $g_1^{-1}\bar{g} - 1 \in H$, then $g_2^{-1}(g_1^{-1}\bar{g}_1)(g_2^{-1})^{-1} \in H$ by normality. And since $g_2^{-1}\bar{g}_2 \in H$, then this whole product is in H, so $(g_1g_2)H = (\bar{g}_1\bar{g}_2)H$.

After well-definedness, the rest of the proof is straightforward. Checking the group axioms just involves multiplying out the representatives to check the axioms.

Finally, we can go back and prove that π is a homomorphism: $\pi(g_1g_2) = g_1g_2H = (g_1H)(g_2H) = \pi(g_1)\pi(g_2)$. □

Since $(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1}$, then it suffices to check normality on the generators of H on G. On G, this is true for products but not inverses.

Example 6.2. Consider $\langle r \rangle \trianglelefteq D_6$. $D_6/\langle r \rangle = \{\langle r \rangle, s\langle r \rangle\} \cong \mathbb{Z}/2\mathbb{Z}$.

In the linear-algebraic analogy, quotient groups are akin to quotient vector spaces (though these aren't usually covered in elementary linear algebra courses). If V is a vector space of which W is a subspace, then you can obtain another subspace V/W.

Theorem 6.1 (Lagrange). *If $H \leq G$ and $|G|$ is finite, then $|G/H| = |G|/|H|$.*

[10] The textbook uses a different definition in which G/H is only defined when $H \trianglelefteq G$.

Proof. Any element $gH \in G/H$ is a subset of G and there is a bijection $H \to gH$ given by $h \mapsto gh$ (with inverse $h \mapsto g^{-1}h$), so $|gH = H|$.

Since the cosets form a partition (i.e. are disjoint and cover all of G), then $|G| = |H||G/H|$. □

7. Consequences of Lagrange's Theorem: 10/8/12

If G is abelian, then all of its subgroups are normal, since all elements commute, not just the members of the subgroup. Normality isn't really present in the vector-space analogue, since it would be trivially satisfied by all subspaces.

Example 7.1. Consider some $n \in \mathbb{Z}$. It is a matter of notation to write $n\mathbb{Z} = \langle n \rangle = \{an \mid a \in \mathbb{Z}\}$ (since the group is written additively). Since $\mathbb{Z}$ is abelian, then $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, so $\mathbb{Z}/n\mathbb{Z}$ is a group, which happens to be the familiar integers mod n, and is the reason for their at first somewhat obscure notation.

Here are some consequences of Lagrange's Theorem; for each of the following corollaries, assume G is a finite group.

Corollary 7.1. *If $H \leq G$, then $|H| \mid |G|$.*

Proof. $|G/H| \in \mathbb{Z}$ (whether or not H is normal), so $|H||G/H| = |G|$, so $|H| \mid |G|$. □

Corollary 7.2. *If $|G|$ is prime, then the only subgroups of G are $\{1\}$ and G.*

Proof. If $H \leq G$, then $|H| \mid |G|$ and $1 \in H$. Thus, either $|H| = 1$, in which case $|H = \{1\}$, or $|H| = |G|$, in which case $H = G$. □

Corollary 7.3. *If $x \in G$, then $|x| \mid |G|$.*

Proof. $|x| = |\langle x \rangle|$, and $\langle x \rangle \leq G$, so $|x| = |\langle x \rangle| \mid G$. □

This last corollary is particularly helpful, as it allows one to calculate the orders of elements in a group by limiting their possibilities (which can then just be checked).

Corollary 7.4. *If $x \in G$, then $x^{|G|} = 1$.*

Proof.

$$x^{|G|} = \left(x^{|x|}\right)^{\frac{|G|}{|x|}} = 1^{\frac{|G|}{|x}} = 1.$$ □

Corollary 7.5. *If $|G| = p$ for some prime p, then $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. $|G| > 1$, so choose an $x \in G \setminus \{1\}$. Then, $|x| > 1$ and $|x| \mid p$, so $|x| = p = |G|$ and $\langle x \rangle = G$. Thus, G is cyclic, and by Theorem 3.3, any two cyclic groups of the same order are isomorphic, so $G \cong \mathbb{Z}/p\mathbb{Z}$. □

Step back and see that these all follow from the group axioms in an entirely non-obvious way. This is an illustration of the power of these group axioms, even though they are so simply defined.

Lagrange's Theorem is only applicable to finite groups, but it can be generalized carefully. For example, if G is infinite and $H \leq G$ is finite, then G/H is also infinite. However:

Example 7.2. For an $n \in \mathbb{Z}$, $|\mathbb{Z}/n\mathbb{Z}| = n$ is finite, but both $\mathbb{Z}$ and $n\mathbb{Z}$ are infinite (and, in fact, $\mathbb{Z} \cong n\mathbb{Z}$). It is meaningless to say that $n = \infty/\infty$, however.

Example 7.3. The quotient of an infinite group by an infinite subgroup is not always finite, however; $\mathbb{Z} \trianglelefteq (\mathbb{Q}, +)$, but $\mathbb{Q}/\mathbb{Z}$ is infinite.

Lagrange's Theorem also says nothing about the group structure on the quotient, only the number of elements.

Example 7.4. Suppose $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $H_1 = \langle(\bar{1}, \bar{0})\rangle \cong \mathbb{Z}/2\mathbb{Z}$ and $H_2 = \langle(\bar{0}, \bar{2})\rangle \cong \mathbb{Z}/2\mathbb{Z}$. Then, both H_1 and H_2 are normal in G, and by Lagrange's Theorem, $|G/H_1| = |G/H_2| = 4$.

However, $G/H_1 \ncong G/H_2$: $G/H_1 = \mathbb{Z}/4\mathbb{Z}$, but $G/H_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (which has no elements of order 4).

Definition. The index of a subgroup $H \leq G$ is $|G : H| = |G/H|$.

Normality can be defined in many different ways: in addition to the provided definition that $H \trianglelefteq G$ if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$, one could use many competing definitions, such as:

- $gHg^{-1} = H$ for every $g \in G$ (where $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$).[11]
- $Hg = gH$ for all $g \in G$.

[11] This works because if $H \leq G$, then $gHg^{-1} \subseteq G$ for all $g \in G$.

- $N_G(H) = G$, where $N_G(H)$ is the normalizer, defined below.

Definition. The normalizer of a subgroup $H \leq G$ is $N_G(H) = \{g \in G : gHg^{-1} = H\}$.

Lemma 7.6. *$N_G(H)$ is the largest subgroup of G such that $H \trianglelefteq N_G(H) \leq G$.*

Proof. $1 \in N_G(H)$ trivially, and if $g_1, g_2 \in N_G(H)$, then

$$(g_1g_2)H(g_1g_2)^{-1} = g_1(g_2Hg_2^{-1})g_1^{-1} = g_1Hg_1^{-1} = H,$$

and inverses follow similarly. Additionally, $H \trianglelefteq N_G(H)$ pretty much by the definition; this is straightforward to check. □

Example 7.5. Consider $\langle r\rangle \leq D_{2n}$, as in Example 6.2 (let $G = D_{2n}$ and $H = \langle r\rangle$); Lemma 7.6 makes the proof that $\langle r\rangle \trianglelefteq D_{2n}$ much simpler. Since

$$2 = |G : H| = |G|/|H| = \frac{|G|}{|N_G(H)|}\frac{|N_G(H)|}{|H|},$$

but all of these are integers, then $|H : N_G(H)| = 1$ or 2, and verifying that $s \in N_G(H)$ implies that this is 2, so $H \trianglelefteq G$.

Definition. The centralizer of a sub*set* $A \subseteq G$ is $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$.

This looks similar to the normalizer, but the centralizer has the stricter condition of equality, rather than just inclusion in the subgroup.

Definition. The center of a group G is $Z(G) = C_G(G) = \{g \in G \mid ga = ag \text{ for all } a \in G\}$.

Lemma 7.7. *The centralizer (and therefore the center) of G are subgroups.*

Proposition 7.8. *If $H \leq G$ and $|H : G| = 2$, then $H \trianglelefteq G$.*

This is only true when $|H : G| = 1$ or 2. The proof of this proposition will be deferred to the next lecture.

To what extent is the converse of Lagrange's Theorem true? Generally, it is not true that if G is finite and $d \mid |G|$, then there is necessarily a subgroup of order d (for example, there is a group of order 12 with no subgroups of order 6), but there are some partial answers.

Theorem 7.9 (Cauchy)**.** *If G is finite and $p \mid |G|$ for some prime p, then there is some $x \in G$ for which $|x| = p$.*

Theorem 7.10 (Sylow)**.** *If $|G| = p^\alpha m$ for some prime $p \nmid m$, then there is a subgroup $H \leq G$ such that $|H| = p^\alpha$.*

Sylow's Theorem is a very deep theorem that is essential for understanding subgroups.

8. The First Isomorphism Theorem: 10/10/12

Definition. A right coset of a subgroup $H \leq G$ is a set $Hg = \{hg \mid h \in H\}$ for some $g \in G$.

Sometimes, the set of right cosets of H in G is denoted $H\backslash G$, but this clashes with complements of sets and will not be used here.

Right cosets are very much like left ones: G is partitioned into right cosets, for example, and the proof of this is essentially the same as in the left case.

The function $G \xrightarrow{f} G$ given by $x \mapsto x^{-1}$ is usually not a homomorphism, but it gives a bijection $gH \leftrightarrow Hg$.

Proof of Proposition 7.8. Since $|G : H| = 2$, then there are 2 right cosets. One of these is $H1 = H$, and since the right cosets form a partition, then the only other coset of $H \setminus G$. But this is also true of the left cosets: $G/H = \{H, G \setminus H\}$. Thus,

$$gH = \left\{\begin{array}{ll} H, & g \in H \\ G \setminus H, & g \notin H \end{array}\right\} = Hg.$$

Thus, $gH = Hg$ for all $g \in G$, so $H \trianglelefteq G$. □

Example 8.1. The now familiar $\langle r\rangle \trianglelefteq D_{2n}$ is proven trivially, since $|D_{2n} : \langle r\rangle| = 2$.

Lemma 8.1. *If φ is a group homomorphism, then φ is injective iff* $\operatorname{Ker}(\varphi)$ *is trivial.*

"The proof has two directions: one is completely trivial, and the other is almost trivial."

Also, this lemma is true for injective maps between vector spaces for the linear-algebra scheme, but this is about as helpful for visualization as for groups.

Proof of Lemma 8.1. In the forward direction, if $g \in G \setminus \{1\}$, then $\varphi(g) \neq \varphi(1) = 1$, so $g \notin \operatorname{Ker}(\varphi)$.

In the reverse direction, suppose $g_1, g_2 \in G$. If $\varphi(g_1) = \varphi(g_2)$, then

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_1)^{-1} = 1,$$

so $g_1 g_2^{-1} \in \operatorname{Ker}(\varphi)$, so $g_1 g_2^{-1} = 1$ and $g_2 = g_2$. Thus, φ is injective. □

In some sense, the size of $\operatorname{Ker}(\varphi)$ measures how "non-injective" a homomorphism φ is.

There are four isomorphism theorems, but the first is by far the most important:

Theorem 8.2 (First Isomorphism Theorem)**.** *If $\varphi : G \to H$ is a homomorphism, then*

(i) $\operatorname{Ker}(\varphi) \trianglelefteq G$*,*

(ii) $\operatorname{Im}(\varphi) \leq H$*, and*

(iii) $G/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$ *by the well-defined isomorphism* $gK \overset{\bar{\varphi}}{\mapsto} \varphi(g)$*.*

"When you see normality, you should feel the urge to take a quotient."

Example 8.2. Consider the homomorphism $(\mathbb{R}, +) \xrightarrow{\varphi} \mathbb{C}^\times$ (i.e. $(\mathbb{C} \setminus \{0\}, \cdot)$ given by $\varphi(t) = e^{2\pi i t}$). Then, $\operatorname{Ker}(\varphi) = \mathbb{Z}$, and $\operatorname{Im}(\varphi) = \{z \in \mathbb{C} \mid |z| = 1\} = C$ (i.e. the unit circle). Using the 1st Isomorphism Theorem, $C \cong \mathbb{R}/\mathbb{Z}$!

Example 8.3. For a nonabelian example, consider $\mathrm{G}\ell_n(\mathbb{R})$ and $\mathrm{S}\ell_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\}$. Then, $\mathrm{S}\ell_n(\mathbb{R}) \trianglelefteq \mathrm{G}\ell_n(\mathbb{R})$ and $\mathrm{G}\ell_n(\mathbb{R})/\mathrm{S}\ell_n(\mathbb{R}) \cong \mathbb{R}^\times$ (i.e. $(\mathbb{R} \setminus \{0\}, \cdot)$). This is because $\det : \mathrm{G}\ell_n(\mathbb{R}) \to \mathbb{R}^\times$ is a group homomorphism (since $\det AB = \det A \det B$) and is surjective (so that $\operatorname{Im}(\det) = \mathbb{R}^\times$ and $\operatorname{Ker}(\det) = \mathrm{S}\ell_n(\mathbb{R})$).

Proof of Theorem 8.2. Part i is a restatement of Lemma 5.1

Part ii: if $h_1, h_2 \in \operatorname{Im}(\varphi)$, then $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$ for some $g_1, g_2 \in G$. Thus, $\varphi(g_1 g_2) = h_1 h_2 \in H$ (and inverses are essentially similar).

Part iii: Let $K = \operatorname{Ker}(\varphi)$. Then, if $g_1 K = g_2 K$, then $g_2^{-1} g_1 \in K$, so $g_2^{-1} g_1 = 1$ and $g_1 = g_2$, so $\bar{\varphi}$ is well-defined.

$\bar{\varphi}$ is a homomorphism because it inherits the previous homomorphism structure from φ. It is surjective because, "uh, well. . . it is;" to be precise, surjectivity is inherent in the definition of the image.

If $\bar{\varphi}(gH) = 1$, then $g \in K$, so $gK = 1K = 1 \in G/K$. Thus, by Lem 8.1, $\operatorname{Ker}(\bar{\varphi}) = 1$, so $\bar{\varphi}$ is injective. □

There will almost certainly be a problem on the midterm that uses the First Isomorphim Theorem to prove normality or isomorphisms, so remember it well.

Philosophically, modding out by the kernel makes a homomorphism injective, and replacing the target by the image makes it surjective.

If $H \trianglelefteq G$, where $H \neq \{1\}$ and $H \neq G$, one can "decompose" G into H and G/H. Unlike the equivalent result for vector spaces, though, it is *not* generally true that $G \cong H \times G/H$. Nonetheless, it may be possible to learn things about larger groups by studying their decompositions. And if G is finite, this process must terminate.

Definition. A group is simple if $\{1\}$ and G are its only normal subgroups.

Example 8.4. By Lagrange's Theorem, the only subgroups of $\mathbb{Z}/p\mathbb{Z}$ are $\{\bar{0}\}$ and $\mathbb{Z}/p\mathbb{Z}$ when p is prime, so for p prime, $\mathbb{Z}/p\mathbb{Z}$ is simple.

It is harder to come up with nonabelian examples; the smallest simple nonabelian group has 60 elements and is the group of symmetries of the regular icosahedron. (Similarly to the calculation of $|D_{2n}| = 2n$, there are 12 vertices, and to completely specify an element, pick one vertex and send it to another, and then send one neighbor to one of the five new neighbors, giving 60 options). This group is isomorphic to A_5, an alternating group, which will be talked about later.

This leads natually to the goal of classifying all finite simple groups. This is in fact exceedingly difficult, and was only finished in the 1980s. There are a bunch of families, such as $\mathbb{Z}/p\mathbb{Z}$ for prime p, $\mathrm{S}\ell_n(\mathbb{F}_q)/Z(\mathrm{S}\ell_n(\mathbb{F}_q))$, for various n and q, and so on. There are also 26 "sporadic" groups, the largest of which is called the Monster group, which has $|M| \approx 8 \cdot 10^{53}$ elements!

The proof that these were all the finite simple groups is a large number of papers totalling about 10000 pages.

9. The Alternating Group: 10/12/12

Recall that any $\sigma \in S_n$ can be written as a product of disjoint cycles (Theorem 2.1), but

$$(a_1\ a_m) \cdots (a_1\ a_3)(a_1\ a_2) = (a_1\ a_2\ a_3\ \cdots\ a_{m-1}\ a_m),$$

so σ can be written as a product of (not necessarily disjoint) 2-cycles (which are generally called transpositions). Thus, $S_n = \langle (i\ j) \mid 1 \leq i < j \leq n \rangle$.

Pictorially, if one draws arrows from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$, each intersection of the arrows represents a transposition between two elements.

This decomposition into transpositions is not unique (since $\sigma = \sigma\tau_{12}\tau_{21}$, for example), but it is always unique $\mod 2$; that is, every 2-cycle decomposition of a given $\sigma \in S_n$ has either an odd or an even number of elements. More formally, let $r(\sigma) = |\{(i\ j) \mid i < j, \sigma(i) > \sigma(j)\}|$ (i.e. $r(\sigma)$ is the number of inversions) and let $\varepsilon(\sigma) = (-1)^{r(\sigma)}$. Thus, ε returns $+1$ if there are an even number of permutations, and -1 if there are an odd number.

The book defines $\Delta = \prod_{1 \leq i < j \leq n}(x_i - x_j)$ and $\sigma(\Delta) = \prod_{1 \leq i < j \leq n}(x_{\sigma(i)} - x_{\sigma(j)}) = \varepsilon(\sigma)\Delta$. Each transposition switches two elements and thus flips the sign of Δ, so the total number of sign flips is $r(\sigma)$.

Lemma 9.1. *$\varepsilon : S_n \to (\{\pm 1\}, \cdot)$ is a homomorphism.*

Proof.

$$r(\tau\sigma) = r(\sigma) + r(\tau) - 2|\{(i\ j) \mid i < j, \sigma(i) > \sigma(j), \tau\sigma(i) < \tau\sigma(j)\}|,$$

but the last term is even and thus disappears when you exponentiate by -1. Thus, $(-1)^{r(\tau\sigma)} = (-1)^{r(\sigma)+r(\tau)}$. □

(An actual, formal proof would have to be a bit more formal and use some principles of inclusion and exclusion.)

Definition. $\sigma \in S_n$ is even if $\varepsilon(\sigma) = 1$ (i.e. $r(\sigma)$ is even), and is odd otherwise (i.e. $\varepsilon(\sigma) = -1$ and $r(\sigma)$ is odd).

Definition. The alternating group of order n is the group of even permutations of $\{1, \ldots, n\}$. $A_n = \operatorname{Ker}(\varepsilon)$ given the above definition of ε.

Example 9.1. Suppose $\sigma = (i\ j)$. Then $\varepsilon(\sigma) = -1$.

If $\sigma = (a_1\ \ldots\ a_m)$, then $\varepsilon(\sigma) = (-1)^{m-1}$ because the transposition decomposition is into $m - 1$ transpositions and ε is a homomorphism.[12]

Thus, one can obtain $\varepsilon(\sigma)$ for any $\sigma \in S_n$ from its cycle homomorphism.

By the First Isomorphism Theorem and Lagrange's Theorem, $\{\pm 1\} = S_n/A_n$, so $2 = |S_n|/|A_n|$, so $|A_n| = n!/2$.

This grows very quickly; $|M| = 8 \cdot 10^{53}$ from the last lecture, but $|A_{100}| \gg |M|$.

Example 9.2. $A_2 = \{1\}$, and A_3 has order 3, so $A_3 = \langle(1\ 2\ 3)\rangle \cong \mathbb{Z}/3\mathbb{Z}$.

$|A_4| = 12$, and in fact it is isomorphic to the symmetry group of the tetraherdon.

Notice that $6 \mid 12$, but A_{12} has no subgroup of order 6, so the converse of Lagrange's Theorem is untrue.

Suppose $H < A_4$ and $|H| = 6$. Since $|A_4 : H| = 2$, then $H \lhd A_4$. Thus, $A_4/H \cong \mathbb{Z}/2\mathbb{Z}$ because 2 is prime.

Let $A_4 \xrightarrow{\varphi} A_4/H$ be the canonical homomorphism. Then, for any $x \in A_4$, $\varphi(x^3) = 3\varphi(x) = \varphi(x)$, so $x \in \operatorname{Ker}(\varphi)$ and φ sends anything of order 3 to 1.

However, there are at least 8 elements of A_4 of order 3: $(1\ 2\ 3)$, $(1\ 3\ 4)$, $(1\ 2\ 4)$, $(2\ 3\ 4)$, and their (distinct) inverses. Thus $|H| \geq 8$, which is a contradiction.

Lemma 9.2. *$\langle(i\ j\ k) \mid 1 \leq i < j < k \leq n\rangle = A_n$.*

Proof. First show inclusion. If σ is any product of 3-cycles $\sigma_1, \ldots, \sigma_k$, then $\varepsilon(\sigma) = \prod_{j=1}^{k} \varepsilon(\sigma_i) = 1$.

Then, show reverse inclusion: suppose $\sigma \in A_n$. Since $\sigma \in S_n$, then write σ as a product of 2-cycles. Since $\sigma \in A_n$, then there will necessarily be an even number of these cycles. Thus,

$$\sigma = \prod_{j=1}^{k}(a_i\ b_i)(c_i\ d_i) = \prod_{j=1}^{k}(c_i\ a_i\ d_i)(a_i\ b_i\ c_i),$$

where all the $a_i \neq b_i$ and $c_i \neq d_i$. Thus, σ is generated by 3-cycles. □

Theorem 9.3. *A_n is simple for $n \geq 5$.*

This is much deeper than it looks; the fact that A_5 is simple means there is no quintic formula of radicals (in integers, $+$, $-$, $\times$, $/$, and k^{th} roots) to solve fifth-degree polynomials.

This is the domain of Galois theory, invented by a mathematician named Galois, who died in a duel (possibly over a girl) at age 20... and yet still found time to revolutionize a branch of mathematics.

[12] This can be confusing: a cycle of even length is odd, and vice versa.

10. Proof That A_n is Simple when $n \geq 5$: 10/15/12

Though the proof is for the case when $n \geq 5$, $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ is clearly simple, as are the trivial A_1 and A_2. But A_4 is not simple.

The book uses a different proof, but it is less direct. Informally, this proof will show that any $N \trianglelefteq A_n$ for $n \geq 5$ such that $N \neq \{1\}$ contains all 3-cycles and thus $N = A_n$. Unfortunately, this is a proof by casework.

Proof of Theorem 9.3. Suppose $n \geq 5$, $N \trianglelefteq A_n$, and $N \neq \{1\}$.

Case 1. Suppose there is some 3-cycle $(a\ b\ c) \in N$. Then, $N = A_n$.

Proof. Since N is normal, then let $\tau = (a'\ b'\ c') \in A_n$ be another 3-cycle. Then, if $\sigma = (a\ a')(b\ b')(c\ c') \in S_n$, then $\sigma \circ (a\ b\ c) \circ \sigma^{-1} = \tau$. (If σ is odd when given in this manner, then use the fact that $n \geq 5$ and use instead $\sigma' = \sigma \circ (d\ e)$, which is even if σ isn't, and still satisfies $\sigma' \circ (a\ b\ c) \circ (\sigma')^{-1} = \tau$.)

Thus, N contains every 3-cycle, and since A_n is generated by 3-cycles, then $N = A_n$. □

Case 2. Suppose $\sigma \in N$ is a product of disjoint 2-cycles.

Case 2a. If $\sigma = (a\ b)(c\ d)$, then, using the fact that there are at least five elements, let $\tau = (c\ d\ e)$. Then, $\tau\sigma\tau^{-1} = (a\ b)(d\ c)$, so $\tau\sigma\tau^{-1}\sigma^{-1} = (c\ e\ d)$, so $N = A_n$ by Case 1.

Case 2b. Otherwise, $\sigma = (a\ b)(c\ d)(e\ f)\mu$ for some μ that is a product of disjoint 2-cycles (i.e. $n \geq 6$). Then, the same trick will be used: let $\tau = (c\ d\ e)$, so that $\tau\sigma\tau^{-1}\sigma^{-1} = (c\ e)(d\ f)$, which leads back to Case 2a.

Case 3. If there are no products of transpositions, then N must contain a cycle σ of length strictly greater than 3.

Case 3a. Suppose $\sigma = (a\ b\ c\ d\ e)\mu$. Then, let $\tau = (c\ d\ e)$ and use the same trick: $\sigma\tau\sigma^{-1}\tau^{-1} = (a\ d\ c)$, which yields Case 1.

Case 3b. If $\sigma = \tau\mu$ for an m-cycle τ where $m > 5$, the proof is essentially the same as in the previous case.

Case 3c. If $\sigma = (a\ b\ c\ d)(e\ f_1\ \cdots\ f_n)\mu$, let $\tau = (c\ d\ e)$ and do the same thing again, yielding $\tau\sigma\tau^{-1}\sigma^{-1} = (a\ f\ c\ d\ e)$, which reduces to Case 3a.

Case 4. The only remaining case is the one in which $\sigma \in N$ is a product of 3-cycles. Then, using $\tau = (c\ d\ e)$, one obtains $\tau\sigma\tau^{-1}\sigma^{-1} = (a\ f\ c\ d\ e)$, which reduces to Case 3a.

Thus, if $N \neq \{1\}$, $N \trianglelefteq A_n$, and $n > 5$, then $N = A_n$, so A_n is simple. □

In general, proving something is simple is difficult, and it tends to involve lots of casework.

Definition. A finite group G is solvable if there exist subgroups $G_i \leq G$ such that

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

and G_i/G_{i-1} is abelian.

In some sense, this offers a decomposition into abelian groups.

All abelian groups are clearly solvable, as are many others: $\{1\} \trianglelefteq \langle r \rangle \trianglelefteq D_{2n}$, and $D_{2n}/\langle r \rangle \cong \mathbb{Z}/2\mathbb{Z}$. However, nonabelian simple groups aren't solvable.

Claim. S_5 is another example of a group that is not solvable.

Proof. Suppose $\{1\} = G_0 \trianglelefteq \cdots \trianglelefteq G_n = S_5$, and let $G_i' = G_i \cap A_5$.

Then, because conjugation in G_i' is closed, then $\{1\} = G_0' \trianglelefteq G_1' \trianglelefteq \cdots \trianglelefteq G_n' = A_5$. But since A_5 is simple, then $G_i' = A_5$ if $A_5 \leq G_i$, and $G_i' = \{1\}$ otherwise.

But if $A_5 \leq G_i < S_5$, then $G_i = A_5$, because $|A_5 : S_5| = 2$ (by Lagrange's Theorem). Otherwise, if $\sigma \in G_i$, then $\sigma^2 \in G_i \cap A_5 = \{1\}$, so $\sigma = 1$ and $G_i = \{1\}$.

Thus, the decomposition series is $\{1\} \trianglelefteq A_5 \trianglelefteq S_5$, which doesn't work because $A_5/\{1\}$ is not abelian. □

Every polynomial $p(t) = \sum_{j=0}^{n} a_j t^j$ has a group associated with it called the Galois group, $\mathrm{Gal}(p)$. One of the main results of Galois theory is that this group is solvable iff the roots of the polynomial have a formula in radicals (for the more specific notion of this defined above). The Galois group of $p(t) = t^5 - t + 1$ is $\mathrm{Gal}(p) = A_5$, so there is no explicit formula for the solutions of p.

Galois was the first person to use the word group, even though others had used the concept before.

11. Group Actions: 10/17/12

Definition. An action of a group G on a set A is a function $G \times A \to A$ (traditionally written as multiplication, e.g. $(g, a) \mapsto g \cdot a$) such that:

i. $1 \cdot a = a$ for every $a \in A$, and
ii. $(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a)$ for all $a \in A$ and $g_1, g_2 \in G$,

so that the group action reflects the group structure.

Grammatically, one says that G acts on A, even though the action is not an inherent property of G.

Example 11.1. 1. S_n acts on $\{1, \ldots, n\}$. There are many functions for which this works, but the natural one is $\sigma \cdot i = \sigma(i)$. Both axioms are easy to check.

2. S_n also acts on $\{1, \ldots, n\}$ (and in fact, any group can act on any set) by $\sigma(i) = i$. This satisfies the axioms even more trivially.
3. $\mathrm{G}\ell_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by $A \cdot \mathbf{v} = A\mathbf{v}$. In general, if a group G is a group of symmetries of something, it tends to act on that thing in some natural way. In this case, $\mathrm{G}\ell_n(\mathbb{R})$ is the group of symmetries of $\mathbb{R}^n$.

Group actions are useful both in the applications of group theory and in understanding the groups themselves.

There's another way of looking at an action called the permutation representation: given $G \times A \to A$, every $g \in G$ is asociated with an $A \overset{\varphi(g)}{\to} A$ such that $a \mapsto g \cdot a = (\varphi(g))(a)$.

Then, $\varphi(1) = 1_A$ (i.e. the identity map) and $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$. Thus, $\varphi(g^{-1}) = \varphi(g)^{-1}$, so all of the $\varphi(g)$ are bijections. This means that $\varphi(g) \in S_A$ (i.e. the symmetric group of A) and $\varphi : G \to S_A$ is a homomorphism. [13]

Conversely, given a $\varphi : G \to S_A$, one can define a group action by $g \cdot a = (\varphi(g))(a)$.

Definition. Let G act on A. The stabilizer of an $a \in A$ is $G_a = \{g \in G \mid g \cdot a = a\}$.

Lemma 11.1. *The stabilizer is a subgroup of G for any $a \in A$.*

(This is proved by simply checking the axioms.)

Example 11.2. Using S_n acting on $\{1, \ldots, n\}$ as in Example 11.1, the natural action gives $G_n \cong S_{n-1}$; the trivial action gives $G_n = S_n$.

This example indicates that G_s is not always normal.

Definition. The orbit of $a \in A$ is $G \cdot a = \{g \cdot a \mid g \in G\} \subseteq A$.

If there exists an $a \in A$ such that $G \cdot a = A$, then the action is called transitive.

For example, $S_n \cdot n = S_n$ in the natural action.

Theorem 11.2 (Orbit-Stabilizer)**.** *If G acts on A and $a \in A$, there is a bijection $G/G_a \to G \cdot a$ given by $gG_a \mapsto g \cdot a$.*

The proof (specifically, checking well-definedness, surjectivity, and injectivity) is as in the 1st Isomorphism Theorem.

Even when $G_a \ntrianglelefteq G$, this still works, just as the set of left cosets rather than a group.

Corollary 11.3. *The size of the orbit is equal to the index of the stabilizer group: $|G/G_a| = |G : G_a| = |G \cdot a|$, and if G is finite, then these are all also equal to $|G|/|G_a|$ by Lagrange's Theorem.*

Orbits form a partition of A, since $G \cdot a = G \cdot b$ iff $b \in G \cdot a$, which is also equivalent to $G \cdot a \cap G \cdot b \neq \emptyset$; the proof is as in that for left cosets. In particular, if A is finite, then let $\mathcal{A}$ be a set that contains one representative of each orbit. Then, $|A| = \sum_{a \in \mathcal{A}} |G \cdot a|$ (like in the proof of Lagrange's Theorem).

Thus, $|A| = \sum_{a \in \mathcal{A}} |G : G_a|$. This can be quite useful, often in unexpectedly clever ways:

Proof of Theorem 7.9. We want to show that if $p \mid |H|$ for some prime p, then there is an $x \in H$ such that $|x| = p$.

Let $G = \mathbb{Z}/p\mathbb{Z}$ act on $A = \{(x_0, \ldots, x_n) \in H^p \mid \prod_{i=0}^{p-1} x_i = 1\}$, where $\bar{n} \cdot (x_0, \ldots, x_{p-1}) = (x_{\bar{n}}, \ldots, x_{\overline{n+p-1}})$ (i.e. moving everything around: an action might send $(1, 2, 3, 4)$ to $(\ , 1, 2, 3) 4$ to $(4, 1, 2, 3)$).

This is well-defined, and one can straightforwardly prove that it's an action.

The stabilizer of $a \in A$ must be either $\{1\}$ or G, since G is simple. In particular, $G_a = G$ if $x_0 = \cdots = x_{p-1}$, and otherwise, only the identity preserves them, so $G_a = \{1\}$.

Thus, $|A| = \sum_{a \in \mathcal{A}} = |H|^{p-1} \equiv 0 \bmod p$. But, since $|G : G_a| = 1$ or p, this is either 0 or $1 \bmod p$. Thus, $|A| \equiv |\{a \in \mathcal{A} \mid G_a = G\}| = |\{(x, \ldots, x) \mid x^p = 1\}|$. Obviously, $(1, \ldots, 1)$ is in this set, but since its order is $0 \mod p$, then there must be at least one other element, so there is some other $x \in H$ such that $x^p = 1$. □

[13] This is one of the reasons symmetric groups are so interesting.

Note that this proof was not Cauchy's original proof; he used induction on the number of elements.

Example 11.3. Any group can act on itself in various ways. Consider the action $g \cdot a = ga$, $g, a \in G$.

Theorem 11.4 (Cayley)**.** *Every group is isomorphic to a subgroup of a symmetric group.*

Proof. The permutation representation of G acting on itself in Example 11.3 is an injective homomorphism $G \overset{\varphi}{\to} S_G$, because if $g \in \operatorname{Ker}(\varphi)$, then $\varphi(g) = 1$ in S_G, so $\varphi(g)(h) = h$, so $g = 1$. Thus, the kernel of φ is trivial, so it is an injection.

Thus, $G \cong \operatorname{Im}(\varphi) \leq S_G$. □

If G is finite, then this becomes $G \cong H \leq S_{|G|}$ since all symmetric groups on n elements are isomorphic.

This theorem seems like something that would be really useful, but for some reason it doesn't appear in any proofs of things.

12. Applications of Group Actions: 10/19/12

Claim. Suppose G is the group of symmetries of a cube $C = [-1, 1]^3$. Then, $G \cong S_4$.

Proof. let A be the set of lines that intersect a vertex, so that $|A| = 4$, and let G act on A. $|G| = 24$, since each of the 8 vertices is sent to any of the vertices, and then there are 3 possible rotations.

The permutation representation gives $G \overset{\varphi}{\to} S_A \cong S_4$.

Claim. φ is surjective.

Proof. It suffices to prove that any 2-cycle $(a\ b) \in \operatorname{Im}(\varphi)$, since transpositions generate S_4. This requires finding a symmetry that swaps any 2 lines and preserves the rest. This can be done by rotations by 180° around the line that is halfway between the two lines to be swapped. □

Thus, $G/\operatorname{Ker}(\varphi) \cong S_4$ and $|G| = |S_4| = 24$, so $|G|/|\operatorname{Ker}(\varphi)| = 24/|\operatorname{Ker}(\varphi)|$ by lagrange's Theorem, so the kernel is trivial. Thus φ is injective, and thus is an isomorphism, so $G \cong S_4$. □

Similar arguments can be given for the other Platonic solids: the tetrahedron has symmetry group A_4, the octahedron has symmetry group S_4 (since it is dual to the cube; dual polyhedra have the same symmetry group), and the dodecahedron and icosahedron have symmetry group A_5.

In general, group actions can be used to show isomorphisms in this manner.

Example 12.1. If G is a group and $H \leq G$, then G acts on G/H by $g \cdot (aH) = (ga)H$ for $g \in G$, $aH \in G/H$. (Well-definedness is easy to check.)

If $|G : H| = n$, then $G \overset{\varphi}{\to} S_{G/H} \cong S_n$. (Sometimes this is interesting, sometimes not.) Then,

$$\begin{aligned} K = \operatorname{Ker}(\varphi) &= \{g \in G \mid g \cdot (aH) = aH \text{ for all } aH \in G/H\} \\ &= \{g \in G \mid g \in aHa^{-1} \text{ for all } a \in G\} = \bigcap_{a \in G} aHa^{-1} \leq H. \end{aligned}$$

If $|G : H| = 2$, then $\varphi : G \to S_2$, so $2 = |\operatorname{Im}(\varphi)| = |G : K| = |G : H||H : K|$, but $|G : H| = 2$, so $|H : K| = 1$ and $H = \operatorname{Ker}(\varphi) \trianglelefteq G$.

This is a new proof that subgroups of index 2 are normal. But this is interesting because it can be extended: suppose $|G : H| = p$, where p is the smallest prime that divides $|G|$. Then, the same analysis shows that $|H|/|K| \mid (p-1)!$ and $|H|/|K| \mid |H| \mid |G|$, so $|H|/|K| = 1$, since no primes could divide it (they would also have to divide $|G|$ and be strictly less than p). Thus, $|H : K| = 1$, so $H = K \trianglelefteq G$.

In the original proof, 2 is used because it is the smallest prime.

Definition. If p is prime, a p-group is a finite group G such that $|G| = p^\alpha$ for some $a \in \mathbb{N}$.

Theorem 12.1. *Any nontrivial p-group has a nontrivial center.*

Corollary 12.2. *No p group is simple except for $\mathbb{Z}/p\mathbb{Z}$.*

Corollary 12.3. *Every p-group is solvable.*

Proof of Theorem 12.1. Let G act on itself (but let $A = G$ to make the notation clearer, so that G acts on A) by $g \cdot a = gag^{-1}$. That this is a group action is pretty obvious; just check the axioms.

The orbit of an $a \in A$ is $G \cdot a = \{gag^{-1} \mid g \in G\}$ (which is sometimes called the conjugacy class of a) and its stabilizer is $G_a = \{g \mid gag^{-1} = a\} = C_G(a)$.

Thus, similarly to the proof of Cauchy's Theorem, $|G| = \sum_{a \in \mathcal{G}} |G : C_G(a)|$, where $\mathcal{G}$ is the set of conjugacy classes of G, and $|G : C_G(a)| = 1$ iff $C_G(a) = G$, which is also equivalent to $a \in Z(g)$. Otherwise, this would be greater than 1, so it must be divisible by p. Reducing mod p, this gives $0 \equiv \sum_{a \in Z(G)} 1$. $1 \in Z(G)$ trivially, but there must be at least $p - 1$ other elements in the center, so it is nontrivial. □

Corollary 12.4. $|G| = |Z(G) + \sum_{a \in \mathcal{A}(G \setminus Z(G))} |G : C_G(a)|$, *where* $\mathcal{A}(G \setminus Z(G))$ *is the set of conjugacy classes of* $G \setminus Z(G)$.

This leads to the question of Sylow's Theorem: how is a finite group "built out of p-groups," where p is a prime divisor of $|G|$?

13. Sylow's Theorems: 10/22/12

Definition. The group action of G on itself in which $g \cdot a = gag^{-1}$ is called the conjugation action.

Sylow was (unusually) a high-school teacher when he proved these theorems.

Suppose p is prime, G is a finite group, and $|G| = p^\alpha m$, where $(p, m) = 1$ (i.e. p^α is the largest possible power of p that still divides the order of G). By Lagrange's Theorem, if $P \leq G$, then $|P| \mid p^\alpha$.

Definition. $P \leq G$ is a Sylow p-subgroup if $|P| = p^\alpha$.

Example 13.1. $\langle r^2 \rangle \leq D_{12}$ is a Sylow 3-subgroup (and in fact is the only one).

$\langle r^3, s \rangle$ is a Sylow 2-subgroup (since it has order 4). Other Sylow 2-subgroups of D_{12} include $\langle r^3, sr \rangle$, or any $\langle r^3, g \rangle$ where $|g| = 2$ (since $r^3 \in Z(D_{12})$).

Notationally, the set of Sylow p-subgroups of G is denoted $\mathrm{Syl}_p(G)$, and the number of them is $n_p(G) = |\mathrm{Syl}_p(G)|$. thus, $n_3(D_{12}) = 1$, $n_2(D_{12}) = 3$, and $\mathrm{Syl}_p(D_{12}) = \{\{1\}\}$ when $p \geq 5$ (though the last example is less interesting).

If $P \in \mathrm{Syl}_p(G)$, then $gPg^{-1} \in \mathrm{Syl}_p(G)$, so this defines an action of G on $\mathrm{Syl}_p(G)$ in which $g \cdot P = gPg^{-1}$. Also, if $P \leq H \leq G$ and $P \in \mathrm{Syl}_p(H)$, then $P \in \mathrm{Syl}_p(G)$ by Lagrange's Theorem.

Using this action, the stabilizer of $P \in \mathrm{Syl}_p G$ is $\{g \mid gPg^{-1} = P\} = N_G(P)$. Additionally, $\mathrm{Syl}_p(G)$ is one orbit, so $|\mathrm{Syl}_p(G)| = |G : N_G(P)| \mid |G|$.

Theorem 13.1 (Sylow)**.** *Suppose G is finite and p is prime. Then,*

(1) $\mathrm{Syl}_p(G) \neq \emptyset$,
(2) If $P, Q \in \mathrm{Syl}_p(G)$, then there exists a $g \in G$ such that $gPg^{-1} = Q$, and
(3) $n_p(G) \equiv 1 \bmod p$.

Continuing Example 13.1, one can conclude that $n_3(G) \equiv 1 \bmod 3$ and $n_3 \mid 4$, so $n_3 = 1$ or 4. Then, $P = \langle r^2 \rangle \trianglelefteq D_{12}$ implies $N_G(P) = G$, so $|D_{12} : N_{D_{12}}(\langle r^3 \rangle)| = 1$, so P is the only Sylow 3-subgroup. (A Sylow p-subgroup is normal iff it is the only such subgroup, by Sylow's Theorem.)

Similarly, $n_2(D_{12}) = 1$ or 3, but we have two examples, so $n_2(D_{12}) = 3$.

This stategy is fairly typical: one finds which options satisfy the conditions and rules the incorrect ones out.

Proof of Theorem 13.1. Part 1: Proof by induction on $|G|$, where p is fixed, so that $|G| = p^\alpha m$.

If $\alpha = 0$, then $\{1\} \in \mathrm{Syl}_p(G)$, and if $\alpha = 1$, then Cauchy's Theorem shows such a Sylow p-subgroup exists.

Case 1. $p \mid |Z(G)|$. Choose an $x \in Z(G)$ such that $|x| = p$. Then, $\langle x \rangle \trianglelefteq G$, so $G \xrightarrow{\pi} G/\langle x \rangle$ is a homomorphism. Thus, by Lagrange's Theorem, $|G/\langle x \rangle| = p^{\alpha-1} m$, so by the inductive assumption, $G/\langle x \rangle$ has a Sylow-p subgroup Q. Thus, $P = \pi^{-1}(Q) \trianglerighteq \langle x \rangle$. Since $\pi : P \to Q$ is a surjection and $\mathrm{Ker}(\pi) = \langle x \rangle$, then $Q \cong P/N$, so $|P| = |\langle x \rangle||Q| = p(p^{\alpha-1}) = p^\alpha$, so $P \in \mathrm{Syl}_p(G)$.

Case 2. $p \nmid |Z(G)|$ will be proved in the next lecture.

Part 2: Cook up an action of G on G/P by $g \cdot (aP) = (ga)P$, and restrict this to Q: $g \cdot (aP) = (ga)P$ where $g \in Q$.

The stabilizer of a $gP \in G/P$ is $\{q \in Q \mid q \cdot (gP) = gP\} = gPg^{-1}$.

Since the stabilizer has index 1, then if $\mathcal{G}$ is a set that includes one element of each orbit of G/P, then $|G/P| = \sum_{g \in \mathcal{G}} |Q : Q_{gP}|$. Each of the entries in this sum is either 1 or is 0 mod p, but $\frac{p^\alpha m}{p^\alpha} = m = |G/P| \not\equiv 0 \bmod p$, so there has to be some $gP \in G/P$ such that $Q_{gP} = Q$, so $Q \leq gPg^{-1}$.

Since Q is also a Sylow-p subgroup, then it has the same number of elements as P, so $Q = gPg^{-1}$.

14. More on Sylow's Theorems: 10/26/12

One of the uses of Part 2 of Sylow's Theoem is that finding all of the Sylow p-subgroups is no more difficult than finding one of them; then, just conjugate it with everything. Additionally, by Part 3, $n_p(G) = |G : N_G(P)|$, so $n_p(G) \mid m$.

Continuing with the proof: consider Case 2 of the proof of Part 1, in which $|Z(G)| \not\equiv 0 \bmod p$, so there exists some $a \in G \setminus Z(G)$ such that $0 \not\equiv |G : C_G(a)| \bmod p$.

But $|G : C_G(a)| = |G|/|C_G(a)| \in \mathbb{Z}$ by Lagrange's Theorem. Since $|G| = p^\alpha m$ and $|G : C_G(a)| \nmid p$, then $p^\alpha \mid |C_G(a)|$. However, since $G \setminus Z(G)$ is nonempty, then $C_G(a) < G$, so by the inductive assumption, pick a $P \in \mathrm{Syl}_p(C_G(a))$. Thus, $P \leq C_G(a) \leq G$, and since $p^\alpha \mid |C_G(a)|$, then $p^\alpha \mid |P|$ and $p^{\alpha+1} \nmid |P|$, so $P \in \mathrm{Syl}_p(G)$.

This proof is very nonconstructive — so nonconstructive that in the absence of any other information, it's often better to just guess and check to find a Sylow p-subgroup.

Corollary 14.1. $\mathrm{Syl}_p(G) = \{P\}$ *iff* $P \trianglelefteq G$*.*

Corollary 14.2. *Since* $P \trianglelefteq N_G(P) \leq G$*, then* $\mathrm{Syl}_p(N_G(P)) = \{P\}$ *if* $P \in \mathrm{Syl}_p(G)$*.*

The proof can now be finished, and Part 3 can be shown:

Consider the action $G \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G)$ given by $(g, P) \mapsto gPg^{-1}$. It is easy to check that this is an action. By Part 2, this action is transitive, so there is only one orbit. Thus,

$$\begin{aligned} |\mathrm{Syl}_p(G)| &= |G : G_P| \text{ for some } P \in \mathrm{Syl}_p(G) \\ &= |G : N_G(P)| \text{ by the proof of Part 1.} \end{aligned}$$

Restrict this to an action $P \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G)$, where $(g, Q) \mapsto gQg^{-1}$. Now, there is more than one orbit, so counting orbit by orbit is more meaningful.

The stabilizer of a $Q \in \mathrm{Syl}_p(G)$ is $\{g \in P \mid gQg^{-1} = Q\} = P \cap N_G(Q) \leq P$, and the two are equal iff $P \subseteq N_G(Q)$ (i.e. $P \leq N_G(Q)$).

Since $Q \trianglelefteq N_G(Q) \leq G$, then $P, Q \in \mathrm{Syl}_p(N_G(Q))$, so $P = Q$ by Corollary 14.1 and $|P| = |Q| = p^\alpha$.

Thus, the stabilizer of Q in $\mathrm{Syl}_p(G)$ is P if $P = Q$ and a strict subgroup of P otherwise, so the orbit of Q has size 1 if $P = Q$ and is equal to 0 mod p otherwise.

Overall, one orbit has size 1 and the rest are congruent to 0 mod p, so $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$. □

A typical application of Sylow's Theorem is to deduce things about a group given its order.

Example 14.1. Suppose $|G| = pq$ for distinct primes p and q. Then, G is not simple.

Proof. Without loss of generality assume $p < q$, and pick a $Q \in \mathrm{Syl}_q(G)$ (which is guaranteed by Part 1). Then, $n_q(G) \equiv 1 \bmod q$, so $n_q(G) \mid p$ (since it doesn't divide q). Thus, $n_q(G) = 1$, so $Q \trianglelefteq G$ by Corollary 14.1. □

Example 14.2. If $|G| = p^2 q$, where p and q are distinct primes, then G is not simple.

The proof of this can be found in the book.

Exercise 14.1. How many Sylow-2 subgroups does A_5 have?

Results such as this eventually lead to the following:

Theorem 14.3. *If* $|G| = 60$ *and* G *is simple, then* $G \cong A_5$*.*

Proof. First, factor 60 as $2^2 \cdot 3 \cdot 5$, and look at the Sylow-2 subgroups.

$n_2(G) \mid 15$, but $n_2(G) > 1$, since G is simple. Suppose $n_2(G) = 3$.

Then, G acts transitively on $\mathrm{Syl}_2(G)$, so if $n_2(G) = 3$, then there is a homomorphism $G \overset{\varphi}{\to} S_3$ such that $\mathrm{Ker}(\varphi) \triangleleft G$, so $\mathrm{Ker}(\varphi) = \{1\}$ (since G is simple). Thus, φ is injective, which is impossible, because $|S_3| < |G|$.

If $n_2(G) = 5$, then $N = N_G(P) \leq G$ has index 5. Then, G acts on G/N with $g \cdot aN = (ga)N$. This leads in the same way to a nontrivial homomorphism with trivial kernel. However, consider the diagram

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[dr, dashed, "\varphi\circ\varepsilon"'] & S_5 \arrow[d, "\varepsilon"] \\ & \{\pm 1\}, \end{tikzcd}$$

so that $\mathrm{Ker}(\varepsilon \circ \varphi) = G$. Thus, φ is an injection, so $G \cong A_5$. □

15. Direct Products: 10/29/12

If G is simple and $\varphi : G \to H$ is a homomorphism, then since $\text{Ker}(\varphi) \trianglelefteq G$, then φ is either injective or trivial.

Some Sylow-2 subgroups for A_5 are of the form $H = \{1, (a\ b)(c\ d), (a\ c)(b\ d), (a\ d)(b\ c)\}$ for various $a, b, c, d \in \{1, \dots, 5\}$. Thus, $N_{A_5}(H) \geq K \cong A_4$, where K is the subgroup of even permutations of $\{1, \dots, 4\}$ in A_5.

Thus, $|N_{A_5}(H)| \geq 12$, so $|N_{A_5}(H) : A_5| \leq 60/12 = 5$, so $n_2(A_5) \leq 5$ and thus must be equal to 5.

Recall that for Theorem 14.3, it was shown that if $|G| = 60$ and G is simple, then $G \cong A_5$ or $n_2(G) = 15$. Technically, this last case needs to be dealt with, so suppose $n_2(G) = 15$.

Claim. There exist $P, Q \in \text{Syl}_2(G)$ such that $|P \cap Q| = 2$.

Proof. Suppose not; then, the 15 elements $P_1, \dots, P_{15} \in \text{Syl}_2(G)$ must have $P_i \cap P_j = \{1\}$ for all $i \neq j$ (since $|P_i| = 4$ for all i). This means there are 45 elements of order 2 or 4 in G.

Now look at the Sylow-5 subgroups: $n_5(G) \mid 12$ and $n_5(G) \equiv 1 \bmod 5$, so $n_5(G) = 6$ (since if it were 1, then G wouldn't be simple). Since all groups of order 5 are cyclic, then all of these groups are distinct except for the identity (otherwise, a non-identity element they have in common would generate both groups). Thus, there are 24 elements of order 5. But $45 + 24 > 60$, which creates a contradiction. □

Thus, choose P, Q such that $P \cap Q = \{1, x\}$. Since $|P| = |Q| = 4$, then P and Q are abelian. Let $M = C_G(x)$, so that $P, Q \leq M < G$ (since G has no interesting normal subgroups).

Thus, $4 \mid |M|$, $|M| \mid 60$, and $4 < |M| < 60$. Additionally, $|G : M| \neq 2, 3$, or 4 since G acts transitively on G/M (and this could be used to establish an injection from G into S_k with $k = 2, 3$, or 4, which is a problem).

Thus, $|M| = 12$ and $|G : M| = 5$. Again, G acts transitively on G/M, so there is a homomorphism $G \to S_5$, which implies (by the same argument as in the previous case) implies $G \cong A_5$. □

Note that this last case can't actually happen, since the isomorphism is between groups with different numbers of Sylow-2 subgroups. But viewing it as a proof by contradiction makes the theorem just as valid.

Just as there are ways of decomposing groups, one can use direct products to construct groups. Some groups are isomorphic to the direct product of two smaller groups, even though it isn't clear from the definition: $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, given by $\bar{x} \mapsto (\bar{x}, \bar{x})$ (where these three bars mean the equivalency classes in $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/4\mathbb{Z}$ respectively for a given $x \in \mathbb{Z}$), and $D_{12} \cong D_6 \times \mathbb{Z}/2\mathbb{Z}$.[14]

How can one recognize whether this happens? It was shown that if $\tilde{A}, \tilde{B} \leq A \times B$ (where $A \cong \tilde{A} = \{(a, 1) \mid a \in A\}$ and $\tilde{B}$ is given similarly), then $\tilde{A}, \tilde{B} \trianglelefteq A \times B$.

Thus, if $G \cong H \times K$, then there are two normal subgroups of G whose intersection is the identity. Thus, simple groups cannot be written as direct products in a nontrivial way. Some non-simple ones also have this property, such as D_{10}.

Definition. If $H, K \leq G$, then $HK = \{hk \mid h \in H, k \in K\} \subseteq G$.

HK is not necessarily a subgroup of G, and the map $f : H \times K \to G$ given by $(h, k) \mapsto hk$ (such that $\text{Im}(f) = HK$) is usually not an isomorphism.

Theorem 15.1. *If $H, K \trianglelefteq G$ and $H \cap K = \{1\}$, then $HK \leq G$ and $H \times K \cong HK$ via the isomorphism f given above.*

Example 15.1. In D_{12}, let $H = \langle r^2, s \rangle$ and $K = \langle r^3 \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Then, $H \cap K = \{1\}$, and $K \leq Z(G)$, so that $K \trianglelefteq G$, and one can check that $H \trianglelefteq G$.

Thus, $H \times K \cong HK \leq G$, but $|HK| = |G|$, so $HK = G$. Thus, $H \times K \cong G$.

Proof of Theorem 15.1. Let $h \in H$, $k \in K$, and consider their commutator $hkh^{-1}k^{-1}$.

Since $K \trianglelefteq H$, then $hkh^{-1} \in K$, and similarly $kh^{-1}k^{-1} \in H$, so $hkh^{-1}k^{-1} \in H \cap K = \{1\}$, so $hkh^{-1}k^{-1} = 1$, so $hk = kh$.

Given this, it is possible to check that f is a homomorphism. Then, $\text{Ker}(f) = \{(h, k) \mid hk = 1\}$, which implies that $h = k^{-1}$, so $h = k = 1$ since $h, k \in H \cap K$.

Thus, f is injective, since its kernel is trivial, so it is an isomorphism onto its image. □

There is a related notion called the semidirect product except that it doesn't require K to be normal in G, but rather just a subgroup. Then, $HK \leq G$, but $HK \ncong H \times K$ in all cases. Instead, one writes $HK \cong H \rtimes K$.

Example 15.2. If $|G| = pq$, for distinct primes p, q with $p < q$, then pick a $P \in \text{Syl}_p(G)$ and a $Q \in \text{Syl}_q(G)$, so that $P \cap Q = \{1\}$, $P \trianglelefteq G$, and $Q \leq G$. Thus, $G \cong P \rtimes Q$.

Since P and Q are both cyclic, this is the complete classification of groups of order pq for distinct primes p and q.

[14] One also has $G \cong G \times \{1\}$, but this is usually not included, since it is not very interesting.

16. Introduction to Rings: 10/31/12

Recall that groups arose as symmetries of things. By contrast, rings occur in many different contexts, but can be thought of as numbers. In this case, they are more algebraic than groups.

The prototypical example of a ring is $\mathbb{Z}$ withn the usual operations of addition and multiplication, but this is slightly deceptive: the integers are better behaved than some other rings.

Definition. A ring R is a set with two binary operations $+, \times : R \to R$ such that:

i. $(R, +)$ is an abelian group,
ii. $\times$ is associative: $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$, and
iii. $+$ and $\times$ are distributive: $a \times (b + c) = a \times b + a \times c$, and $(a + b) \times c = a \times c + b \times c$ for all $a, b, c \in R$.

Multiplication is often denoted ab or $a \cdot b$ if it is clear what this means; however, addition never is, even if the underlying group would be written multiplicatively.

Notice that the mutiplication operation doesn't require the existence of an identity[15] or inverses, and it is not commutative in general.

Example 16.1. Many examples of rings will be familiar:

- $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ under the usual addition and multiplication.
- $M_n(\mathbb{R})$, under the usual addition and matrix multiplication. Not all elements have inverses.
- $2\mathbb{Z} \subset \mathbb{Z}$ (i.e. the even numbers). Notice that this ring has neither identity nor inverses.
- The "trivial ring" or "stupid ring" $\{0\}$ where $0 + 0 = 0 \times 0 = 0$.

Definition. A ring R has identity (or has 1) if there is a $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

Definition. A ring R is commutative if $ab = ba$ for all $a, b \in R$.

All the rings in Example 16.1 are commutative except for $M_n(\mathbb{R})$ when $n \geq 2$.

Lemma 16.1. *If a ring R has identity, then the identity is unique.*

The proof is just as in the corresponding proof for groups.

Some more notation: the additive identity is usually denoted 0, and the multiplicative identity (if it exists) is written 1. The additive inverse of $a \in R$ is denoted $-a$.

Lemma 16.2. *If $a, b \in R$, then*

i. $0 \cdot a = a \cdot 0 = 0$.
ii. $-a \cdot b = a \cdot -b = -(ab)$.
iii. $(-a)(-b) = ab$.

These proofs are by direct application of the axioms: for example,

Proof of i. Since $0 + 0 = 0$, then $a(0 + 0) = a \cdot 0$, so $a \cdot 0 + a \cdot 0 = a \cdot 0$, so $a \cdot 0 = 0$ (subtracting $a \cdot 0$ on both sides). □

Thus, if $1 = 0$ in any ring R with identity, then R is the trivial ring, since $a \cdot 0 = a \cdot 1 = 0 = a$.

Definition. A subring S of a ring R is a subgroup of $(R, +)$ that is closed under multiplication (i.e. if $a, b \in S$, then $ab \in S$ as well).

Example 16.2. Again, many of these examples will be familiar:

- $\mathbb{Z}$ in $\mathbb{Q}$ in $\mathbb{R}$ in $\mathbb{C}$.
- $\{0\} \subseteq R$ where R is any ring.
- $2\mathbb{Z} \subseteq \mathbb{Z}$.

There is no standard notaton for subrings, so usually one just writes "S is a subring of R," or such.

Notice that it is possible for a ring to have identity but a subring to lack it, or vice versa; and since $\{0\} \subseteq R$ for any R, then a subring and a ring may both have identity, but with these two identities different.

In general, $(R, \cdot)$ is not a group; that would imply that 0^{-1} exists, and that $1 = 0$, yielding the trivial ring.

Definition. If R is a ring with identity, then an $a \in R$ is a unit if $ab = ba = 1$ for some $b \in R$. The set of units of R is denoted $R^\times$.

[15] . . . sometimes. Different books give different definitions of a ring as requiring an identity or not, which may also affect further definitions or theorems down the line. Be careful!

$R^\times$ is not a subring unless R is trivial (since in general $0 \notin R^\times$), and $(R^\times, +)$ is a group, but not a subgroup of $(R, +)$.

Definition. A division ring is a ring with 1 such that $R^\times = R \setminus \{0\}$.

This is the nicest that multiplication can behave without the ring being trivial.

A field is just a commutative division ring: thus, $\mathbb{C}$ is a field, but $M_n(\mathbb{R})$ is not. (Interestingly, its group of units is $M_n(\mathbb{R})^\times = \mathrm{G}\ell_n(\mathbb{R})$).

$\mathbb{Z}$ is not a division ring, and $\mathbb{Z}^\times = \{\pm 1\}$. In particular, $\mathbb{Z}$ is a subring of the field $\mathbb{Q}$, but it is not a field itself.

A ring homomorphsm is very reminiscent of the corresponding definition for groups:

Definition. Let R, S be rings. A (ring) homomorphism is a map $\varphi : R \to S$ such that for all $a, b \in R$:

i. $\varphi(a + b) = \varphi(a) + \varphi(b)$ (i.e. $\varphi : (R, +) \to (S, +)$ is a group homomorphism), and
ii. $\varphi(ab) = \varphi(a)\varphi(b)$.[16]

One example is $\mathbb{Z} \to \mathbb{R}$ given by $x \mapsto x$. However, most of the group homomorphisms considered thus far (such as $M_n(\mathbb{R}) \overset{\det}{\to} \mathbb{R}$) aren't ring homomorphisms.

Definition. If $\varphi : R \to S$ is a ring homomorphism, then $\mathrm{Im}(\varphi) = \{\varphi(r) \mid r \in R\}$ and $\mathrm{Ker}(\varphi) = \{r \in R \mid \varphi(r) = 0\}$ (which is just the kernel of the underlying group homomorphism).

Claim. The image is a subring of S, and the kernel is a subring of R.

Proof. The proof is for the image, and the proof for the kernel is essentially the same.

Clearly, $\mathrm{Im}(\varphi)$ is closed under addition, and if $x, y \in \mathrm{Im}(\varphi)$, then there exist $a, b \in R$ such that $x = \varphi(a)$ and $y = \varphi(b)$, so $xy = \varphi(ab) \in \mathrm{Im}(\varphi)$. □

In fact, the kernel is better than a subring: if $a \in \mathrm{Ker}(\varphi)$ and $b \in R$, then $\varphi(ab) = 0$, so $ab \in \mathrm{Ker}(\varphi)$, and similarly for ba.

Definition. A subring I of a ring R is:

i. A left ideal if for all $a \in R$ and $b \in I$, $ab \in I$,
ii. A right ideal if for all $a \in R$ and $b \in I$, $ba \in I$, and
iii. An ideal (or two-sided ideal) if it is both a left and a right ideal.

This definition is analogous to the notion of normality in groups.

Thus, the kernel of a ring homomorphism is an ideal. Another example is $2\mathbb{Z} \subset \mathbb{Z}$, and $\mathbb{Z} \subset \mathbb{Q}$ is an example of a subring that isn't an ideal. (Again, there is no compact notation for ideals.)

Similarly to groups, if $I \subseteq R$ is a subring, then R/I will be a ring iff I is an ideal (where $+$ and $\times$ are given naturally).

17. Ring Homomorphisms: 11/2/12

If $I \trianglelefteq (R, +)$, then cosets in the quotient group R/I are denoted $a + I$ for an $a \in R$, since multiplication means something different.

If $R \overset{\pi}{\to} R/I$ is given by the canonical homomorphism of the additive groups, it would be nice to define multiplication in R/I in a way that makes π a ring homomorphism. The only real option is to let $(a + I)(b + I) = ab + I$. It turns out this is well-defined: if $a' + I = a + I$ and $b' + I = b + I$, then

$$ab = ab' + a(b - b') = a(b - b') + a'b' + (a - a')b'.$$

Since $a - a' \in I$ and $b - b' \in I$ (because of the way cosets work), and because I is both a left and a right ideal, then $a(b - b') \in I$ and $(a - a')b' \in I$, so $ab = a'b' + k$ for some $k \in I$. Thus, they lie in the same coset, so coset multiplication is well-defined. Then, the ring axioms are easy to check, and so R/I with these rules of addition and multiplication is called a quotient ring.

Example 17.1. Suppose $n \in \mathbb{Z}$ and $I = n\mathbb{Z}$. Then, I is an ideal of $\mathbb{Z}$, so the quotient ring is the familiar $\mathbb{Z}/n\mathbb{Z}$.

Theorem 17.1 (The First Isomorphism Theorem for Rings)**.** *Let $\varphi : R \to S$ be a ring homomorphism. Then,*

i. $\mathrm{Im}(\varphi)$ is a subring of S.
ii. $\mathrm{Ker}(\varphi)$ is an ideal of R.
iii. $R/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$ given by the isomorphism $a + I \mapsto \varphi(a)$.

[16] Some books additionally stipulate that $\varphi(1) = 1$, which doesn't follow from these axioms, though $\varphi(0) = 0$ does follow.

Everything additively follows from the First Isomorphism Theorem for groups, and multiplicatively, everything works because φ is a ring homomorphism.

Definition. If R is a ring, then $R[x]$ is the set of polynomials over R, given by the set of functions $f : R \to R$ such that $f(x) = \sum_{j=0}^{n} a_j x^j$, with $a_1, \dots, a_n \in R$ and $n \in \mathbb{N}$ (or possibly $n = 0$).

One can define addition and multiplication on $R[x]$: suppose $f, g \in R[x]$ with $f(x) = \sum_{j=1}^{n} a_j x^j$ and $g(x) = \sum_{j=1}^{m} b_j x^j$. Then,

$$(f + g)(x) = \sum_{j=0}^{\max(m,n)} (a_j + b_j)x^j,$$

where $a_j = 0$ if $j > n$ and $b_j > 0$ if $j > m$, and

$$(fg)(x) = \sum_{k=1}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

This is just the usual addition and multiplication of polynomials, and is probably familiar from previous examples of polynomials over $\mathbb{R}$ or $\mathbb{C}$.

Lemma 17.2. *$R[x]$ is a ring under these operations of addition and mulitplication.*

The proof is a bit tedious and not terribly surprising, so it has been omitted.

Example 17.2. Consider the homomorphism $\mathbb{R}[x] \xrightarrow{\varphi} \mathbb{R}$ given by $\varphi(f) = f(0)$. It is easy to check that this is a ring homomorphism. $\operatorname{Im}(\varphi) = \mathbb{R}$ and

$$\operatorname{Ker}(\varphi) = \left\{ \sum_{j=0}^{n} a_j x^j \mid a_0 = 0 \right\} = \{xf(x) \mid f(x) \in \mathbb{R}[x]\}$$

is an ideal.

Then, the First Isomorphism Theorem implies that $\mathbb{R}[x]/\operatorname{Ker}(\varphi) \cong \mathbb{R}$ (and something similar can be done with $f(1)$, etc.).

One can also consider the ring homomorphism $\mathbb{R}[x] \to \mathbb{C}$ given by $f(x) \mapsto f(i)$;[17] this is also a ring homomorphism. Here, $\operatorname{Im}(\varphi) = \mathbb{C}$, and $\operatorname{Ker}(\varphi) = \{(x^2 + 1)f \mid f \in \mathbb{R}[x]\}$, which makes intutive sense but does require some rigor to prove. Thus, the First Isomorphism Theorem shows that $\mathbb{C} \cong \mathbb{R}[x]/\operatorname{Ker}(\varphi)$.

Though the terminology is very suggestive, elementary group theory and elementary ring theory have a lot in common: subgroups correspond to subrings, normal subgroups to ideals, quotient groups to quotient rings, and the First Isomorphism Theorem for groups corresponds to the same-named theorem for rings.

Thus, one could look for an analogue to generators in ring theory. This is not exactly the same, but one can construct the smallest ideal containing a given element or set of elements:

Definition.

$$(A) = \bigcap_{\substack{I \subseteq R \text{ ideal} \\ A \subseteq I}} I.$$

Notationally, one can also write (f) for $(\{f\})$, or $(f_1, \dots, f_n)$ for $(\{f_1, \dots, f_n\})$.

This is pretty clearly an ideal of R, and thus is the smallest ideal containing A, since it is in an intersection including itself.

(A) can be written more explicity as

$$RAR = \left\{ \sum_{j=1}^{n} r_j a_j r_j' \mid r_j, r_j' \in R, a_j \in A, n \in \mathbb{N} \right\}.$$

Lemma 17.3. *$RAR \subseteq R$ is an ideal.*

[17] Even though the polynomial f is over $\mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, so f can be naturally extended into a function $f : \mathbb{C} \to \mathbb{C}$.

This is another lemma that is easy to check, and checking the ideal properties follow nicely from associativity. Additionally, if $A \subseteq I \subseteq R$ with I ideal, then $RAR \subseteq I$, by the absorption property, so $RAR = (A)$.

If R is commutative, $RAR = RA = \{\sum_{j=1}^{n} r_j a_j \mid r_j \in R, a_j \in A, n \in \mathbb{N}\}$. (This set is defined even when R is noncommutative, but is not equal to RAR in that case.) If additionally $A = \{f\}$ for some $f \in R$, then $RA = \{r_1 f + \cdots + r_n f\} = \{(r_1 + \cdots + r_n)f\}$, so $(f) = \{rf \mid f \in R\}$.

Example 17.3. If $\mathbb{R}[x] \xrightarrow{\varphi} \mathbb{R}$ is as in Example 17.2, then $\operatorname{Ker}(\varphi) = (x)$, and in the second homomorphism, $\mathbb{R}[x] \to \mathbb{C}$, $\operatorname{Ker}(\varphi) = (x^2+1)$. Thus, $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$.

In general, modding out polynomial rings is a good way to forge interesting new rings.

18. The Chinese Remainder Theorem: 11/5/12

Today's lecture was by Dr. Akshay Venkatesh.

Theorem 18.1 (Chinese Remainder Theorem)**.** *Given two relatively prime integers p and q, one can always find an integer x with prescribed residues* $\bmod p$ *and* $\bmod q$*.*

The words "prescribed residues" mean that there is an x such that $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$. For example, if $x \equiv 4 \pmod{6}$ and $x \equiv 4 \pmod{7}$, then $x = -3, 39, 81 \dots$

There is a similar theorem for more than 2 p, q, but it's a fairly straightforward generalization.

The CRT has a generalization in terms of ring theory:

Definition. If I and J are ideals of a commutative ring with 1 R, then the product ideal of I and J is

$$IJ = \left\{ \sum_{k=1}^{n} i_k j_k \mid i_k \in I, j_k \in J \right\},$$

so that IJ is closed under addition.

Theorem 18.2 (Chinese Remainder Theorem for Ideals)**.** *Suppose R is a commutative ring with 1 and I and J are ideals of R such that $I + J = R$ (where $I + J = \{i + j \mid i \in I, j \in J\}$). Then, $R/IJ \cong R/I \times R/J$.*

More precisely, if $r \in R$, then $r + IJ \mapsto (r+I)(r+J)$ is an isomorphism. This is useful because R/IJ tends to be larger than R/I and R/J, so computations can be simplified with this decomposition.

The CRT for ideals also has a generalization for more than 2 ideals, but this is what one might expect: $R/\left(\prod_{k=1}^{n} I_k\right) \cong \prod_{k=1}^{n} R/I_k$.

Example 18.1. Consider the ring $\mathbb{Z}$ and let $I = (p)$ and $J = (q)$ for primes p and q. Then, since p and q are relatively prime, $I + J = \mathbb{Z}$. This means that $\mathbb{Z}/(pq) \cong \mathbb{Z}/(p) \times \mathbb{Z}/(q)$, so $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. This implies the narrow version of the theorem; in the example given, $\mathbb{Z}/(42) \cong \mathbb{Z}/(6) \times \mathbb{Z}/(7)$ via the isomorphism $(13 \bmod 42) \mapsto (1 \bmod 6, 6 \bmod 7)$.

Exercise 18.1. In the above example, it was asserted that $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$ because p and q are relatively prime. Why does the one follow from the other?

Similarly, if $p_1, \dots, p_n$ are relatively prime, then

$$\mathbb{Z}/\left(\prod_{i=1}^{n} p_i\right) \cong \prod_{i=1}^{n} \mathbb{Z}/(p_i),$$

which is nice because large numbers such as $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ can be factored when computing in ideals, making the ring much better behaved.

Example 18.2. Consider the ring $\mathbb{C}[x]$. Pick some complex numbers $\alpha_1, \dots, \alpha_n \in \mathbb{C}$, and let $I_k = (x - \alpha_k)$ for $1 \le k \le n$. In other words, $I_k = \{f \in \mathbb{C} \mid f(\alpha_k) = 0\}$. As long as the α_j are distinct, $I_i + I_j = R$. One can apply the many-ideal version of the CRT to this.

In fact, $R/I_k \cong \mathbb{C}$ as a ring (which was a consequence of the First Isomorphism Theorem for rings), so the Chinese Remainder Theorem says that $R/\prod_{k=1}^{n} I_k \cong \mathbb{C}^n$ via the explicit isomorphism

$$f + \prod_{k=1}^{n} I_k \mapsto (f(\alpha_1), \dots, f(\alpha_n)).$$

The surjectivity of this isomorphism implies that for any $t_1, \dots, t_n \in \mathbb{C}$, there exists a polynomial $f \in \mathbb{C}[x]$ such that $f(\alpha_k) = t_k$ for all k. This gives a polynomial interpolation formula that seems quite unrelated to the CRT for integers on the surface.

Exercise 18.2. Again, why is $I_i + I_j = R$ if $\alpha_i \neq \alpha_j$ in the above example?

Proof of Theorem 18.2. Define $\varphi : R \to R/I \times R/J$ such that $\varphi(r) = (r + I, r + J)$. It is easy to show that φ is a ring homomorphism.

Claim. $\text{Ker}(\varphi) = IJ$ and $\text{Im}(\varphi) = R/I \times R/J$.

Proof. If $r \in \text{Ker}(\varphi)$, then $r + I = 0$ in R/I, so $r \in I$. Similarly, $r \in J$ by the same line of reasoning. Thus, $r \in I \cap J$. While in general $IJ \neq I \cap J$ (as in $I = J = (2) \subseteq \mathbb{Z}$), we also have that $I + J = R$:

- If $x \in IJ$, then $x \in I$ and $x \in J$ by the absorption property, so $x \in I \cap J$.
- If $x \in I \cap J$, then $x = x \cdot 1 = x(i + j)$ for some $i \in I$ and $j \in J$, since $1 \in I + J = R$. Since $i + j \in IJ$, then $x \in IJ$ as well.

Thus, $\text{Ker}(\varphi) = IJ$.

The case of the image is similar to the CRT for integers: for $r, x, y \in R$ the goal is to find a solution where $r \equiv x \bmod I$ and $r \equiv y \bmod J$, in a sense (though this notation isn't standard).

Again, start with $1 = i + j$ for an $i \in I$ and a $j \in J$. Then,

$$\varphi(i) = (i + I, i + J) = (0, (i + j) - j + J) = (0, 1 + J) = (0, 1),$$

and similarly $\varphi(j) = (1, 0)$. Thus, for any $x, y \in R$, $\varphi(xj + yi) = (x + I, y + J)$, so φ is surjective, since every element in $R/I \times R/J$ is of this form. □

Thus, the theorem itself falls out as a result of the First Isomorphism Theorem for rings. □

Exercise 18.3. Trace through this proof in the case of Example 18.2 in order to obtain the explicit polynomial interpolation formula.

19. Integral Domains and Maximal Ideals: 11/7/12

Definition. Let R be a ring with identity $1 \neq 0$. An element $a \in R$ is a zero divisor if $a \neq 0$ and there exists a $b \in R \setminus \{0\}$ such that $ab = 0$ or $ba = 0$.

Definition. An integral domain is a commutative ring with identity $1 \neq 0$ that has no zero divisors.

This means that if $ab = 0$, then $a = 0$ or $b = 0$. An integral domain is not a field, but it's a step in that direction.

$\mathbb{Z}$ is an integral domain, though $\mathbb{Z}/6\mathbb{Z}$ isn't: $2 \cdot 3 = 0$.

Claim. A zero divisor cannot be a unit.

Proof. If $ac = 1$ and $ab = 0$, then $abc = 0 = b(1)$, so $b = 0$, which is a contradiction. □

If F is a field, then $F^\times = F \setminus \{0\}$, so fields don't have zero divisors. Thus they are integral domains. There are plenty of integral domains that aren't fields, however, such as $\mathbb{Z}$.

Integral domains also allow for cancellation: one can divide in fields, but in an integral domain, one has $ab = ac$ implies $b = c$ if $a \neq 0$. This is meaningful because a^{-1} might not exist.

(The full proof is that since $ab = ac$, then $a(b - c) = 0$, so either $a = 0$ or $b - c = 0$.)

For the rest of this lecture, all rings will be commutative and have an identity $1 \neq 0$. Then, one can ask for a ring R, which ideals $I \subseteq R$ make R/I a field, an integral domain, etc.?

Example 19.1. Any ideal $I \subseteq \mathbb{Z}$ is an additive subgroup, so $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Then, $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime, and $\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff n is prime or $n = 0$ (since $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$).

Definition. An ideal $I \subsetneq R$ is maximal if the only ideals $J \subseteq R$ such that $I \subseteq J$ are $J = I$ an $J = R$.

For example, $6\mathbb{Z} \subseteq \mathbb{Z}$ is not maximal because $6\mathbb{Z} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}$. $2\mathbb{Z} \subseteq \mathbb{Z}$ is maximal, however. In general, the maximum ideals of $\mathbb{Z}$ are $p\mathbb{Z}$ with p prime.

Lemma 19.1. *Suppose R is a ring.*

i. Let $I \subseteq R$ be an ideal. Then, $I = R$ iff $I \cap R^\times \neq \emptyset$ (i.e. I contains a unit), and
ii. R is a field iff $\{0\}$ is maximal.

Proof. Part i:

$\Rightarrow$: completely obvious, since $1 \in R^\times$ and $1 \in R = I$.
$\Leftarrow$: If $x \in R$, then $1 \cdot x = x \in I$, so $I = R$.

Part ii:

- $\Rightarrow$: If $\{0\} \subsetneq J \subseteq R$ is an ideal, then $R^\times = R \setminus \{0\}$, which implies that J contains a unit, so $J = R$ by Part i.
- $\Leftarrow$: If $\{0\} \subseteq R$ is maximal, let $x \in \mathbb{R} \setminus \{0\}$ and let $J = (x)$, so that $\{0\} \subsetneq J \subseteq E$, so that $J = R$ (since $\{0\}$ is maximal). Then, $1 \in J$, so x is a unit (since $J = \{rx \mid r \in R\}$). □

The Second Isomorphism Theorem (sometimes called the Lattice Isomorphism Theorem) for rings is much more useful than the corresponding theorem for groups:

Theorem 19.2 (Second Isomorphism Theorem for Rings)**.** *Suppose R is a ring and $I \subseteq R$ is an ideal. Then, the projection $R \xrightarrow{\pi} R/I$ gives a bijection between the ideals $\bar{J} \subseteq R/I$ and the ideals $J \subseteq R$ such that $I \subseteq J$ given by $J \subseteq R \mapsto J/I$ with $I \subseteq J$, and $\bar{J} \mapsto \pi^{-1}(J)$.*

The proof of this theorem involves checking a lot of not too difficult things, but is somewhat complicated.

Proposition 19.3. *$I \subseteq R$ is maximal iff R/I is a field.*

Proof. R/I is a field iff $\{0\} \subseteq R/I$ is maximal, which is true iff the only ideals of R/I are $\{0\}$ and R/I. Thus, I is maximal iff I and R are the only ideals of R. □

As a corollary, $n\mathbb{Z} \subseteq \mathbb{Z}$ is maximal iff n is prime. Similarly, since $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, then (x^2+1) is maximal, since $\mathbb{C}$ is a field.

Now, what about integral domains?

Definition. A prime ideal of a ring R is an ideal $I \subseteq R$ such that for all $a, b \in R \setminus I$, then $ab \in R \setminus I$.

For example, $2\mathbb{Z} \subseteq \mathbb{Z}$ is prime. Note that R is not considered a prime ideal of itself.

Proposition 19.4. *If $I \subseteq R$ is an ideal, then R/I is an integral domain iff I is prime.*

Proof. In the forward direction, let $a, b \in R \setminus I$, so that $a + I, b + I \in (R/I) \setminus \{0\}$. Then, since R/I is an integral domain, $ab + I \in (R/I) \setminus \{0\}$, so $ab \notin I$.

The reverse is similar. □

Corollary 19.5. *If $I \subseteq R$ is maximal, then I is prime.*

The converse is false: $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ is in an integral domain that is not a field, so $0\mathbb{Z}$ is prime but not maximal. (This makes sense: $0\mathbb{Z} \subseteq n\mathbb{Z}$ for any $n \in \mathbb{Z}$.)

20. PIDs and UFDs: 11/9/12

Again, for this lecture assume R is a commutative ring with identity $1 \neq 0$ for the extent of this lecture.

Definition. Let R be an integral domain. An element $r \in R$ such that $r \neq 0$ and $r \notin R^\times$ is reducible if there exist $a, b \in R \setminus \{1\}$ such that $r = ab$.

r is irreducible if $r = ab$ implies that one of a and b is a unit.

The irreducible elements of a ring are the analogue of primes in $\mathbb{Z}$ (as well as the negative primes, since they are irreducible elements as well).

Definition. If $r \in R$ such that $r \neq 0$ and $r \notin R^\times$, then r is prime if (r) is a prime ideal.

This coincides with the definition of prime already seen in $\mathbb{Z}$. In particular, $r \in \mathbb{Z}$ is irreducible iff r is prime. In general, this is not true, and one may have irreducible elements which are not prime. However, all primes are irreducible:

Lemma 20.1. *If r is prime, then r is irreducible.*

Proof. Let $r \in R$ be prime, so that (r) is a prime ideal. If $r = ab$, then $ab \in (r)$. Since (r) is prime, then at least one of a or b is in (r). Without loss of generality, suppose that $a \in (r)$, so that $a = rx$ for some $x \in R$. Thus, $a = abx$, so $bx = 1$, so $b \in R^\times$, since integral domains allow cancellation. □

Definition. An integal domain is a unique factorization domain (UFD) if any $r \in R$ that is not 0 and not a unit can be written as $r = p_1 p_2 \ldots p_n$, where the $p_i \in R$ are irreducible, and that this is unique up to units and reordering.

The obvious example is $\mathbb{Z}$.

Proposition 20.2. *If R is a UFD, then $r \in R$ is prime iff it is irreducible.*

Proof. The forward direction was already proven in Lemma 20.1. For the reverse direction: suppose r is irreducible, and choose a, b such that $ab \in (r)$. Then, write $a = p_1 \dots p_n$ and $b = q_1 \dots q_m$, where the p_i and q_i are irreducible.

If one of the $a, b \in R^\times$, the other is in the ideal, which implies r is prime, so suppose that a and b are not units.

Then, $ab = p_1 \dots p_n q_1 \dots q_m = rx$ for some $x \in R$. Decompose $x = s_1 \dots s_l$ for irreducible s_i, so that $ab = rs_1 \dots s_l$ as well. Since this decomposition, then $r = up_i$ or $r = uq_i$ with $u \in R^\times$. Without loss of generality, suppose this is p_i (since we can just switch it if otherwise), so that $a = p_i(s)$ for some s, so $a \in (r)$, so r is prime. ☐

Example 20.1. Consider the ring $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, which is a subring of $\mathbb{C}$. This is clearly an integral domain.

Claim. 3 is irreducible in R.

Proof. This proof uses a trick that really only works in $\mathbb{Z}[\sqrt{-5}]$: define the norm of a $z = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ to be $N(z) = a^2 + 5b^2 = |z|_{\mathbb{C}}^2 = z\bar{z}$, so that $N(zw) = N(z)N(w)$.

Suppose that $3 = zw$ for $z, w \in \mathbb{Z}[\sqrt{-5}]$. Then, $N(3) = 9 = N(z)N(w)$. Either $N(z) = 1$ or $N(w) = 1$, which decomposes 3 into $1 \cdot 3$ (which isn't important for irreducibility), or $N(z) = N(w) = 3$. However, there is no way to write $3 = a^2 + 5b^2$ for $a, b \in \mathbb{Z}$. Thus, 3 is irreducible. ☐

This argument works just as well for $2 + \sqrt{-5}$, since $N(2 + \sqrt{-5}) = 9$, so it can be plugged into the same proof. This also works for $2 - \sqrt{-5}$; thus, they are both irreducible. This means that

$$9 = (3)(3) = (2 + \sqrt{-5})(2 - \sqrt{-5}),$$

and both of these factorizations are into irreducible elements.

If $\mathbb{Z}[\sqrt{-5}]$ were a UFD, then $2 + \sqrt{-5} = 3u$ for some $u \in \mathbb{Z}[\sqrt{-5}]^\times$, but this isn't possible, so $\mathbb{Z}[\sqrt{-5}]$ is an integral domain that is, surprisingly, not a UFD. It can be shown that there is a factorization for every element, but that it is not necessarily unique.

Additionally, 3 is not prime in this ring: if it were, then one of $2 \pm \sqrt{-5} \in (3)$, but neither can be written as $3(a + b\sqrt{-5})$ for $a, b \in \mathbb{Z}$.

Definition. An ideal $I \subseteq R$ is principal if there exists an $r \in R$ such that $(r) = I$. This is analogous to the group-theoretic notion of a cyclic group.

Definition. A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Example 20.2. Since every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z} = (n)$ for some $n \in \mathbb{Z}$ (in fact, for n nonnegative), then the integers are a PID.

Corollary 20.3. *$\mathbb{Z}[\sqrt{-5}]$ is not a PID.*

The proof will have to wait until the next lecture, where it will be shown that every PID is a UFD. However, the converse is not true; if $\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}/2\mathbb{Z}$ is given by $\varphi : f(x) \mapsto f(0) \bmod 2$, then $I = \operatorname{Ker}(\varphi) = (2, x)$, which is not principal, but $\mathbb{Z}[x]$ is a unique factorization domain (which is difficult to prove).

21. Proof that PIDs are UFDs: 11/12/12

Throughout this lecture, R will be an integral domain.

Definition. $r, r' \in R$ are associated if there is a $u \in R^\times$ for which $r' = ur$.

If r and r' are associated, then $(r) = (r')$.

The following lemma will be true because of the main result, but it's also a necessary ingredient of the proof, so it is presented here.

Lemma 21.1. *If R is a PID, then $r \in R$ is irreducible iff it is prime.*

Proof. The reverse direction is already known via Lemma 20.1. Thus, assume $r \in R$ is irreducible. It suffices to prove that (r) is maximal, by Corollary 19.5, so suppose $(r) \subseteq I \subseteq R$, where I is an ideal of R.

Since R is a PID, $I = (x)$ for some $x \in R$, so $(r) \subseteq (x) \subseteq R$, so $r \in (x)$, which implies that $r = xy$ for some $y \in R$.

Since r is irreducible, then either $x \in R^\times$, in which case $I = R$, or $y \in R^\times$, so that x and r are associated, and $(x) = (r)$. ☐

The actual result proven is slightly stronger:

Corollary 21.2. *Any nonzero ideal in a PID is generated by some nonzero element, and if $r \in R$ is prime, then (r) is maximal.*

Note that 0 is not prime, and (0) is not maximal.

Theorem 21.3. *If R is a PID, then R is a UFD.*

Proof. In order to show that R is a UFD, it will be necessary to show the existence of a factorization for every element and the uniqueness of said factorization up to units and reordering. Thus, there will be two steps:

Step 1. (existence) — this proof will be sort-of-indirect, and apparently it even needs the Axiom of Choice in the general state.

Suppose $r \in R$ cannot be written as a product of irreducibles (and that $r \neq 0$, $r \notin R^\times$). Then, r is not irreducible, so $r = r_1 r'$, with $r_1 r' \notin R^\times$ so $r \in (r_1)$, and in particular $(r) \subsetneq (r_1)$ (otherwise, $r_1 = xr$ and $r_1 \in R^\times$).

Similarly, $(r_1) \subsetneq R$ (if so, then $1 = r_1 x$, so $r_1 \in R^\times$).

Thus, either r_1 or r' cannot be written as a product of irreducible elements. Without loss of generality assume r_1 has this property.

Applying this again, one obtains a sequence $r, r_1, r_2, \dots$ such that

$$(r) \subsetneq (r_1) \subsetneq (r_2) \subsetneq \cdots \subsetneq R.$$

This is perfectly fine... except that R is a PID: let $I = \bigcup_{i=1}^{\infty} (r_i)$. Then, I is an ideal:

- If $x, y \in I$, then $x \in (r_m)$ and $y \in (r_n)$ for some $m, n \in \mathbb{N}$, so $x, y \in (r_{\max(m,n)})$. Thus, $x+y \in (r_{\max(m,n)}) \subset I$, so I is a subring.
- If $x \in I$ and $y \in R$, then $x \in (r_n)$ for some $n \in N$, so $xy \in (r_n) \subset I$, so I has the absorption property.

Thus, $I = (p)$ for some $p \in R$, since R is a PID. Since I is a union, then $p \in r_i$ for some $i \in \mathbb{N}$: then, $I = (p) \subseteq (r_i) \subsetneq (r_{i+1}) \subseteq I$, which is a contradiction.

Thus, a factorization exists.

Step 2. (uniqueness).

Suppose $r = p_1 \dots p_n = q_1 \dots q_m$ for irreducibles p_i, q_i.

Proof by induction on n: $q_1 \dots q_m = p_1 x$ for some $x \in R$, so $q_1 \dots q_m \in (p_1)$. Since p is irreducible in a PID, then it is prime by Lemma 21.1, so (p_1) is a prime ideal.

Thus, one of the $q_i \in (p_1)$. Assume $i = 1$, since they can be reordered. Then, $q_1 = p_1 x$ for some $x \in R^\times$, since p_1 and q_1 are irreducible. Thus, p_1 and q_1 are associated, and

$$r = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m = p_1(x q_2 \dots q_m) = p_2 \dots p_n = (x q_2) q_3 \dots q_m,$$

since integral domains have cancellation.

Now, there is a product of $n-1$ irreducibles, so apply the inductive hypothesis. Thus, after reordering, $n = m$ and $p_i \sim q_i$ (under association). ☐

Corollary 21.4. *Here are some examples:*

1. *$\mathbb{Z}$ is a UFD (though this was already known through a direct proof), and*
2. *$\mathbb{Z}[\sqrt{-5}]$ is not a PID (since it's not a UFD), though a direct proof exists. In fact, $(3, 2 + \sqrt{-5})$ is an ideal which is not principal.*

How might one best determine whether something is a PID? For $\mathbb{Z}$, this involved listing all the additive subgroups, but this is a bit much to ask for in general.

Definition. A norm N on an integral domain R is a function $R \to \{0, 1, 2 \dots\}$ such that $N(0) = 0$.

Definition. A norm N on an integral domain R is a norm such that if $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that $a = bq + r$ such that $N(r) < N(b)$ or $N(b) = 0$.

Definition. A Euclidean domain is an integral domain with some analogue of division with remainder: to be precise, it is a ring R with a Euclidean norm.

Example 21.1. While it will be proven next lecture that all Euclidean domains are PIDs (and therefore UFDs), here are some examples:

1. $\mathbb{Z}$ is a Euclidean domain, with $N(x) = |x|$.
2. If F is a field, then $F[x]$ is a Euclidean domain, with the norm of a polynomial equal to its degree.
3. $\mathbb{Z}[i]$ (the Gaussian integers), with $N(x + iy) = x^2 + y^2$.

In general, proving something is a Euclidean domain is a good way to show that it is a PID.

22. Euclidean Domains: 11/14/12

Theorem 22.1. *A Euclidean domain is a PID (and therefore a UFD).*

Proof. Let I be an ideal of a Euclideam domain R.

Case i. Suppose $I = \{0\}$. Then, $I = (0)$, so I is principal.

Case ii. Supose $I \setminus \{0\} \neq \emptyset$, and let $d = \min\{N(x) \mid x \in I \setminus \{0\}\}$ (the minimum exists because this is a nonempty subset of $\mathbb{N}$). Then, choose an $f \in I \setminus \{0\}$ such that $N(f) = d$.

Claim. $I = (f)$.

Proof. Since $f \in I$, then $fx \in I$ for any $x \in R$, so $(f) \subseteq I$.

Let $a \in I$ and write $a = qf + r$, with $q, r \in R$ and either $r = 0$ or $N(r) < N(f)$. If $r = 0$, then $a = qf \in (f)$; otherwise, $r = a - qf \in I \setminus \{0\}$, but $N(r) < N(f)$, which is a contradiction, since $N(f)$ is the minimum nonzero norm. □

Thus, R is a principal ideal domain. □

Theorem 22.2. *Suppose F is a field and let $N : F[x] \to \{0, 1, 2 \dots\}$ be given by the degree: $N(f) = \deg(f)$. Then, $F[x]$ is a Euclidean domain with this norm.*

Proof. Suppose $a, b \in F[x]$ and $b \neq 0$. Write $a = \sum_{j=1}^{n} a_j x^j$ and $b = \sum_{j=1}^{m} b_j x^j$, and proceed by induction.

If $n < m$, let $q = 0$ and $r = a$, so that $a = qb + r$ with $\deg(r) < \deg(b)$,

If $n \geq m$, write

$$a(x) = \left(\frac{a_n}{b_m} x^{n-m}\right) b(x) + q'(x), \text{ where } q'(x) = a(x) - \left(\frac{a_n}{b_m} x^{n-m}\right) b(x).$$

The highest terms in $q'(x)$ cancel, so $\deg(q') < n = \deg(a)$.

Applying the inductive hypothesis to q': $q' = q''b + r$ for $r, q'' \in F[x]$ such that $\deg(r) < \deg(b)$, so

$$a(x) = \left(\frac{a_n}{b_m} x^{n-m}\right) b(x) + q''(x)b(x) + r(x) = \left(\frac{a_n}{b_m} x^{n-m} + q''(x)\right) b(x) + r(x).$$ □

If one extracts the algorithm from this, one obtains the familiar method of polynomial long division.

An interesting question to ask in a UFD is what the irreducibles are. In some cases, a complete answer is possible:

- In $\mathbb{C}[x]$, f is irreducible iff $\deg(f) = 1$. This leads to the Fundamental Theorem of Algebra: that if $\deg(f) > 0$, then there exists a $\lambda \in \mathbb{C}$ such that $f(\lambda) = 0$. If f is irredicuble, then $f = qg + r$ implies $q \in \mathbb{C}[x]^\times$, which is just the set of constant polynomials.[18]

  Thus, an arbitrary $f \in \mathbb{C}[x]$ can be written as a product of the irreducible $(x - \lambda)$ terms and a unit.
- On $\mathbb{R}[x]$ life is a bit more interesting. $f \in \mathbb{R}[x]$ is irreducible iff $\deg(f) = 1$ or $\deg(f) = 2$ and the discriminant is negative (i.e. $f(x) = ax^2 + bx + c$, where $b^2 - 4ac < 0$).
- $\mathbb{Q}[x]$ is "very interesting" (i.e. rather difficult). There are irreducible polynomials of every degree.
- In $\mathbb{Z}$, there is no non-algorithmic way to list irreducibles (i.e. the primes).
- In $\mathbb{F}_p[x]$, there are also irreducible polynomials of any degree.

Since the irreducible elements of UFDs are prime, then their ideals are maximal, so taking quotients gives a field. This is an interesting way of making new fields from old ones: if $f \in F[x]$ and $\alpha = x + (f)$, then any $z \in f[x]/(f)$ can be written uniquely as $z = \sum_{j=0}^{\deg(f)-1} a_j \alpha^j$ with $a_j \in F$ (i.e. a linear combination of the powers of α),

Fr example, if $F = \mathbb{F}_q$, then $F[x]/(f) \cong \mathbb{F}_{q^{\deg(f)}}$, since it has $q^{\deg(f)}$ elements. Thus, for any prime p and $n \in \mathbb{N}$, one can construct a field with p^n elements.

23. Examples of Euclidean Domains: 11/16/12

As seen before, if R is an intergral domain and $a, b \in R[x]$, then $\deg(ab) = \deg(a) + \deg(b)$. Additionally, if $f \in R[x]$ is a unit, then $\deg(f) = 0$.

Note that for $f(x) = 1 + 2x \in \mathbb{Z}/4\mathbb{Z}[x]$, then $f^2 = 1$, so this doesn't always work if f isn't an integral domain.

The following lemma is an easy criterion for some polynomials:

Lemma 23.1. *If F is a field, $f \in F[x]$, and $\deg(f) \leq 3$, then f is irreducible iff f has no roots.*

[18] In general, if a ring R has no zero divisors, then $R^\times \cong R[x]^\times$, because $\deg(a) = 0$ if $1 = ab$.

Proof. If f is not irreducible, then $f = ab$ and $\deg(f) = \deg(a) + \deg(b)$. Since $\deg(f) \leq 3$, then one of a or b has degree 1. Without loss of generality, suppose $\deg(a) = 1$.

Thus, $a(x) = a_1x + a_0$, so $x = -a_0/a_1$ is a root of a and therefor f.

Conversely, if f has a root λ such that $f(\lambda) = 0$, then let $b(x) = x - \lambda$.

Then, $f = qb + r$ such that $\deg(r) < \deg(b) = 1$, so $\deg(r) = 0$, so r is coistant and therefore a unit (since F is a field). Thus, $f(\lambda) = q(\lambda)b(\lambda) + r$, so $r = 0$. Thus, $f = qb$ with q, b not units, so f is reducible. □

Example 23.1. Over a finite field, one can just check all possible candidates for a root: consider $f(x) = x^2+x+1 \in \mathbb{F}_2[x]$. Then, $f(0) = f(1) = 1$, so f is irreducible.

Thus, $(x^2 + x + 1) \subseteq \mathbb{F}_2[x]$ is maximal. Taking quotients, let $F = \mathbb{F}_2[x]/(x^2 + x + 1)$, so $|F| = 4$. (Similarly, if one wants a field with 8 elements, guess an irreducible polynomial of degree 3.)

It turis out that there is exactly one finite field F such that $|F| = p^k$ up to isomorphism (with p prime, $k \in \mathbb{N}$), and these are all the finite fields.

Proposition 23.2. *$\mathbb{Z}[i]$ is Euclidean, with norm $N(a + bi) = a^2 + b^2$.*

Proof. Suppose $a, b \in \mathbb{Z}[i]$ and $b \neq 0$. Then, define q to be the closest point in $\mathbb{Z}[i]$ to a/b (which is in $\mathbb{C}$ but not necessarily $\mathbb{Z}[i]$), and let $r = a - qb = b(a/b - q)$. Then, $|a/b - q| \leq \sqrt{2}/2$, so

$$N(r) = |r|^2 = |b|^2 \left|\frac{a}{b} - q\right| \leq \frac{|b|^2}{2}$$

or $r = 0$; thus, either $r = 0$ or $0 < N(r) < N(b)$. □

This geometric proof works in some other examples: let $\omega = e^{2\pi i/3}$ (a third root of unity), so that $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ is a subring. The geometry is more hexagonal, but a similar argument shows that $\mathbb{Z}[\omega]$ is Euclidean.

Over $\mathbb{Z}[i]$, $x^2+y^2 = (x+iy)(x-iy)$, and over $\mathbb{Z}[\omega]$, $x^3+y^3 = (x-y)(x+\omega y)(x+\omega^2 y)$. This can (eventually, with a lot of work) be used to prove Fermat's Last Theorem in the case $n = 3$: $z^3 = x^3+y^3 = (x-y)(x+\omega y)(x+\omega^2 y) \in \mathbb{Z}[\omega]$, and it helps greatly to know that $\mathbb{Z}[\omega]$ is a UFD.

Unfortunately, this doesn't work for all n, since not all $\mathbb{Z}\left[e^{2\pi i/n}\right]$ are UFDs.

Since $\mathbb{Z}[i]$ is a UFD, let's find its irreducibles (i.e. the "Gaussian primes"). The units are $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

One could guess that all the primes in $\mathbb{Z}$ are the primes in $\mathbb{Z}[i]$. This isn't quite true: if $p = x^2 + y^2$ for $x, y \in \mathbb{N}$, then $p = (x + iy)(x - iy)$ and p isn't irreducible. For example, 3 is prime in $\mathbb{Z}[i]$, but 5 isn't.

However, $\pi \in \mathbb{Z}[i]$ is irredicuble iff (π) is prime.

Lemma 23.3. *Let $\varphi : R \to S$ be a ring homomorphism and R, S be commutative with 1, with $\varphi(1) = 1$. If I is a prime ideal in S, then $\varphi^{-1}(I) \subseteq R$ is also a prime ideal.*

If φ is just given by inclusion, then $(\pi)\cap\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal, so there must be a prime $p \in \mathbb{Z}$ such that $(p) = \mathbb{Z}\cap(\pi) \subset \mathbb{Z}[i]$ (where $(p) \subset \mathbb{Z}$).

Thus, $p = \pi a$, with $a \in \mathbb{Z}[i]$, so $N(p) = p^2 = N(\pi)N(a)$, so $N(\pi) = p$ or p^2, since π is not a unit.

If $N(\pi) = p^2$, then $N(a) = 1$, so π and p are associated in $\mathbb{Z}[i]$. Thus, $\pi = \pm p$ or $\pi = \pm ip$.

If $N(\pi) = p$, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Thus, $p \in \mathbb{Z}$ is prime in $\mathbb{Z}[i]$ iff p cannot be written as a sum of two squares.

24. Factorization in the Gaussian Integers: 11/26/12

Here is a summary of some facts about the Gaussian primes, based on the material in the previous lecture:

- If $\pi \in \mathbb{Z}[i]$ is prime, such that $\pi\mathbb{Z}[i]$ is a prime ideal, then $\pi\mathbb{Z}[i] \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, so that $\pi\mathbb{Z}[i] \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p.
- Two things can happen as a result:
  1. if $N(\pi) = p^2$, then π and p are associate, so $\pi = \pm p$ or $\pi = \pm ip$ (since $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$). In this case, p is said to be ramified.
  2. if $N(\pi) = p$, then $p = \pi\bar{\pi}$, so p is not prime in $\mathbb{Z}[i]$, though π and $\bar{\pi}$ are. In this case, $\pi = a + ib$ and $p = a^2 + b^2$, and p is said to split.
- It's possible to go the other way, too: if $p \in \mathbb{Z}$ is prime, then one can ask whether it is also prime in $\mathbb{Z}[i]$. If $p = \pi x$ in $\mathbb{Z}[i]$, then $N(p) = N(\pi)N(x) = p^2$, so $N(\pi) \in \{p, p^2\}$. Then, any prime $p \in \mathbb{Z}$ is hit by some prime $\pi \in \mathbb{Z}[i]$, which falls into one of the two possibilities above. In particular, the second option only happens when $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$.

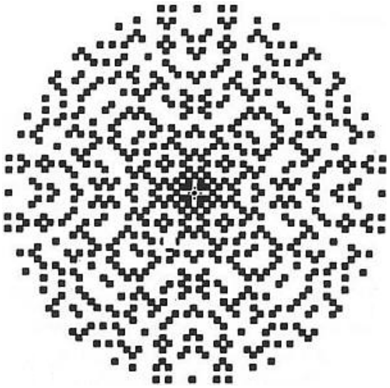


Figure 1. The Gaussian primes centered at zero.

Since $\mathbb{Z}[i]$ is a UFD, then if π, π' both give p. then $p = N(\pi) = \pi\bar{\pi} = N(\pi') = \bar{\pi}'$, which implies that $\pi' = u\pi$ for a $u \in \mathbb{Z}[i]^\times$ (i.e. $\{\pm 1, \pm i\}$).

A necessary condition for a $p \in \mathbb{Z}$ to be written as $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$ is:

$$a^2 \overset{\text{mod } 4}{\equiv} \begin{cases} 0, & a \equiv 0 \bmod 4 \\ 1, & a \equiv 1 \bmod 4 \\ 0, & a \equiv 2 \bmod 4 \\ 1, & a \equiv 3 \bmod 4, \end{cases}$$

so $a^2 + b^2 \equiv 0, 1, 2 \bmod 4$. Since p is prime, $p \not\equiv 0 \bmod 4$, and $p \equiv 2 \bmod 4$ iff $p = 2$, so either $p = 2$ or $p \equiv 1 \bmod 4$.

This is also a sufficient condition, so it's about as easy to list all the primes in $\mathbb{Z}[i]$ as in $\mathbb{Z}$.

Theorem 24.1 (Fermat). *If $p \equiv 1 \bmod 4$, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.*

Proof. It suffices to prove that p is reducible in $\mathbb{Z}[i]$, as per the above discussion.

Claim. If $p \equiv 1 \bmod 4$, then there exists an $n \in \mathbb{N}$ such that $n^2 \equiv -1 \bmod p$.

Then, $p \mid n^2 + 1$, so $pk = (n+i)(n-i)$ for some $k \in \mathbb{Z}[i]$ and $n \in \mathbb{Z}$. In particular, p appears in the prime factorization of $n + i$ or $n - i$. Without loss of generality suppose the former. If p is irreducible, then $n + i = py$ for some $y \in \mathbb{Z}[i]$, so $1 = p\operatorname{Im}(y)$, which is a constradiction (since $p \in \mathbb{R}$). Thus, p must be reducible.

Proof of the claim. This proof is almost entirely group-theoretical: consider the group of units of $\mathbb{Z}/p\mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})^\times$, which is a group of order $p - 1 \equiv 0 \bmod 4$ if $p \equiv 1 \bmod 4$. Thus, $|(\mathbb{Z}/p\mathbb{Z})^\times|$ is divisible by 4.

Then, $\overline{-1} \in (\mathbb{Z}/p\mathbb{Z})^\times$ is the unique element of order 2: if $m^2 \equiv 1 \bmod p$, then $p \mid m^2 - 1$ (in $\mathbb{Z}$), which implies that $p \mid (m-1)(m+1)$. Since p is prime, it divides one of these, so $m = \pm 1 \bmod p$. Since $|1| = 1$, then $|-1| = 2$ is unique.

Additionally, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is an abelian group of order dividing 4, then the (unique) Sylow-2 subgroup P is of order 2^k for some $k > 2$. Thus, P has at least 4 elements,at most one of which has order 2, so there exists an $x \in P \setminus \{\pm 1\}$ (which is nonempty) with $|x| > 2$ and $|x| \mid 2^k$. Thus, $|x| = 2^\ell$ for som $\ell > 2$. Let $n = x^{2^{\ell-2}}$, so that $n^2 = x^{2^{\ell-1}}$, which isn't 1, but $(n^2)^2 = x^{2^\ell} = 1$. Thus, $n = -1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. □

The full proof follows as above. □

The uniqueness of this decomposition is also worth mentioning. If $p = a^2 + b^2 = c^2 + d^2$, let $\pi = a + ib$ and $\tau = c + di$, so that π, τ are irreducibles. Thus, they are associate, so $\pi = \pm\tau$, $\pi = \pm\bar{\tau}$, $\pi = \pm i\tau$, or $\pi = \pm i\bar{\tau}$. This amounts to only changing the signs of a and b and/or swapping them to obtain c and d.

Exercise 24.1. Suppose $p \equiv 1 \bmod 4$. How would one find a, b such that $p = a^2 + b^2$? Is there a better way than the brute-force, $O(p^2)$ approach?

if $n \in \mathbb{Z}$ is not necessarily prime, then $n = a^2 + b^2$ if $n \geq 0$ and n can be written as a product of primes such that

$$n = 2^k p_1^{a_1} \cdots p_\ell^{a_\ell} q_1^{b_1} \cdots q_m^{b_m}, \;\; p_i \equiv 1 \bmod 4, q_i \equiv 3 \bmod 4.$$

The question asks if n is the norm of some Gaussian integer, or, alternatively, what is the image if $N : \mathbb{Z}[i] \to \mathbb{Z}$? $N : \mathbb{Z}[i]^\times \mapsto 1$, $q \equiv 3 \bmod 4 \mapsto q^2$, and $p \equiv 1 \bmod 4 \mapsto p$. (Note that N is not a ring homomorphism, because of -1.)

Thus, the image is all n such that $b_1, \ldots, b_m$ are all even, since the image is $b_1 \cdots b_m$.

25. Finite Fields: 11/28/12

Definition. The spectrum of a commutative ring R with identity is $\mathrm{Spec}(R)$, the set of prime ideals of R.

Thus, if R and S are commutative rings with 1 and $\varphi : R \to S$ is a ring homomorphism, then it induces a map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ (by a problem in the homework).

For a special example, consider $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ given by the inclusion homomorphism, which induces $\mathrm{Spec}(\mathbb{Z}[i]) \to \mathrm{Spec}(\mathbb{Z})$.

The spectrum has a lot of extra structure associated with it; but this would involve wandering into algebraic geometry, and that is a story for another day.

The main focus of this lecture is finite fields; just as we considered finite groups, it is possible to investigate finite fields. The classification is particularly nice; first consider the following very non-obvious theorem:

Theorem 25.1. *If F is a finite field, then $F^\times$ is a cyclic group.*

Corollary 25.2. *If $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, then $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$, so there exists an $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $\langle x \rangle = (\mathbb{Z}/p\mathbb{Z})^\times$.*

For example, $(\mathbb{Z}/5\mathbb{Z})^\times = \langle \overline{2} \rangle$. If p is large, though, the best algorithm is to try a random element, which is reasonably likely to work.

It is actually possible to prove a slightly stronger result than Theorem 25.1:

Theorem 25.3. *If F is any field and $G \leq F^\times$ for some finite group G, then G is cyclic.*

For example, the nth roots of unity in $\mathbb{C}$ form a cyclic group.

Proof of Theorem 25.3. Since $x \in G$ has order $n = |G|$ iff $x^n = 1$, then $x \in G \subseteq F$ is a root of $f(x) = x^n - 1$ in $F[x]$. There are at most n elements of order dividing n, so f has at most n roots by the following lemma:

Lemma 25.4. *If F is a field and $f \in F[x]$ has degree n, then $f(x) = 0$ has at most n solutions.*

Proof. Use division with remainder: if $\lambda \in F$ is a solution, then f can be divided by $x - \lambda$ as $f(x) = (x - \lambda)q(x) + r(x)$, where $\deg(r) < \deg(x - \lambda)$, so $\deg(r) = 0$. Plugging in $x - \lambda$, $r = 0$ as well.

Since $\deg(q) = n - 1$, then apply induction. □

It turns out, via a counting argument, that any group G with this property must be cyclic; proceed by induction on $|G|$ (which in particular implies that all proper subgroups of G are cyclic).

Suppose that $p_1, \dots, p_r$ are the primes dividing $|G|$. Let P_i be the unique Sylow-p_i subgroup of G (since G is abelian), so that all of the P_i are cyclic, $|P_i| < |G|$ and $P_i \trianglelefteq G$. Then, $G \cong \prod_{i=1}^r P_i$: the map

$$(x_1, \dots, x_r) \mapsto \prod_{i=1}^r x_i$$

is injective because if $(x_1, \dots, x_r) \mapsto 1$, then $x_1 = (x_2 \cdots x_r)^{-1}$ in P_1, so $|x_1| = p_1^k$, so $x_1 = 1$, and similarly for every other x_i. Since the two sets are the same size, then the map is also surjective.[19]

But since $(p_i, p_j) = 1$ whenever $i \neq j$, then by the Chinese Remainder Theorem,

$$G = \prod_{i=1}^r \mathbb{Z}/p_i\mathbb{Z} = \mathbb{Z}/\left(\prod_{i=1}^r p_i\right)\mathbb{Z},$$

so G is cyclic.

The remaining case is when $|G| = p^\alpha$ for some $\alpha \in \mathbb{N}$ and prime p. Then, $f(x) = x^{p^{\alpha-1}} - 1 \in F[x]$ has at most $p^{\alpha-1}$ roots, so G has at most $p^{\alpha-1}$ elements of order $p^{\alpha-1}$.

By counting, this implies the existence of an $x \in G$ such that $|x| \mid p^\alpha$ and $|x| \nmid p^{\alpha-1}$, so $|x| = p^\alpha$, making G cyclic. □

Definition. If F is a ring, there is a ring homomorphism $\mathbb{Z} \xrightarrow{\varphi} F$ given by $\varphi(n) = 1 + 1 + \overset{n}{\ldots} + 1$. Since $\mathbb{Z}$ is a PID, then $\mathrm{Ker}(\varphi) = (n)$ for some $n \in \mathbb{Z}$.

Then, the characteristic of F is $\mathrm{Char}(F) = n$.

If F is a finite field, then $\mathrm{Ker}(\varphi)$ is nontrivial, since φ can't be injective into a finite set, so $\mathrm{Char}(F) \neq 0$. However, since every subring of a field is an integral domain (since there are no zero divisors) and $\mathrm{Im}(\varphi) \subseteq F$, then $\mathrm{Im}(\varphi) \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p. In particular, there is a subring of F isomorphic to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Claim. $|F| = p^\alpha$ for some $\alpha \in \mathbb{N}$.

[19] This depends on a slightly generalized version of the Recognition Theorem for Direct Products (i.e. Theorem 15.1) than the one proven in lecture, but it is not difficult to extend.

Proof. Two proofs are given: the first is cleaner but is slightly beyond the scope of the class.

(1) If $\mathbb{F}_p \subseteq F$, then F is an $\mathbb{F}_p$-vector space, so there is an $\mathbb{F}_p$-basis for F. Thus, $F \cong \mathbb{F}_p^\alpha$ and $|F| = p^\alpha$.

(2) Suppose not; then, there exists a prime $q \neq p$ and an $x \in (F, +)$ such that $|x| = q$ by Cauchy's Theorem. Then, with φ as above,
$$x + x + \overset{q}{\ldots} + x = 0 = x(1 + 1 + \overset{q}{\ldots} + 1) = x\varphi(q),$$
but $\varphi(q) \neq 0$ since $q \neq p$, so $\varphi(q) \in (\mathbb{Z}/p\mathbb{Z})^\times$, so $x = 0$. □

26. Existence of Finite Fields of Order p^n: 11/30/12

From the previous lecture, if F is a finite field, then $F \cong \prod_{j=1}^{\alpha} \mathbb{Z}/p\mathbb{Z}$. But a more complete answer exists: there is exactly one finite field, up to isomorphism, for every prime p and $\alpha \in \mathbb{N}$. This lecture will focus on the existence argument.

Proposition 26.1. *If K is a field and $f \in K[x]$, then there exists a field L and a $\lambda \in L$ such that K is a subfield of L up to isomorphism and $f(\lambda) = 0$.*

Proof. This proof will be a generalization of the strategy used in Example 17.2.

Pick an irreducible $p \in K[x]$ such that $f = pq$ for some $q \in K[x]$. Then, $(p) \subseteq K[x]$ is maximal, so $L = K[x]/(p)$ is a field, and $K \cong \tilde{K} = \{k + (p) \mid k \in K\}$ is a subfield.

Let $\lambda = x + (p) \in L$, so that when considering $f \in L[x]$ through the isomorphism $K \to \tilde{K}$, $f(\lambda) = f(x + (p)) = f(x) + (p) = 0$, since $f \in (p)$ and $(p) = 0$ in L. □

Corollary 26.2. *If $f \in K[x]$ and $\deg(f) = n$, then there exists a field L such that $K \subseteq L$ is a subfield up to isomorphism and $f \in L[x]$ can be factorized as*
$$f(x) = u\prod_{i=1}^{n}(x - \lambda_i), \ u \in L[x]^\times, \ \lambda_1, \ldots, \lambda_n \in L.$$

Proof. Proceed by induction on n: the base case is trivial.

If $n > 1$, then find an $L_1 \supseteq K$ and a $\lambda \in L$ such that $f(\lambda) = 0$. Then, with $f(x) \in L_1[x]$, $f(x) = (x - \lambda)q(x)$ for some $q(x) \in L_1[x]$ with $\deg(q) = n - 1$. By induction, $q = u\prod_{i=1}^{n-1}(x - \lambda_i)$ in $L \supseteq L_1$, with $q \in L[x]$, $u \in L[x]^\times$, and $\lambda_1, \ldots, \lambda_n \in L$. Then, $f \in L[x]$ can be written as
$$f(x) = u(x - \lambda)\prod_{i=1}^{n-1}(x - \lambda_i).$$
□

To construct an F such that $|F| = p^n$, one must find a field $K \subseteq \mathbb{F}_p$ such that $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ can be split into linear factors: $f(x) = \prod_{i=1}^{p^n}(x - \lambda_i) \in K[x]$, with $\lambda_1, \ldots, \lambda_{p^n} \in K$.

Lemma 26.3. *If R is a commutative ring and $\mathrm{Char}(R) = p$ for some prime p, then $R \to R$ given by $r \mapsto r^p$ is a ring homomorphism, called the Frobenius homomorphism.*

Proof. The commutativity of R implies that this map preserves multiplication.

For addition, since the Binomial Theorem holds in any ring, then $(r + s)^p = \prod_{i=1}^{p} \binom{p}{i} r^i s^{p-i}$, so for some $k \in \mathbb{Z}$,
$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)!}{i!(p-i)!} = pk \equiv 0 \bmod p,$$
where $1 \leq i \leq k - 1$. Thus, everything goes to 0 except for $r^p + s^p = \varphi(r) + \varphi(s)$. □

Lemma 26.4. *If R is a ring and $\varphi : R \to R$ is a ring homomorphism, then $\{r \in R \mid \varphi(r) = r\}$ is a subring of R, called the fixed ring of R. If R is a field, then this is a subfield as well.*

The proof of this is a straightforward check of the axioms.

Returning to the construction, if K, f are as above, then take $F = \{r \in K \mid r^{p^n} = 1\}$, the set of roots of f. This is the fixed ring of φ^n (i.e. $\varphi \circ \cdots \circ \varphi$), where φ is the Frobenius homomorphism. Since φ is a homomorphism, then φ^n is as well, so $F \subseteq K$ is a subfield.

This looks like a field with p^n elements, but it's necessary to check that all of the λ_i are distinct in F:

Claim. $\lambda_i \neq \lambda_j$ whenever $i \neq j$, and thus $|F| = p^n$.

Proof. Suppose not: then, there exist $p.q \in K[x] \setminus K$ such that $f(x) = p^2 q$ (i.e. there are repeated roots). Then, $f'(x) = p^n x^{p^n - 1} - 1 = -1$, since $\mathrm{Char}(K) = p$, but $f'(x) = p^2 q' + 2pp'q = p(q' + 2pq)$, so p is a unit, which is a contradiction. □

There's something up, though — differentiation isn't necessarily defined on $K[x]$! Instead of mucking about with limits and tangent lines, one can just define it to have the required properties:

Lemma 26.5. *The function* $\frac{\mathrm{d}}{\mathrm{d}x} : K[x] \to K[x]$ *given by* $\sum_{i=1}^n a_i x^i \mapsto \sum_{i=1}^n a_i i x^{i-1}$ *is a well-defined function such that*

$$\frac{\mathrm{d}}{\mathrm{d}x}(fg) = \frac{\mathrm{d}}{\mathrm{d}x}(f)g + \frac{\mathrm{d}}{\mathrm{d}x}(g)f \text{ and } \frac{\mathrm{d}}{\mathrm{d}x}(f+g) = \frac{\mathrm{d}}{\mathrm{d}x}(f) + \frac{\mathrm{d}}{\mathrm{d}x}(g).$$

The proof is by induction on the degrees of f and g.

Thus, there does exist a field with p^n elements, usually denoted $\mathbb{F}_{p^n}$ or $\mathbb{F}_q$, where $q = p^n$. Often, it is called "the" finite field with p^n elements, though this requires the proof of uniqueness up to isomorphism that will be done in the next section.

Corollary 26.6. *In* $\mathbb{F}_p[x]$*, there exist irreducible elements of any degree* $n \geq 1$.

Proof. Choose the field F such that $|F| = p^n$ and a generator λ for $F^\times$. Then, $\mathbb{F}_p \subseteq F$, and $\mathbb{F}_p[x] \xrightarrow{\varphi} F$ given by $f(x) \mapsto f(\lambda)$ is a surjective homomorphism. Then, $F \cong \mathbb{F}_p[x]/(p)$ for some $f \in \mathbb{F}_p[x]$ (since $\mathbb{F}_p[x]$ is a PID). Since the quotient is a field, then (f) is a prime ideal, so f is irreducible, and $p^{\deg(f)} = |\mathbb{F}_p[x]/(f)| = |F| = p^n$, so $\deg(f) = n$. □

27. Uniqueness of Finite Fields of Order p^n: 12/3/12

Suppose F is a field with $|F| = p^n$. If $q = \mathrm{Char}(F)$, then $\mathbb{Z}/q\mathbb{Z} \subseteq F$ is a subfield (up to isomorphism), so $\mathrm{Char}(f) = q = p$, and in particular, $\mathbb{F}_p \subseteq F$ is a subfield.

If λ generates the group of units of F ($\lambda \in F^\times$, which is cyclic), there is a surjective homomorphism $\mathbb{F}_p[x] \xrightarrow{\varphi} F$ given by $f(x) \mapsto f(\lambda)$, as in the previous lecture.

Thus, $\mathrm{Ker}(\varphi) = (f)$ for some $f \in \mathbb{F}_p[x]$, since $\mathbb{F}_p[x]$ is a PID, so $F \cong \mathbb{F}_p[x]/(f)$ and $\deg(f) = n$.

Consider the "special polynomial" used previously, $x^{p^n} - x$. Since $\lambda \in F^\times$ and $|F^\times| = p^n - 1$, then

$$\varphi\left(x^{p^n} - x\right) = \lambda^{p^n} - \lambda = \lambda\left(\lambda^{p^n - 1} - 1\right) = 0,$$

so $x^{p^n} - x = fq$ for some $q \in \mathbb{F}_p[x]$.

Moreover, $x^{p^n} - x \in \mathbb{F}_p[x] \subseteq F[x]$, so any $\alpha \in F$ is a root of $x^{p^n} - x$, since $\alpha = 0$ or $\alpha \in F^\times$ and $x^{p^n} - x = \prod_{\lambda \in F}(x - \lambda)$.

Theorem 27.1. *If* F_1, F_2 *are finite fields, each with* p^n *elements, then* $F_1 \cong F_2$.

Proof. From the above discussion, $F_1 \cong \mathbb{F}_p[x]/(f_1)$ and $F_2 \cong \mathbb{F}_p[x]/(f_2)$, where $f_1, f_2 \in \mathbb{F}_p[x]$ are irreducible factors of $x^{p^n} - x$ of degree n.

Since $\mathbb{F}_p \subseteq F_2$, then there exists an injective ring homomorphism $\mathbb{F}_p[x] \to F_2[x]$ such that if $x^{p^n} - x = f_1 q$ for $q \in \mathbb{F}_p[x]$, then all of these can be regarded as elements of $F_2[x]$, and in particular, $x^{p^n} - x = \prod_{\lambda \in F_2}(x - \lambda)$ in $F_2[x]$.

Since $F_2[x]$ is a UFD, then write f_1 and q as products of irreducibles in $F_2[x]$. (Of course, just because f_1 is irreducible in $\mathbb{F}_p[x]$ doesn't imply that it's irreducible in the larger $F_2[x]$.) The irreducibles of f_1 and q must be a subset of the irreducible factors of $x^{p^n} - x$.

Thus, $f_1(x) = \prod_{i=1}^n (x - \lambda_i)$ for some distinct $\lambda_i \in F_2$. Pick a $\lambda \in F_2$ such that $f_1(\lambda) = 0$, which yields a ring homomorphism $\mathbb{F}_p[x] \xrightarrow{\Psi} F_2$ such that $f(x) = f(\lambda)$. Then, $\mathrm{Ker}(\Psi) = (g)$ for some $g \in \mathbb{F}_p[x]$, since $\mathbb{F}_p[x]$ is a PID. Since $\Psi(f_1) = 0$, then $f_1 = gq'$ for some $q \in \mathbb{F}_p[x]$. But f_1 is irreducible in $\mathbb{F}_p[x]$, so $q \in \mathbb{F}_p[x]^\times$ and $\mathrm{Ker}(\Psi) = (g) = (f_1)$.

Thus, by the First Isomorphism Theorem,

$$F_1 \cong \mathbb{F}_p[x]/(f_1) = \mathbb{F}_p[x]/\mathrm{Ker}(\Psi) \cong \mathrm{Im}(\Psi) \subseteq F_2.$$

But since $|F_1 = |F_2|$ is finite, then $\mathrm{Im}(\Psi) = F_2$, so $F_1 \cong F_2$. □

Because of this, it is possible to refer to "the" field with p^n elements, and it is denoted $\mathbb{F}_{p^n}$.

This is reminiscent of cyclic groups, for which this uniqueness was also present. It was also proven that subgroups of a cyclic group are cyclic, and $\mathbb{Z}/m\mathbb{Z} \leq \mathbb{Z}/n\mathbb{Z}$ (up to isomorphism) iff $m \mid n$. So what are the subfields of $\mathbb{F}_{p^n}$?

Obviously, $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$, and since the subfields are finite, then if $F \subseteq \mathbb{F}_{p^n}$, then $F \cong \mathbb{F}_{q^m}$ with $q^m \leq p^n$, q prime, and $m \in \mathbb{Z}$. In particular, since $(\mathbb{F}_{q^m}, +) \leq (\mathbb{F}_{p^n}, +)$, then $q = p$. $m = 1$ and $m = n$ are both possible, so there are at most n possible subfields.

Now consider the multiplicative groups. A necessary condition for $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ is that $\mathbb{Z}/(p^m - 1)\mathbb{Z} \cong \mathbb{F}_{p^m}^\times \leq \mathbb{F}_{p^n}^\times \cong \mathbb{Z}/(p^n - 1)\mathbb{Z}$, so $(p^m - 1) \mid (p^n - 1)$.

Lemma 27.2. *$p^m - 1 \mid p^n - 1$ iff $m \mid n$.*

Proof. If $p^m - 1 \mid p^n - 1$, then $n = dm + r$, with $0 \leq r < m$. Then,

$$\begin{aligned} p^n - 1 &= p^r(p^{dm} - 1) + p^r - 1 \\ &= p^r(p^m - 1)((p^m)^{d-1} + (p^m)^{d-2} + \cdots + 1) + p^r - 1, \end{aligned}$$

so $p^m - 1 \mid p^{dm} - 1$, so it also divides $p^r - 1$, which is less than $p^m - 1$, so $r = 0$.

The other direction is similar. □

This is also a sufficient condition: for each $m \mid n$, there exists a unique subfield $F \subseteq \mathbb{F}_{p^n}$, which strongly resembles the result for cyclic groups.

In particular, this means that $\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^6} \subseteq \cdots \subseteq \mathbb{F}_{p^{n!}} \subseteq \dots$ Taking the union of these, one obtains the algebraic closure of the $\mathbb{F}_p$: $\bar{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$, which is algebraically closed and contains every $\mathbb{F}_{p^n}$ as a subfield.

28. Review of Group Theory: 12/5/12

The last two lectures are reviews of the course material. Most concepts will be named without going into too much depth.

Some examples of groups:

- $\mathbb{Z}/n\mathbb{Z}$
- $D_{2n} = \langle r, s \rangle$
- $\mathrm{GL}_n(F)$ and $\mathrm{SL}_n(F)$, where F is a field.
- S_n and A_n. The cycle notation is worth knowing (particularly multiplication), though it makes conjugation much easier:
$$\sigma \circ (a_1 \ \cdots \ a_m) \circ \sigma^{-1} = (\sigma(a_1) \ \cdots \ \sigma(a_m)).$$

Here are some notions that will be useful to review: subgroups and cosets of a subgroup, normal subgroups, quotient groups (and their relation to cosets — in particular, Lagrange's theorem that $|G/H| = |G|/|H|$ for finite groups G, H). If $H \trianglelefteq G$ then G/H is a group.

Recall the First Isomorphism Theorem: if $\varphi : G \to H$ is a group homomorphism, then $\mathrm{Im}(\varphi) \leq H$, $\mathrm{Ker}(\varphi) \trianglelefteq G$, and $G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.

Example 28.1. If $G = \mathrm{GL}_3(\mathbb{C})$ and $H = \{A \in G \mid |\det A| = 1\}$, then it is easy to show that $H \trianglelefteq G$ and $G/H \cong \mathbb{R}^+$.

The above example is screaming to use the First Isomorphism Theorem using $\varphi(A) = |\det A|$.

A simple group is a group with no nontrivial normal subgroups. Examples: A_n, for $n \geq 5$.

Lemma 28.1. *If $\varphi : G \to H$ is a homomorphism and G is simple, then φ is injective (since $\mathrm{Ker}(\varphi) = 1$) or φ is trivial (and the kernel is G), since $\mathrm{Ker}(\varphi) \trianglelefteq G$, so it must be trivial or all of G.*

It is also worth reviewing semidirect products, even though they weren't mentioned explicitly in class.

A group action can be viewed in two ways. It is a map $\cdot : G \times A \to A$ with 2 axioms, but also as a group homomorphism $\varphi : G \to S_A$, the symmetric group on A. These are equivalent; which is more useful depends on context.

- The orbit of $x \in A$ is $G \cdot x = \{g \cdot x \mid g \in G\} \subseteq A$.
- The stabilizer of an $x \in A$ is $G_x = \{g \mid g \cdot x = x\} \leq G$.

In particular, consider the Orbit-Stabilizer Theorem: it asserts that there is a bijection between G/G_x and $G \cdot x$ for any $x \in A$. (This is true even if the set of cosets G/G_x doesn't have a group structure.) This can be used in a counting argument, counting $|A|$ one orbit at a time:

$$|A| = \sum_{\text{one } x \text{ per orbit}} |G : G_x|.$$

There are several special actions:

- G acts on itself by translation: $g \cdot h = gh$ for $g, h \in G$.
- G acts on G/H (for an $H \leq G$) by translation: $g_1 \cdot (g_2 H) = g_1 g_2 H$ for $g_1, g_2 \in G$.
- G acts on itself by conjugation: $g \cdot h = ghg^{-1}$ for $g, h \in G$.

This last action leads to the class formula: if $\mathcal{G}$ is a set containing one conjugacy class of $G \setminus Z(G)$, then

$$|G| = |Z(G)| + \sum_{a \in \mathcal{G}} |G : C_G(a)|.$$

In particular, if G is a p-group (i.e. $|G| = p^n$), then $Z(G)$ is nontrivial.

However, the most important consequence of group actions is probably Sylow's Theorem:

Theorem. *If $|G| = p^\alpha m$, with p prime, $p \nmid m$, then $P \leq G$ is a Sylow p-subgroup of G if $|P| = p^\alpha$. The set of such subgroups is $\operatorname{Syl}_p(G)$, and $n_p(G) = |\operatorname{Syl}_p(G)|$. Then,*

(1) $\operatorname{Syl}_p(G) \neq \emptyset$,
(2) If $P, Q \in \operatorname{Syl}_p(G)$, then there exists a $g \in G$ such that $gPg^{-1} = Q$; that is, the action of G on $\operatorname{Syl}_p(G)$ by conjugation is transitive, and
(3) $n_p(G) \equiv 1 \bmod p$, and $n_p(G) \mid m$.

As a corollary, $N_p(G) = |G : N_G(P)|$, so $n_p(G) = 1$ iff $P \trianglelefteq G$ (is the only Sylow-p subgroup).

These allow one to find $n_p(G)$ by listing the divisors of m and then removing those that aren't 1 mod p. For example, if G is known to be simple, then $n_p(G) > 1$ for any prime p dividing the order of G. The action by conjugation of G on $\operatorname{Syl}_p(G)$ comes with an induced homomorphism $G \to S_{n_p(G)}$, and if G is simple, then this is injective (since it is transitive), so it is nontrivial.

"I think one reason Sylow's theorems are so popular is because it is so easy to make problems." For example, one might have to state things about subgroups of a simple group of some reasonable order, particularly on one's P.h.D. quals.

Example 28.2. If $|G| = 6545 = 5 \cdot 7 \cdot 11 \cdot 17$, then G cannot be simple.

Suppose G were simple: then,

- $n_5(G) = 11$, since $n_5(G) \mid 7 \cdot 11 \cdot 17$, $n_5(G) \equiv 1 \bmod 5$, and $n_5(G) \neq 1$. Thus, there are 44 elements of order 5.
- By essentally the same line of reasoning, $n_7(G) = 85$, so there are $6 \cdot 85 = 520$ elements of order 7.
- Then, $n_{11}(G) = 5 \cdot 7 \cdot 17$ with the same argument, so there are $10 \cdot 5 \cdot 7 \cdot 11 \cdot 17$ elements of order 11.
- The real problem happens with $n_{17}(G)$, for which there are 35 elements. This forces a contradiction, since the total number of elements accounted for so far is more than the order of the group!

Thus, G cannot be simple. □

29. Review of Ring Theory: 12/7/12

In ring theory there are a lot of words. In addition to rings there are commutative rings and rings with identity. These combine in the concept of a commutative ring with identity. Then, there is the following series of inclusions:

Commutative rings with 1 $\supset$ Integral Domains $\supset$ UFDs $\supset$ PIDs $\supset$ Euclidean domains $\supset$ Fields.

- An integral domain is a commutative ring with 1 that has no zero divisors.
- A UFD (unique factorization domain) is an integral domain in which all irreducible elements are prime, and (equivalently) every element can be uniquely factorized into irreducible elements (up to units and reordering).
- A PID (principal ideal domain) is a commutative ring with identity such that every ideal is generated by one element.

Example 29.1. Suppose R is a ring.

- The ring of $n \times n$ matrices $M_n(R)$.
- The ring of polynomials $R[x]$: these are the formal expressions (or functions) $f(x) = \sum_{j=0}^{n} a_j x^j$.
- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ for p prime is a field; in general, $\mathbb{Z}/n\mathbb{Z}$ is a ring.
- $\mathbb{F}_{p^n}$ is a field for p prime and $n \in \mathbb{N}$.

The First Isomorphism for Rings is useful: if $\varphi : R \to S$ is a ring homomorphism, then $\operatorname{Im}(\varphi) \subseteq S$ is a subring and $\operatorname{Ker}(\varphi) \subseteq R$ is an ideal.

In general, if $I \subseteq R$ is an ideal, then the quotient ring is $R/I = \{r + I \mid r \in R\}$.

If $r_1, \dots, r_n \in R$, then $(r_1, \dots, r_n) \subseteq R$ is the ideal generated by $r_1, \dots, r_n$. For example, one has the ideal $(2, x) \subseteq \mathbb{Z}[x]$.

For commutative rings with an identity $1 \neq 0$, an ideal can be:

- principal (i.e. $I = (f)$ for some $f \in \mathbb{R}$),
- prime if whenever $ab \in I$, then $a \in I$ or $b \in I$, where $I \neq R$. In this case, R/I is an integral domain.
- maximal if $I \neq R$ and whenever $I \subseteq J \subseteq J$ with J an ideal of R, then $I = J$ or $J = R$. In this case, R/I is a field.

Within integral domains, there is factorization theory, which is mostly about multiplication. Even in $\mathbb{Z}$ the primes behave very badly with respect to addition.

The group of units of a ring is $R^\times$, and $f, g \in R$ are associated ($f \sim g$) if $f = gu$ for some $u \in R^\times$. An element $f \in R$ is irreducible if $f = ab$ necessarily implies that $a \in R^\times$ or $b \in R^\times$, and is prime if (f) is a prime ideal. Notice that irreducible implies prime, but not necessarily the reverse.

For UFDs, an element is prime iff it is irreducible. Given some integral domain R, one can ask if it is a UFD, and if so, what are its irreducibles (i.e. what are its prime ideals)?

- For example, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.
- $\mathbb{Z}$ is a UFD, and its irreducibles are the primes $\{2, 3, 5, 7, 11 \dots\}$.
- If F is a field, then $F[x]$ is a UFD, and the answer to the latter question depends on F itself:
  - In $\mathbb{C}[x]$, the irreducibles are $x - a$ for $a \in \mathbb{C}$ and associates.
  - In $\mathbb{R}[x]$, the irreducibles are $x - a$ for $a \in \mathbb{R}$ and $x^2 + bx + c$ where $b, c \in \mathbb{R}$ and $b^2 - 4ac < 0$.
  - In $\mathbb{Q}[x]$, it is difficult to establish irreducibility, but there are irreducibles of any degree (e.g. $x^n - 2$ for $n > 1$).
  - In $\mathbb{F}_p[x]$, there are irreducibles of any degree, and if $\deg(f) = n$, then $f \mid (x^{p^n} - x)$.
- $\mathbb{Z}[i]$ is a UFD, and its primes correspond to those of $\mathbb{Z}$: $2 \in \mathbb{Z}$ corresponds to $1 \pm i$ in $\mathbb{Z}[i]$, $p \equiv 3 \bmod 4$ in $\mathbb{Z}$ corresponds to $p \in \mathbb{Z}[i]$, and $p \equiv 1 \bmod 4$ in $\mathbb{Z}$ corresponds to $a \pm ib \in \mathbb{Z}[i]$, where $p = a^2 + b^2$.

The general result is that ED $\implies$ PID $\implies$ UFD, as above. If R is a PID, then $I \subsetneq R$ is prime iff I is maximal or $I = (0)$.

For fields, if $G \leq F^\times$ such that G is finite, the G is cyclic. If $f \in F[x]$, then there exists a field $K \supseteq F$ such that f factors linearly as an element of $K[x]$.

The characteristic of a field (or really, of any ring with 1) is $\mathrm{Char}(F) \in \mathbb{N} \cup \{0\}$.

For finite fields, $F^\times$ is cyclic, and $|F| = p^n$ for a prime p and an $n \in \mathbb{N}$. In fat, for each p and n, there is exactly one field F such that $|F| = p^n$, up to isomorphism (existence and uniqueness are required for this).This field is usually written $\mathbb{F}_{p^n}$, and is the set of roots of $x^{p^n} - x \in \mathbb{F}_p[x]$ within some $K \supset \mathbb{F}_p$ such that $x^{p^n} - x$ factor linearly as

$$x^{p^n} - x = \prod_{\lambda \in \mathbb{F}_{p^n}} (x - \lambda).$$

$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{q^m}$ (up to isomorphism) iff $p = q$ and $n \mid m$.

One thing that doesn't easily fit in elsewhere is the Chinese Remainder Theorem, which would also be useful to remember.