Abstract Algebra II Lecture Notes

Simon Xiang

These notes were transcribed from my physical lecture notes for the Spring 2020 undergraduate/graduate section of Abstract Algebra II (Math 4510) at UNT, taught by Dr. Shepler, which I took while I was at TAMS. Source files: https://git.simonxiang.xyz/math_notes/files.html

Contents

1 January 13, 2020

Nostalgic notes...

Definition 1.1. A number $\alpha \in \mathbb{R}$ is said to be **constructable** if we can construct a line segment of length $|\alpha|$ in a finite number of steps using only a straightedge and compass.

Theorem 1.1. *If α, β are constructable, then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. We show α, β are constructable for $\alpha, \beta > 0$ (refer to [Fra03] §32, page 294). Assume α and β have been constructed. Construct a line segment B to the line containing A such that it is parallel to the line sgment from P (of length 1) to A containing B (in three steps). This yields congruent triangles $\Delta OAP, \Delta OQB$ respectively, where Q is the intersection of $\overline{OA}$ with the line parallel to $\overline{PA}$ containing B. Therefore $\overline{PA}$ is parallel to $\overline{BQ}$, and since ΔOAP and ΔOQB are congruent, $\|\overline{OA}\|/\|\overline{OP}\| = \frac{\|\overline{OQ}\|}{\|\overline{OB}\|}$. So $\alpha/1 = \|\overline{OQ}\|/\beta$, which implies $\|\overline{OQ}\| = \alpha \cdot \beta$ and is constructable. ⊠

Similar results with α/β ($\beta \neq 0$) and $\alpha - \beta$ imply the following theorem.

Theorem 1.2. *The set of all constructable numbers in $\mathbb{R}$ form a field.*

Some ancient questions answered:

(1) It is impossible to construct a cube with double the volume of another. If α is constructed, consider a cube with volume α^3. Then it is impossible to construct a β such that cube having length β satisfies $\mathrm{vol}(\beta^3) = 2\alpha^3$.
(2) It is impossible to square the circle. Given a circle with area A, we cannot find a square with area A (constructed with a compass and straightedge).
(3) It is impossible to trisect an angle using only a compass and straightedge. (But you can biset an angle in a finite amount of steps!)

Some formulas for roots of polynomials in a single variable.

- **QUADRATIC:** Known since approximately 1000 BC.
- **CUBIC**: Known.
- **QUARTIC**: Use a flowchart.
- **QUINTIC**: There is no POSSIBLE quintic formula. The reason is that A_5 is simple. These are all connected through field extensions and Galois theory.

2 January 15, 2020

We want coefficients for polynomials from $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$, etc.

Example 2.1 (Freshman's dream)**.** If the coefficients are from $\mathbb{Z}/5\mathbb{Z}$, then $(x+y)^5 = x^5 + y^5$.

Definition 2.1. For a ring R, then $R[x] = \{a_0 + a_1x + a_2x^2 + \cdots a_mx^m \mid m \geq 0 \text{ for all } a_i \in R\}$. $R[x]$ is known as the set of **polynomials over** R. A polynomial has **degree** m, **leading coefficient** a_m, and **leading term** a_mx^m.

Example 2.2. For $f(x) = 5$, $f(x)$ is a polynomial in $\mathbb{R}[x]$ and has degree 0.

Note. The zero polynomial $f(x) = 0$ has degree undefined *by convention.* (Some authors define it as having degree -1 or $-\infty$).

Note. Don't regard your polynomials as functions in order to check that two polynomials are the same! For example, $f(x) = x, h(x) = x^3$ are both polynomials in $\mathbb{Z}/3\mathbb{Z}[x]$ (the polynomials of the ring $\mathbb{Z}/3\mathbb{Z}$). If we were to view them as functions, we get the same function! If $f, h\colon \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, then for every $x \in \mathbb{Z}/3\mathbb{Z}$, $f(x) = h(x)$. As functions, they are equivalent. However $f \neq g$ as polynomials. Two polynomials are **equal** iff for every x_i, the coefficients agree for every $i \geq 0$.

Theorem 2.1. *The set of polynomials over a ring R, known as $R[x]$, form a ring under addition and multiplication of polynomials.*

(1) $0_{R[x]} = 0_R$, the zero polynomial.
(2) We view R as a subset of $R[x]$ in this way: for every $\alpha \in R$, there exists a constant polynomial such that $f(x) = \alpha$.
(3) R is commutative implies that $R[x]$ is commutative.
(4) R has unity 1_R implies that $R[x]$ has unity $1_{R[x]} = 1$.

Theorem 2.2 (Evaluation homomorphism)**.** *For a ring R and some $a \in R$, we define the function $\phi_a\colon R[x] \to R$ by $\phi_a\colon R[x] \to R$ by $\phi_a(f(x)) = f(a) \in R$. Then ϕ_a is a ring homomorphism.*

For $a = 0$, the evaluation homomorphism $\phi_0\colon f(x) \mapsto f(0)$ picks off constant terms of any polynomial.

Example 2.3. Let $R = \mathbb{Z}/6\mathbb{Z}$. For $f(x) = \overline{2}x + \overline{3}$, $h(x) = \overline{3}x^2 + \overline{1}$, we have $\deg(f \cdot h) = \overline{6}x^3 + \overline{9}x^2 + \overline{2}x + \overline{3} \equiv \overline{3}x^2 + \overline{2}x + \overline{3} \neq 2 \neq 1 + 3 = \deg(f) + \deg(h)$. This ring messed up because of zero divisors, zero divisors bad.

Lemma 2.1. *If R has no zero divisors, then* $\deg(fg) = \deg(f) + \deg(g)$.

3 August 30, 2021

Example 3.1. Here are some examples of group actions:

(1) Let $G = (\mathbb{Z}, +)$. Then an action of $\mathbb{Z}$ on a set X is equivalent to an isomorphism $T\colon X \xrightarrow{\simeq} X$. Given an action of $\mathbb{Z}$ on X, then for $1 \in \mathbb{Z}$, the map $1 + (-)\colon X \to X$ is a bijection (since we already have the action of $\mathbb{Z}$). Conversely, given a bijection T, define $n + (-)\colon X \to X$ as

$$\begin{aligned} T^n &= \overbrace{T \circ \cdots \circ T}^{n \text{ times}}, \quad n > 0, \\ &= \overbrace{T^{-1} \circ \cdots \circ T^{-1}}^{-n \text{ times}}, \quad n < 0 \\ &= \mathrm{id}, \quad n = 0. \end{aligned}$$

(2) Let $G = (\mathbb{Z}/n, +)$. (You can check that the quotient projection $\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n$ where $m \mapsto m \pmod{n}$ is a homomorphism.) Then an action of G on X is equivalent to a bijection $T\colon X \xrightarrow{\simeq} X$ such that $T^n = \mathrm{id}$.

Example 3.2. If X is a set, then define

$$\mathrm{Aut}(X) = \{\sigma\colon X \to X \mid \sigma \text{ is a bijection}\}.$$

Then $\mathrm{Aut}(X)$ is a group under the multiplication $\sigma_1 \cdot \sigma_2 := \sigma_1 \circ \sigma_2$. There is a canonical action of $\mathrm{Aut}(X)$ on X, where $\sigma \cdot x := \sigma(x)$. An informal claim is that this example is universal. Suppose G acts on X, then we obtain a homomorphism $\varphi\colon G \to \mathrm{Aut}(X)$, where $g \mapsto (x \mapsto g \cdot x)$. Conversely, given $\varphi\colon G \to \mathrm{Aut}(X)$, we obtain an action of G on X by $g \cdot x := \varphi(g)(x)$.

Remark 3.1. Let $X = \{1, \cdots, n\}$, then $\mathrm{Aut}(X)$ is the symmetric group on n letters S_n. So we can think of actions of a group G on finite sets as homomorphisms to symmetric groups.

We spend some time talking about the geometric properties of the action of $\mathbb{Z}/5$ on the pentagon (free and transitive actions?).

Definition 3.1. If G acts on X, then there is an equivalence relation on X where $x \sim y$ iff there exists a $g \in G$ such that $y = gx$. An **orbit** of G on X is an equivalence class for this relation. The set of orbits is denoted X/G.

Example 3.3. Let $G = \mathbb{Z}/5$ act on the vertices of the pentagon, then there is a unique orbit. But if G acts on the set of edges, then there are two orbits of internal and external edges.

4 September 1, 2021

4.1 Quotients

We quickly review equivalence relations.

Definition 4.1. An **equivalence relation** on a set X is a subset $R \subseteq X \times X$ such that:

(1) $x \sim x$,

(2) $x \sim y \iff y \sim x$,

(3) $x \sim y$ and $y \sim z$ implies $x \sim z$.

Example 4.1 (The example to end all examples)**.** Given a map $f\colon X \to Y$, we obtain an equivalence relation on X where $x_1 \sim x_2$ iff $f(x_1) = f(x_2)$.

Now we construct the quotient by an equivalence relation. Given a set X and an equivalence relation $\sim$ on X, where is another set $X/\sim$ which receives a canonical projection $\pi\colon X \to X/\sim$, having the following "universal property": giving a map of sets $X/\sim \xrightarrow{f} Y$ is equivalent to giving a map $X \xrightarrow{\varphi} Y$ such that $x_1 \sim x_2$ implies $\varphi(x_1) = \varphi(x_2)$.

There is an omitted assumption here: given a map $g\colon Y \to Z$ and $f\colon X/\sim \to Y$ corresponding to $\varphi\colon X \to Y$, the maps gf and $g\varphi$ correspond as well (functorality).

Remark 4.1. Informally, a universal property for a set, group, topological space, etc, is a rule for either mapping into the set or mapping out of the set. Mapping out universal properties look like quotient relations, and it can be hard to tell what points are.

Consider the identity map $\mathrm{id}\colon X/\sim \to X/\sim (= Y)$. This corresponds to a canonical map $\pi\colon X \to X/\sim$ such that whenever $x_1 \sim x_2$, $\pi(x_1) = \pi(x_2)$. Moreover, by functorality whenever we have some Y and φ as before, the following diagram commutes:

$$\begin{tikzcd} X \arrow[d, "\pi"'] \arrow[dr, "\varphi"] & \\ X/\sim \arrow[r, "f"] & Y \end{tikzcd}$$

Our relation $\sim$ defines a map $X \xrightarrow{p} \mathcal{P}(X)$ (where $\mathcal{P}(X)$ denotes the power set of X) by sending $x \mapsto p(x) \subseteq X$, where $p(x) := \{y \in X \mid x \sim Y\}$. We formallly construct $X/\sim$ by defining it as the image of the map p. Then by construction, there exists a unique surjection π fitting into

$$\begin{tikzcd} X \arrow[r, "\pi"] \arrow[r, bend left, "p"] & X/\sim \subseteq \mathcal{P}(X) \end{tikzcd}$$

Claim. *$X/\sim$ satisfies the universal property, i.e., given $\varphi\colon X \to Y$ with $\varphi(x_1) = \varphi(x_2)$, for every $x_1 \sim x_2$, there exists a unique factorization*

$$\begin{tikzcd} X \arrow[d, "\pi"'] \arrow[dr, "\varphi"] & \\ X/\sim \arrow[r, dotted, "f"] & Y \end{tikzcd}$$

For the construction of f, observe that $\varphi|_{p(x)}$ is constant with value $\varphi(x)$, i.e, for every $y \in p(x)$, $\varphi(y) = \varphi(x)$.

Proof. We have $y \in p(x)$ iff $x \sim y$ which implies $\varphi(x) = \varphi(y)$. To construct f, suppose we have $S \in X/\sim$ (nonempty by assumption), then choose any $x \in S$ and take $f(S) := \varphi(x)$. This is independent of choice by the observation above. Moreover, the diagram commutes. ☒

Lemma 4.1. *Given $x, y \in X$, $x \sim y$ iff $\pi(x) = \pi(y)$.*

Proof. We want to show that for $S_1, S_2 \in X/\sim$, $S_1 = S_2$ or $S_1 \cap S_2 = \emptyset$. Moreover, $X = \coprod_{S \in X/\sim} S$. For the first claim, $z \in \pi(x) \cap \pi(y)$ implies $x \sim z$ and $y \sim z$ implies $z \sim y$. So $x \sim y$ implies $y \in p(x)$. Moreover, for every $w \in p(y)$, this also shows that $w \sim x$. Then $p(y) \subseteq p(x)$, and by symmetry $p(y) = p(x)$. For the second claim, it suffices to show that $X = \bigcup_{S \in X/\sim} S$, which is clear because $x \in p(x)$ (since $x \sim x$). This gives rise to a partition of X into equivalence classes.

Now to prove Lemma 4.1, suppose $\pi(x) = \pi(y)$. We want to show that $x \sim y$. Then by our first claim, there exists a map $\varphi\colon X \to \{0, 1\}$ with $\varphi(z) = 1$ iff $z \in p(x)$, $\varphi(z) = 0$ otherwise, since $\varphi(z_1) = \varphi(z_2)$ for $z_1 \sim z_2$. By the universal property,

$$\begin{tikzcd} X \arrow[d, "\pi"'] \arrow[dr, "\varphi"] & \\ X/\sim \arrow[r, dotted, "f"] & \{0,1\} \end{tikzcd}$$

Clearly $f(x) = f(y)$. But by the above construction, this implies $x \sim y$. ☒

5 September 3, 2021

todo:missed this lecture

6 September 8, 2021

Observe that all fibers of the map $\pi\colon G \to G/H$ are in *non-canonical* bijection.

Definition 6.1. A **fiber** of a map $f\colon X \to Y$ is a subset of X of the form $f^{-1}(y)$ for some $y \in Y$.

We know that π is surjective. Therefore, there exists a section $\tau\colon G/H \to G$ such that

$$\begin{tikzcd} G/H \arrow[r, "\tau"] \arrow[rr, bend right, "\mathrm{id}_{G/H}"'] & G \arrow[r, "\pi"] & G/H \end{tikzcd}$$

This is called "choosing coset representatives", since the fibers of π are right H-cosets. Then given $x \in G/H$, $\pi^{-1}(x) = \sigma(x) \cdot H$. This is in bijection with H via the map multiplication on the left with $\sigma(x)$.

Lagrange's Theorem. *If G and H are finite, then $|G| = |G/H| \cdot |H|$.*

Proof. If we have $\pi\colon G \to G/H$, all fibers have order $|H|$. ☒

Definition 6.2. A **map/morphism/homomorphism** of sets with G-action is a map $f\colon X \to Y$ such that $f(gx) = gf(x)$ for all $x \in X$, $g \in G$. A **isomorphism** of G-sets is a morphism f with an inverse g ($fg = \mathrm{id}_Y,\ gf = \mathrm{id}_X$). This is equivalent to f being bijective.

Definition 6.3. For X a G-set and $x \in X$, the **stabilizer** of x is the subgroup $\mathrm{stab}(x) = \mathrm{stab}_G(x) = \{g \in G \mid g \cdot x = x\}$.

The implicit claim is that $\mathrm{stab}(x)$ is a subgroup. To check this, $1 \in \mathrm{stab}(x)$ as $1 \cdot x = x$. For $g, h \in \mathrm{stab}(x)$, then $(gh)x = g(hx) = gx = x$, so $gh \in \mathrm{stab}(x)$. Finally, if $g \in \mathrm{stab}(x)$, then $x = 1 \cdot x = g^{-1} \cdot g \cdot x = g^{-1}x$, so $g^{-1} \in \mathrm{stab}(x)$.

Example 6.1. Let $X = G/H$, $x = \pi(1) \in G/H$. Then $\mathrm{stab}(x) = H$, since $g \in \mathrm{stab}(x)$ iff $gH = H$ iff $g \in H$.

Example 6.2. Let $G = S_n$ act on $\{1, \cdots, n\} = X$. Then $\mathrm{stab}(n) = S_{n-1}$, since we fix n and shuffle $1, \cdots, n-1$.

Lemma 6.1. *Suppose we are given a G-set X and a point $x \in X$ such that*

(a) $|X/G| = 1$ *(there exists a unique orbit),*
(b) $\mathrm{stab}(x) = H \subseteq G$.

Then there exists a unique isomorphism of G between $G/H \xrightarrow{\simeq} X$ such that $\pi(1) \mapsto x$.

Proof. To figure out which way maps should go, recall the universal property of G/H.

$$\begin{tikzcd} G \arrow[d, "\pi"'] \arrow[dr, "\widetilde{f}"] & \\ G/H \arrow[r, dotted, "f"] & X \end{tikzcd}$$

Define $\widetilde{f}(g) = gx$. Then by the universal property of quotients, we see that f exists iff $\widetilde{f}(gh) = \widetilde{f}(g)$ for all $g \in G, h \in H$.

todo:not sure what happened here ⊠

Lemma 6.2. *Giving a morphism of all G-sets is equivalent to a point $x \in X$, $f(\pi(1)) = x$, such that* $\mathrm{stab}(x) \supseteq$.

6.1 The structure of G-sets

Suppose G acts on X. Then $X \simeq \coprod_{i \in I} G/H$ as a G-set for I sosme (?). The construction is as follows: let $I = X/G$. Choose some representatives of each orbit, i.e. a section of the map $X \to X/G$. For each $i \in I = X/G$, choose x_i in that orbit. For $i \in I$, take $H_i = \mathrm{stab}(x)$. Now apply our previosu result to obtain the deomposition of X.

7 September 10, 2021

7.1 Normal subgroups

Definition 7.1. A subgroup H is **normal** if either

(a) $gH = Hg$ as sets for every $g \in G$,
(b) for every $g \in H, h \in H$, there exists some $\widetilde{h} \in H$ such that $gh = \widetilde{h}g$,
(c) $ghg^{-1} \in H$ for every $g \in G, h \in G$,
(d) $gHg^{-1} = H$.

In other words, H is normal if its left and right cosets coincide.

Lemma 7.1. *A subgroup H is normal iff there exists a group structure on G/H such that the map $G \xrightarrow{\pi} G/H$ is a homomorphism.*

Proof. If G/H has such a group structure, then we have a commutative diagram

$$\begin{tikzcd} G \times G \arrow[r, "{m_G,\ g_1, g_2 \mapsto g_1 g_2}"] \arrow[d, "\pi \times \pi"] & G \arrow[d, "\pi"] \\ G/H \times G/H = (G \times G)/(H \times H) \arrow[r, dotted, "m_{G/H}"] & G/H \end{tikzcd}$$

By the universal property, the dotted arrow exists uniquely iff for all $(g_1, g_2) \in G \times G$, $(h_1, h_2) \in H \times H$,

$$\pi(g_1 g_2) = \pi(g_1 h_2 g_2 h_2). \tag{1}$$

The reason is that the left hand side is $\pi \circ m_G(g_1, g_2)$, the right hand side is $(\pi \circ m_G)(g_1 h_2, g_2 h_2)$, and $(g_1, g_2) \sim (g_1 h_1, g_2 h_2)$ defines the equivalence relation. The right hand side of Equation (1) is equal to $\pi(g_1 h_1 g_2)$.

Assume H is normal. Then $\pi(g_1 h_1 g_2) = \pi(g_1 g_2 g_2^{-1} h_1 h_2)$, then by the normality of H the last three terms reduce to get $\pi(g_1 g_2)$ which is the left hand side of Equation (1). Conversely, if Equation (1) holds for every g_1, g_2, h_1, h_2, take $g_1 = 1 \in G$, $g_2 = G$, $h_1 = h$, $h_2 = 1$. So $\pi(g) = \pi(1 \cdot h * 8g \cdot 1) = \pi(hg)$. This means there exists some $\widetilde{h} \in H$ such that $g \cdot \widetilde{h} = hg$, which is true iff $\widetilde{h} = g^{-1} hg \in H$. ⊠

Definition 7.2. We say

(a) Two elements $g, h \in G$ **commute** if $gh = hg$;

(b) G is **commutative**/**abelian** if $gh = hg$ for all $g, h \in G$;

(c) The **center** $Z(G)$ is the subset $\{z \in G \mid zg = gz \text{ for all } g \in G\}$.

It is easy to see that $Z(G)$ is a normal subgroup of G. A related construction is the **adjoint** action or **conjugation** action of G on itself. For $g, h \in G$, $\mathrm{Ad}_g(h) := ghg^{-1}$. This defines an action of G on itself with the action map

$$G \times G = G \times X \xrightarrow{(g,h) \mapsto ghg^{-1} = \mathrm{Ad}_g(h)} G$$

NB:[1] The adjoint action mixes left and right actions of G on itself.

Lemma 7.2. *The map $\mathrm{Ad}_g \colon G \to G$ is a group homomorphism.*

Proof. Let $h_1, h_2 \in G$. Then

$$\mathrm{Ad}_g(h_1) \cdot \mathrm{Ad}_g(h_2) = (gh_1 g^{-1})(gh_2 g^{-1}) = gh_1 h_2 g^{-1} = \mathrm{Ad}_g(h_1 h_2).$$

The inverse to Ad_g is $\mathrm{Ad}_{g^{-1}}$: $\mathrm{Ad}_{g^{-1}} \mathrm{Ad}_g(h) = \mathrm{Ad}_{g^{-1}} ghg^{-1} = g^{-1}(ghg^{-1})g = h$. ⊠

Definition 7.3. A **conjugacy class** in G is an orbit for the adjoint action. Two elements g_1, g_2 are **conjugate** if the lie in the same conjugacy class iff there exists a $g_3 \in G$ such that $g_3 g_1 g_3^{-1} = g_2$. Write G/G_{Ad} for the set of conjugacy classes of G.

[1] Nota Bene

7.2 p-groups and Sylow theorems

From now on, p is a prime.

Definition 7.4. A group G is a **p-group** if G is finite, and $|G| = p^r$ for some r.

Definition 7.5. For a group G acting on X, the **fixed point set** of X is the set $X^G = \{x \in X \mid gx = x \text{ for every } g \in G\}$.

Lemma 7.3. *Suppose G is a p-group acting on a finite set X. Then $|X| = |X^G| \pmod p$.*

Proof. Break up $X = \coprod_{i=1}^N X_i$, with the X_i being orbits for the G-action. For every i, choose some $x_i \in X_i$, $H_i = \mathrm{stab}(x_i)$, so $X_i \simeq G/H_i$.

- Option 1: $H_i = G \iff x_i \in X_i^G$.
- Option 2: $H_i \neq G \implies |G| = |H_i| \cdot |G/H_i| \implies P \mid |G/H_i|$. (Note $p^r = p^s \cdot p^{r-s}$ where $s < r, r - s > 0$).

So

$$|X| = \sum_{i=1}^N |X_i| \sum_{i=1}^N |G/H_i| = \sum_{H_i = G} |G/G| + \sum_{H_i \neq G} |G/H_i| = |X^G| + \text{divisible by } P.$$

⊠

8 September 13, 2021

todo:missed this lecture

9 September 15, 2021

Recap from last time: there were two applications of the p-group congruence lemma.

(1) Let G be a p-group, then $Z(G) \neq \{1\}$. The proof idea is to let G act on itself. A corollary is that for G a p-group, $|G| = p^r$ for $r > 0$. This implies that there exists a normal subgroup $\mathbb{Z}/p \subseteq Z(G)$, so that $G/(\mathbb{Z}/p)$ has order p^{r-1}.

(2) Cauchy's theorem: Let G be finite and p be prime, and $p \mid |G|$. Then there exists a $g \in G$ such that $g^p = 1$. This is equivalent to the fact that $\mathbb{Z}/p \to G$ is a non-trivial homomorphism. The proof idea is that $\mathbb{Z}/p$ acts on $Y = G^p = \mathrm{Hom}_{\mathsf{Sets}}(\mathbb{Z}/p, G)$, and contained in this is $\mathbb{Z}/p$ acting on $X = \{(g_1, \cdots, g_p) \mid g_1 \cdots g_p = 1\}$. (The p-group lemma was applied here.)

9.1 Sylow theorems

This is the brief heuristic: let p be a prime and n be a positive integer. Then $n = p^r m$, $p \nmid m$. The Sylow theorems give a sor tof "analogue" for finite groups. Fix p a prime, G be finite, and $p \mid |G|$.

Definition 9.1. A **p-Sylow subgroup of** G is a subgroup $G_p \subseteq G$ such that:

- G_p is a p-group,
- $p \nmid |G/G_p|$.

Note. By Lagrange's theorem,

$$|G/G_p| \cdot |G_p| = |G|.$$

So the conditions for a p-Sylow subgroup is equivalent to saying $|G_p| = p^r$, where $|G| = p^r \cdot m$, $p \nmid m$.

Theorem 9.1 (Sylow I)**.** *Sylow subgroups exist, i.e., if $p \mid |G|$, there exists some $G_p \subseteq G$ a p-Sylow subgroup.*

This is the easiest Sylow theorem to parse, and probably the hardest one to prove.

Proof sketch of Theorem 9.1. The strategy is to proceed by induction.

(a) For all $1 \le s \le r$, we'll show there exists an $H_s \subseteq G$ with $|H_s| = p^r$. The case $s = 1$ is by Cauchy's theorem.

(b) We'll use some observations of p-groups to motivate our approach.

Definition 9.2. Suppose $H \subseteq G$. Then the **normalizer** $N_G(H)$ of H is defined by

$$\{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid ghg^{-1} \in H \text{ for all } h \in H\}.$$

Some easy checks are that $N_G(H)$ is a subgroup, H is normal in $N_G(H)$, and that $N_G(H)$ is the maximal subgroup of G in which H is normal.

Proposition 9.1. *Suppose that G is a p-group, $H \subsetneq G$ is a subgroup. Then $N_G(H) \neq H$.*

Proof of Proposition 9.1. Suppose $|G| = p^r$, $r \ge 1$. We'll proceed by induction on r. If $r = 1$, $G \simeq \mathbb{Z}/p$, and $H \subsetneq G \implies H = \{1\}$, and $N_G(H) = \mathbb{Z}/p$. Now assume the result for integers less than r, we'll prove it for r. Case 1 is that $Z(G) \subsetneq H$. Then there exists a $z \in Z(G)$ such that $z \notin H$. Clearly $z \in N_G(H)$, and we are done. Case 2 is when $Z(G) \subseteq H$. Then take $G_0 := G/Z(G)$, $H_0 := H/Z(G)$. As $Z(G)$ is nontrivial, $|G_0| = p^s$ for some $s < r$. We have $H_0 \subsetneq G_0$ which implies by induction that there exists a $g_0 \in N_{G_0}(H_0)$, $g_0 \notin H_0$. Lift g_0 to an element $g \in G$ and check that $g \in N_G(H)$, $g \notin H$. For the quotient projection $\pi\colon G \to G_0 = G/Z(G)$, for $h \in H$,

$$\pi(ghg^{-1}) = \pi(g)\pi(h)\pi(g^{-1}) = g_0\pi(h)g_0^{-1} \in H_0.$$

By $\pi^{-1}(H_0) = H$, which implies $ghg^{-1} \in H$. So $g \in N_G(H)$. This argument applies for nilpotent groups more generally. ⊠

Now for our actual problem: the strategy is to take $N_G(H_s)$, where $|H_s) = p^s$. We show that for $s < r$, $p^{s+1} \mid |N_G(H_s)|$, then we'll use Cauchy's theorem in $N_G(H_s)/H_s$.

10 September 17, 2021

Last time: we started showing that for G finite, $|G| = p^r \cdot m$ for $p \nmid m$, there exists $G_p \subseteq G$ with $|G_p| = p^r$ (a p-Sylow subgroup). By induction, we will show there exist subgroup

$$H_1 \subseteq H_2 \subseteq \cdots \subseteq H_r = G_p \subseteq G$$

such that $|H_i| = p^i$.

Digression. How did these Sylow theorems come about? When people were working on this in the 1900s, Sylow probably had tools like Cauchy's theorem and worked from there. Computing this is hard: if we have a group of order 1000, to show it has a subgroup of order 125, we need to check $\binom{1000}{3}$ subsets. The technique of choosing a normal subgroup of order 5, quotienting by it, etc, is powerful.

Last time: we argued that if we believe the theorem, then for $i < r$, $N_{G_p}(H_i)/H_i \subseteq N_G(H_i)/H_i$.

Lemma 10.1. *For $i < r$, $p \mid |N_G(H_i)/H_i|$.*

Assuming Lemma 10.1, then there exists a $\Gamma \subseteq N_G(H_i)/H_i$ being a subgroup of order p. Let $\pi\colon N_G(H_i) \to N_G(H_i)/H_i$, and define $H_{i+1} = \pi^{-1}(\Gamma)$. Then $H_i \subseteq H_{i+1}$ is a normal subgrouop, with $H_{i+1}/H_i \simeq \Gamma \simeq \mathbb{Z}/p$. This implies that

$$|H_{i+1}| = \underbrace{|H_i|}_{p_i} \cdot \underbrace{|H_{i+1}/H_i|}_{p}.$$

Proof of Lemma 10.1. The idea is to use the p-group congruence lemma. Let H_i be a p-group, and $X = G/H_i$. Then

$$|X| \equiv |X^{H_i}| \pmod p,$$

where $|X| = |G/H_i| = |G|/|H_i| = m \cdot p^{r-i} \equiv 0 \pmod p$. The homework this week tells us that $(G/H_i)^{H_i} \simeq N_G(H_i)/H_i$. The idea is that given an element $gH_i \in (G/H_i)^{H_i}$, this implies that for all $h \in H_i$,

$$\begin{aligned} ghH_i = gH_i &\iff \\ g^{-1}hgH_i = H_i &\iff \\ g^{-1}hg \in H_i &\iff \\ g \in N_G(H_i)&. \end{aligned}$$

Therefore

$$|N_G(H_i)/H_i| = |(G/H_i)^{H_i}| = |G/H_i| \pmod p.$$ ⊠

This concludes the proof of the first Sylow theorem. ⊠

There are other Sylow theorems, which address the question: How many p-Sylow subgroups are there? How do they compare?

Theorem 10.1 (Sylow II)**.** *All p-Sylow subgroups of G a finite group are conjugate, i.e., given $G_p, \widetilde{G_p} \subseteq G$ two p-Sylow subgroups, there exists a $g \in G$ such that*

$$\widetilde{G_p} = G_p g^{-1} = \mathrm{Ad}_g(G_p),$$

where $\mathrm{Ad}_g \colon G \to G$ is an isomorphism mapping G_p isomorphically onto G_p. In particular, we see that all p-Sylow subgroups are isomorphic.

Proof. We apply the p-group congruence lemma. The group will be G_p, and set $X = G/\widetilde{G_p}$. By the congruence lemma, $|X| = |X^{G_p}| \pmod p$, and $|X| = |G/\widetilde{G_p}| \neq 0$ because these are both p-Sylow subgroups. So $X^{G_p} \neq \emptyset$, which implies there exists some $g \in G$ such that for every $h \in G_p$, $h \cdot g \cdot \widetilde{G_p} = g \cdot \widetilde{G_p}$. Then

$$\begin{aligned} g^{-1}hg \cdot \widetilde{G_p} = g \cdot \widetilde{G_p} &\iff \\ g^{-1}hg \in \widetilde{G_p} &\iff \\ \mathrm{Ad}_{g^{-1}}(G_p) \subseteq \widetilde{G_p}& \end{aligned}$$

up to signs, and we are done. ⊠

Remark 10.1. This argument shows that any p-subgroup of G can be conjugated into a fixed p-Sylow subgroup.

11 September 20, 2021

Recap of last time: so far we were proving Sylow's theorems. Let G be a finite group, p be a prime, and $p \mid |G|$. The first Sylow theorem says that there exists a $G_p \subseteq G$, a p-Sylow subgroup (G_p is a p-group, and pt $|G/G_p|$). The idea of the proof is to use induction with Cauchy's theorem, with H actings on G/H.

The second Sylow theorem says that any subgroup $H \subseteq G$ of oreder p^s can be conjugated into G_p. In particular, any two p-Sylow subgroups are conjugate. A consequence of that is that they're automatically isomorphic. The idea of the proof is to consider the action of H on G/G_p.

A new question is this: how many p-Sylow subgroups are there? It is not always the case that there is a unique p-Sylow subgroup. Let n_p :=the number of p-Sylow subgroups of G.

Theorem 11.1 (Sylow III)**.**

(a) $n_p = |G/N_G(G_p)|$,
(b) n_p *divides* $|G/G_p|$,
(c) $n_p = 1 \pmod p$.

Corollary 11.1. $n_p = 1$ *iff* G_p *is normal in* G.

Proof of Corollary 11.1. In this case, by (a), we have

$$1 = n_p = |G/N_G(G_p)| \iff N_G(G_p) = G$$

by Lagrange's theorem. This is equivalent to the fact that G_p is normal. ⊠

n_p is always compatible with the restrictions (equal to $1 \pmod p$, always divides anything). But: sometimes this is the only integer compatible with the restrictions.

Example 11.1. Let p, q be two distinct primes, and let G be a group of order pq. Suppose $p < q$. Then we claim that $n_q = 1$. We know $n_q = 1 \pmod q$, and

$$n_q \mid |G/G_q| = |G|/|G_q| = pq/q = p.$$

We see that $n_q = 1$ or p, but since $p < q$, we have $n_q = 1$. In particular, any such G has a non-trivial normal subgroup of order q.

Proof of Theorem 11.1. Let $\Sigma_p := \{p\text{-Sylow subgroups of } G\}$. Then G acts on Σ_p by conjugation. By Theorem 10.1, this action is transitive (there is a unique orbit). Moreover, $G_p \in \Sigma_p$, and its stabilizer for this action of G is (by definition) $N_G(G_p)$. We then know that $\Sigma_p \simeq G/N_G(G_p)$ as a G-set. Then (a) follows:

$$n_p := |\Sigma_p| = |G/N_G(G_p)|.$$

Then (b) also follows:

$$|G/G_p| = |G/N_G(G_p)| \cdot |N_G(G_p)/G_p| = n_p \cdot |N_G(G_p)/G_p|.$$

For (c), we want to use the p-subgroup congruence lemma. Let G_p act on $\Sigma_p \simeq G/N_G(G_p)$. We obtain

$$n_p = |\Sigma_p| = |(\Sigma_p)^{G_p}| \pmod p.$$

We want to show that $\Sigma_p^{G_p} = \{G_p\}$. Suppose $\widetilde{G}_p$ is a p-Sylow subgroup in $\Sigma_p^{G_p}$. Unwinding this definition means that for all $g \in G_p$, $g\widetilde{G}_p g^{-1} = \widetilde{G}_p$. This means that $G_p \subseteq N_G(\widetilde{G}_p)$. Now let $H = N_G(\widetilde{G}_p)$. Clearly $\widetilde{G}_p \subseteq H \subseteq G$, this implies that $\widetilde{G}_p$ is a p-Sylow subgroup of H. Also, $\widetilde{G}_p$ is normal in H. By (a), $\widetilde{G}_p$ is the *unique* p-Sylow subgroup of H. But $G_p \subseteq H$ by assumption, and is a p-Sylow subgroup, so $G_p = \widetilde{G}_p$. ⊠

12 September 22, 2021

It's getting hard to continue without examples involving finite fields, so today we make a digression about other algebraic structures.

Definition 12.1. A **monoid** is a triple $(M, m, 1)$ where M is a set, a map $m\colon M \times M \to M$, $(x_1, x_2) \mapsto m(x_1, x_2) = x_1x_2$, and an element $1 \in M$ such that multiplication is associative and $1 \cdot x = x$ for all $x \in M$.

You can think of a monoid as a group without inverses. Homomorphisms of monoids are maps $\varphi\colon M_1 \to M_2$ with $\varphi(1_{M_1}) = 1_{M_2}$, $\varphi(x_1x_2) = \varphi(x_1)\varphi(x_2)$.

Example 12.1. Some examples of monoids:

(1) Any group is a monoid.
(2) $(\mathbb{R}^{\geq 1}, \text{mult})$ or $(\mathbb{R}, \text{mult})$ are monoids with unit one, but are not groups. $(\mathbb{R}^{>1}, \text{mult})$ has an associative multiplication, but no unit, so is not a monoid.

Definition 12.2. A **ring** A is a set A with two binary operations (maps $A \times A \to A$) denoted like multiplication and addition with $1 \in A$, such that

- $(A, \text{mult}, 1)$ is a monoid,
- (A, add) is an abelian group with unit $0 \in A$,
- multiplication and addition are distributive:

$$\begin{aligned} a(b+c) &= ab + ac, \\ (a+b)c &= ac + bc. \end{aligned}$$

Ring homomorphisms are maps of sets that are homomorphisms of monoids for multiplication and addition, i.e., $\varphi\colon A_1 \to A_2$ such that $\varphi(1_{A_1}) = 1_{A_2}$, $\varphi(ab) = \varphi(a)\varphi(b)$, $\varphi(a+b) = \varphi(a) + \varphi(b)$. A ring is **commutative** if multiplication is commutative.

Example 12.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all (commutative) rings. The set of $n \times n$ complex matrices, denoted $M_n(\mathbb{C})$, is non-commutative.

If A is a ring, then let $A^\times = \{a \in A \mid \exists a^{-1} \in A \text{ with } a \cdot a^{-1} = a^{-1} \cdot a = 1\}$ denote the **set of units** of A, which always forms a group under multiplication. Sometimes "ring" means "commutative ring". Sometimes people write "associative ring" to mean "reader, I want to consider non-commutative rings in particular here".

Definition 12.3. A **field** is a commutative ring k such that for all $x \in k$ either $x = 0$, or there exists an $x^{-1} \in k$ such that $x \cdot x^{-1} = 1$. So a field is a commutative ring with $k^\times = k \setminus \{0\}$.

By convention, $\{0\}$ is a ring with $0 = 1$, but it's not a field.

Example 12.3. $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all fields, but $\mathbb{Z}$ is not.

Suppose $\varphi\colon A \to B$ is a map of rings. Then $\ker(\varphi) := \varphi^{-1}(0)$. Observe that for $x, y \in \ker(\varphi)$, then $x + y \in \ker(\varphi)$. For $x \in \ker(\varphi), y \in A$, we have $x \cdot y, y \cdot x \in \ker(\varphi)$:

$$\varphi(xy) = \varphi(x) \cdot \varphi(y) = 0 \cdot \varphi(y) = 0.$$

Definition 12.4. A **two-sided ideal** $I \subseteq A$ is a subset closed under addition and left/right multiplication by elements of A, i.e., $x, y \in I \implies x + y \in I$, and $x \in I$, $y \in A$ implies $xy, yx \in I$. If A is commutative, we simply speak of ideals.

If $I \subseteq A$ is a two-sided ideal, there is a unique ring structrure on $A//I$ (the group quotient) such that the map $A \xrightarrow{\pi} A/I$ is a ring map. We need to check that we have addition on A/I as $I \subseteq A$ is a (necessarily) normal subgroup (under addition). For multiplication:

$$\begin{tikzcd} A \times A \arrow[r, "\text{mult}"] \arrow[d] & A \arrow[d, "\pi"] \\ \underset{=(A\times A)/(I\times I)}{A/I \times A/I} \arrow[r, dotted, "?"] & A/I \end{tikzcd}$$

We need that for all $a, b \in A$, all $x, y \in I$, $\pi(a+b) = \pi((a+x)\cdot(b+y))$. For the right hand side, $\pi(ab + xb + ay + xy) \implies xb + ay + xy \in I$. $\pi(ab) = \pi(ab + \text{something} \in I)$ which implies the equation.

Example 12.4. $\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}$ has a ring structure so $\mathbb{Z} \to \mathbb{Z}/n$ is a homomorphism.

13 September 24, 2021

Last time we did a bunch of algebraic stuff, like rings, fields, ideals, and so on.

Lemma 13.1. *Every ideal I of $\mathbb{Z}$ has form $n \cdot \mathbb{Z}$ for some $n \in \mathbb{Z}$.*

Proof. This was on the homework. But for the sake of the completeness, here's the proof. Option 1: $I = \{0\}$, and we are done. If $I \neq 0$, there exists some $x \in I$, $x > 0$ (since I is closed under additive inverses). Let n be the minimal positive element of I. Clearly $n\mathbb{Z} \subseteq I$. Our claim is that $n\mathbb{Z} = I$, or $I \subseteq n\mathbb{Z}$. If this were not true, there exists some positive $y \in I$ such that $y \notin n\mathbb{Z}$. Let m tbe the minimal positive element, if $m > n$ then $m - n \in I$, $m - n > 0$. So $m - n \in n\mathbb{Z}$ by the minimality of m, which implies $m \in n\mathbb{Z}$. Otherwise, $0 < m \leq n$ contradicting the minimality of n (unless $m = n$). ⊠

Corollary 13.1. *Given integers x, y with $\gcd(x, y) = d \geq 0$, there exists $\alpha, \beta \in \mathbb{Z}$ such that $\alpha x + \beta y = d$.*

Proof. Let I be the ideal $\mathbb{Z}x + \mathbb{Z}y$, i.e.: $\{\gamma x + \delta y \mid \gamma, \delta \in \mathbb{Z}\}$. We know that $I = D \cdot \mathbb{Z}$ for some $D \in \mathbb{Z}$. We can assume $D \geq 0$, by construction $\mathbb{Z}x \subseteq \mathbb{Z}D$, or $x \in \mathbb{Z}D$, also $y \in \mathbb{Z}D$. So $D \mid x$ and $D \mid y$, which implies $D \mid \gcd(x, y) = d$.

On the other hand, $\mathbb{Z}D = \mathbb{Z}x + \mathbb{Z}y \implies D = \alpha x + \beta y$ for some $\alpha, \beta \in \mathbb{Z}$. So the RHS is divisible by d, which implies $d \mid D$, and so $d = D$. ⊠

Corollary 13.2. *Given $n \in \mathbb{Z}$ and $m \in \mathbb{Z}$, then m maps to a unit of $\mathbb{Z}/n$ iff m is coprime to n.*

Proof. First, suppose $\gcd(m, n) = d > 1$. We want to show that m is not a unit mod n. This implies

$$m \cdot \frac{n}{d} = \frac{m}{d} \cdot d \cdot \frac{n}{d} = 0 \pmod{n}.$$

Note that $0 < \frac{n}{d} < n$ implies $\frac{n}{d}$ is not zero mood n. If m were invertible, we could multiply the above by m^{-1} which implies $\frac{n}{d} = 0 \pmod{n}$, a contraction. On the other hand, if m is coprime to n, this implies the existence of $\alpha, \beta \in \mathbb{Z}$ such that $\alpha m + \beta n = 1$. Reduce this mod n to see that $\alpha m = 1 \pmod{n}$, which implies $\alpha = m^{-1}$. ⊠

Corollary 13.3. *If p is prime, then $\mathbb{Z}/p$ is a field.*

Proof. Non-zero elements of $\mathbb{Z}/p$ are in bijection with $\{1, \cdots, p-1\}$ which are all coprime to p, which implies they map to units in $\mathbb{Z}/p$. ⊠

A note on notation: we denote $\mathbb{F}_p = \mathbb{Z}/p$ when we think about it as as field/ring, the finite field with p elements. A natural question to ask is; what does $\mathbb{F}_p^\times$ look like? The answer is that it's a cyclic group of order $p - 1$, i.e., $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)$ as groups non-canonically. We'll show this ... soon. First some digressions. Another note on notation: if A is a commutative ring, then

$$A[t] = \left\{ \sum_{i=0}^{n} a_i t^i \;\middle|\; a_i \in A \right\}.$$

This is the set of polynomials of one variable with coefficients in A. In fact, $A[t]$ is a ring. The setup is that that

$$\sum_{i=0}^{n} a_i t^i + \sum_{i=0}^{m} b_i t^i := \sum (a_i + b_i) t^i$$

and

$$\left(\sum_{i=0}^{n} a_i t^i \right) \left(\sum_{j=0}^{m} b_j t^j \right) = \sum_{j=0}^{m} \sum_{i=0}^{n} a_i b_j t^{i+j}.$$

For example, for $\lambda \in A$, $(1 + \lambda t^{10})(2 + 4 \cdot t^5) = 2 + 4t^5 + 2\lambda t^{10} + 4\lambda t^{15}$.

Definition 13.1. An **integral domain** (often called domain) is a commutative ring A where $xy = 0$ implies $x = 0$ or $y = 0$. We also require $0 \neq 1$.

Example 13.1. Here are some examples of integral domains:

(1) Any field is an integral domain.
(2) Any subring of a field is an integral domain, for example $\mathbb{Z} \subseteq \mathbb{Q}$ is an integral domain.
(3) $\mathbb{Z}/4$ is **not** an integral domain, since $2 \not\equiv 0 \pmod 4$ here, but $2 \cdot 2 \equiv 0 \pmod 4$.

Claim. *If A is an integral domain, then $A[t]$ is as well. A related claim is that for $f(t) \in A[t]$, let $\deg(f)$ be the minimal integer n such that $f(t) = \sum_{i=0}^{n} a_i t^i$, i.e., the maximal integer m such that the coefficient of t^m is nonzero. Then*

$$\deg(fg) = \deg(f) + \deg(g)$$

for all $f, g \in A[t]$.

Proof of both claims. Let

$$f = \underbrace{a_{\deg(f)}}_{\neq 0} t^{\deg(f)} + \underbrace{\cdots}_{\text{lower order terms}}, \quad g = \underbrace{b_{\deg(g)}}_{\neq 0} t^{\deg(g)} + \cdots .$$

This implies that

$$fg = \underbrace{a_{\deg(f)} g_{\deg(g)}}_{\neq 0 \text{ b/c } A \text{ is a domain}} t^{\deg(f)\deg(g)} + \underbrace{\cdots}_{\text{lower order terms}}.$$

$\boxtimes$

14 September 27, 2021

Lats time, we introduced the commutative ring $A[t] = \left\{ \sum_{i=0}^{N} a_i t^i \mid a_i \in A \right\}$ of polynomials in one variable t. We are headed to developing some field theory and properties of polynomials.

Definition 14.1. A **principal ideal domain**, or **PID**, is a commutative ring A that is a domain such that every ideal I is principal, i.e., $I = Ad$ for some $d \in A$.

Example 14.1. $\mathbb{Z}$ is a PID.

Proposition 14.1. *For k a field, $k[t]$ is a PID.*

Definition 14.2. A **Euclidian domain** is a pair (A, δ) where A is a commutative ring, $\delta \colon A \to \mathbb{Z}^{\geq 0}$ such that

- $\delta^{-1}(0) = \{0\}$,
- $\delta(xy) = \delta(x) \cdot \delta(y)$ for all $x, y \in A$,
- For every $f \in A$, the map $A_{<\delta(f)} \to A/f$ is surjective, where for $n \in \mathbb{Z}^{\geq 0}$, $A_{\leq n} := \{g \in A \mid \delta(g) < n\}$.

In other words, a Euclidian domain is a place where the Euclidian algorithm makes sense. The function of δ is some measure of "size" of the elements of A.

Example 14.2. If $A = \mathbb{Z}$, let $\delta = |\cdot|$, i.e., $\delta(m) := |m|$. Note that given $f \in \mathbb{Z}$ non-zero, then $\mathbb{Z}_{<|f|} = \{-f+1, -f+2, \cdots, f-2, f-1\} \subseteq \mathbb{Z}$ surjecting onto $\mathbb{Z}/f$. In fact, even $\{0, 1, \cdots, f-1\}$ surjects. For example, if a clock is represented as $\mathbb{Z}/12$, the fact that you can represent every element $0, \cdots, 11$ as an element of $\mathbb{Z}/12$ should be true, hence the surjection onto $\mathbb{Z}/f$ condition.

Remark 14.1. Sometimes we say A is a Euclidian domain to mean that there exists a δ making d into a Euclidian domain.

Before we prove Proposition 14.1, we prove two intermediary results.

Lemma 14.1. *$k[t]$ is a Euclidian domain.*

Lemma 14.2. *Any Euclidian domain is a PID.*

Proof of Lemma 14.1. Let $\delta(f) := 2^{\deg f}$, where $\deg f$ is assumed to be greater than zero (if not, let $\deg f = -\infty, 2^{-\infty} = 0$). (We can replace 2 with any integer greater than 1.) Clearly $\delta(f) = 0 \iff f = 0$. We also have

$$\begin{aligned}\delta(fg) &= 2^{\deg(fg)} \\ &= 2^{\deg(f)+\deg(g)} \\ &= 2^{\deg(f)} \cdot 2^{\deg(g)} \\ &= \delta(f) \cdot \delta(g).\end{aligned}$$

Given $f \in k[t]$ non-zero with $\deg f = d$, we want to show that the map $k[t]_{\deg<d} \to k[t]/f$ is surjective. Suppose $f = a_d t^d + \cdots + a_0$, then there a_d is non-zero implies a unit in k. $k[t] \cdot f = k[t] \cdot \frac{1}{a_d} \cdot f$ implies that we can replace f by $\frac{1}{a_d} f$ to assume f is **monic** (leading coefficient is1). Let $\pi\colon k[t] \to k[t]/f$ be the projection. We want to show that for every $g \in k[t]$, $\pi(g)$ is in $\pi\left(k[t]_{\deg<d}\right)$.

We proceed by induction on $\deg(g)$. If $\deg(g) < d$ we are done. Otherwise, we can write

$$g = b_e t^e + b_{e-1} t^{e-1} + \cdots + b_0$$

for $b_e \neq 0$ and some $e^{\geq d}$. Observe that

$$g - b_e \cdot t^{e-d} \cdot f = b_e t^e - b_e t^e + \text{lower order terms}, 0 \cdot t^e,$$

i.e., $\deg(g - b_e t^{e-d} \cdot f) < e$. This is pretty much the division algorithm. Therefore, by induction, there exists an $h \in k[t]_{<d}$ such that $\pi(h) = \pi(g - b_e t^{e-d} f)$. But the right hand side obviously equals $\pi(g)$ (since $b_e t^{e-d} f$ is a multiple of f), so we are done. ☒

Proof of Lemma 14.2. Let $I \subseteq A$ be an ideal. If $I = \{0\}$ we are done. Otherwise, let $d \in I$ be a non-zero element with minimal δ, i.e., $d \neq 0$, $d \in I$, $\delta(d) \leq \delta(d')$ for all $d' \in I$ non-zero. Note that this d exists since δ maps into the integers. Clearly $A \cdot dd \subseteq I$. We want to show that this is an equality. Choose some $f \in I$, we want to show that $f \in A \cdot d$.

Let π.?? todo: this proof By assumption on (A, δ), there exists a $\widetilde{f} \in A$ with $\delta(f) < \delta(d)$ and $\pi(\widetilde{f}) = \pi(f)$, i.e., $f = \widetilde{f} + g \cdot d$, $g \in A$. Observe that $\widetilde{f} = f - g \cdot d \in I$. Since $\delta(\widetilde{f}) < \delta(d)$, ☒

15 September 29, 2021

Today, we discuss prime and maximal ideals. The general idea is that we want to reduce commutative algebra to field theory. Fix A a commutative ring.

Definition 15.1. A **prime ideal** in A is an ideal $\mathfrak{p} \subseteq A$ such that $A/\mathfrak{p}$ is a domain. A **maximal ideal** in A is an ideal $\mathfrak{m} \subseteq A$ such that $A/\mathfrak{m}$ is a field.

Remark 15.1. Some remarks:

(1) Maximal implies prime ideal.
(2) Any prime ideal $\mathfrak{p} \subseteq A$ is not equal to A by convention. Essentially, $A/A = 0$, and we assume $1 \neq 0$ in a domain.
(3) $\{0\} \subseteq A$ is prime (resp maximal) iff A is a domain (resp field).

(4) Given a field K and a (resp surjective) homomorphism $\varphi\colon A \to K$, $\ker(\varphi)$ is prime (resp maximal) since $A/\ker(\varphi) \hookrightarrow K$.

(5) By definition, an ideal $\mathfrak{p} \subseteq A$ is prime iff

  (a) $\mathfrak{p} \neq A$,
  (b) For all $f, g \in A$, $fg \in \mathfrak{p}$ implies $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$.

(6) Claim: An ideal $\mathfrak{m} \subseteq A$ is maximal iff

  (a) $\mathfrak{m} \neq A$,
  (b) For all $\mathfrak{m} \subseteq I \subseteq A$ an ideal, $I = \mathfrak{m}$ or $I = A$.

Lemma 15.1. *A commutative ring A is a field iff A has exactly two ideals, the trivial ideal $\{0\}$ and A itself.*

Proof. Assume A is a field. Then $0 \neq 1$ implies $\{0\}$ and A are distinct ideals, so we have at least two ideals. Given $\{0\} \subsetneq I \subseteq A$ a non-zero ideal, take $f \in I$ non-zero. As A is a field, $\frac{1}{f} \in A$. Then for all $g \in A$, $g = \frac{g}{f} \cdot f \in I$ which implies $I = A$. Conversely, if we have exactly two ideals, then $0 \neq 1$ (or I would have one ideal) and for all $f \in A$ non-zero,

$$\begin{aligned} \underbrace{A \cdot f}_{\text{ideal}} \neq 0 &\implies A \cdot f = A \\ &\implies \exists f^{-1} \in A \text{ s.t. } f^{-1} \cdot f = 1 \\ &\implies A \text{ is a field.} \end{aligned}$$

⊠

Ideals generalize the notion of divisibility. The structure of the ideals under inclusion (for the integers for instance) is the same structure as ideals under divisibility. For a field, the idea of divisibility isn't really interesting (2 divides 1 because $2 \cdot \frac{1}{2} = 1$), but for domains they are, hence this result.

To prove the earlier claim, given $\mathfrak{m} \subseteq A$, it is easy to see that ideals $\mathfrak{m} \subseteq I \subseteq A$ correspond to ideals in $A/\mathfrak{m}$, where $I \mapsto I/\mathfrak{m}$.

Proposition 15.1. *Given A a non-zero commutative ring, there exists a maximal ideal $\mathfrak{m} \subseteq A$.*

Remark 15.2.

(1) This produces a non-zero map from A to a field, namely $A/\mathfrak{m}$.
(2) It follows that any $I \subsetneq A$ is contained in a maximal ideal: choose a maximal ideal in A/I, take its inverse image in A.
(3) The proof is non-constructive and uses Zorn's lemma.

Proof of Proposition 15.1. Let $S = \{\text{ideals } I \subseteq A, I \neq A\}$. As $A \neq \{0\}$, we have $S \neq \emptyset$ ($\{0\} \in S$). Consider S as partially ordered under inclusions $I \leq J \iff I \subseteq J$. Given a totally ordered subset $\Theta \subseteq S$, this leads to $I_\Theta := \bigcup_{J \in \Theta} J$.

Claim. *I_Θ is an ideal with $I_\Theta \neq A$.*

To check this claim, $x, y \in I_\Theta$ implies by total orderedness that there exists a $J \in \Theta$, $x, y \in J$, which implies $x + y \in J \subseteq I_\Theta$. Θ being non-empty implies that $0 \in I_\Theta$. For $x \in A$, $y \in I_\Theta$ implies that there exists a $J \in \Theta$ such that $y \in J$ which implies that $xy \in J \subseteq I_\Theta$. We have $I_\Theta \neq A$, otherwise $1 \in I_\Theta$ which implies the existence of a $J \in \Theta$ such that $1 \in J$, which implies $A \subseteq J \implies J = A$, contradicting the definition of S. Clearly $J \subseteq I_\Theta$ for all $J \in \Theta$, which implies I_Θ is a (least) upper bound for Θ. So Zorn's lemma applies and says there exists a $\mathfrak{m} \in S$ a maximal element. By what we did earlier, this means that $\mathfrak{m}$ is a maximal ideal. ⊠

16 October 4, 2021

Today is our first in person class! Today we'll do more on polynomials, discussing irreducibility and roots of polynomials. Let k be a field.

Definition 16.1. A polynomial $f \in k[t]$ is **irreducible** if the following conditions hold:

(1) $f \neq 0$,
(2) f is not a unit ($\deg f > 0$),
(3) whenever $f = f_1 \cdot f_2$, f_1 is a unit or f_2 is a unit.

A reminder that being a unit in this polynomial ring means a polynomial has degree zero.

Example 16.1. Some examples:

(1) $t \in k[t]$ is irreducible.
(2) $\deg(f) = 1$ implies that f is irreducible, since if $f = f_1 \cdot f_2$ then $\deg(f_1) + \deg(f_2) = 1$, therefore one of the numbers has to be zero.
(3) For $k = \mathbb{Q}, \mathbb{R}$, and $f(t) = t^2 + 1$, then f is irreducible. If $f = f_1 \cdot f_2$, then $\deg(f_i) = 0 \implies \deg(f_i) = 1$. We can assume that the f_i's are monic, which implies $f_i = t - \lambda_i$ for $\lambda_i \in k$. So $t^2 + 1 = (t - \lambda_1)(t - \lambda_2)$ for $\lambda_1, \lambda_2 \in \mathbb{Q}, \mathbb{R}$. This is impossible, because for $t = \lambda_1$, $\lambda_1^2 + 1 = 0$, a contradiction.

Remark 16.1. Sometimes it's convenient to think of "plug in λ for t" as considering the (unique) homomorphism $k[t] \xrightarrow{t \mapsto \lambda} k$, which is the identity on $k \subseteq k[t]$.

Note. A note on notation: for A a commutative ring, $f \in A$, then we denote $(f) := Af \subseteq A$, the ideal generated by f (repeated multiples of f). More generally, for $f_1, \cdots, f_n \in A$, we have $(f_1, \cdots, f_n) := Af_1 + \cdots + Af_n$ the ideal generated by the f_i.

Lemma 16.1. *A polynomial $f \in k[t]$ is irreducible if and only if (f) is maximal.*

Proof. Suppose that f is irreducible. We want to show that (f) is maximal. Suppose $(f) \subseteq I \subsetneq k[t]$ where I is some ideal. We want to show that $f = I$. We previously showed that $k[t]$ is a PID, so $I(g)$ for some non-unit polynomial g. Now

$$(f) \subseteq (g) \implies f \in (g) \implies f = g \cdot h$$

for some $h \in k[t]$. Since g is not a unit, and f is irreducible, then h is a unit. Furthermore,

$$h^{-1} \cdot f = g \implies g \in (f) \implies (g) \subseteq f \implies (f) = (g).$$

Conversely, suppose f is maximal. We want to show that f is irreducible. If $f = g \cdot h$ with g not a unit, we want to show that h is a unit. Suppose $(f) \subseteq (g) \subsetneq k[t]$, by maximality we have $(f) = (g)$. This implies there exists an $\eta \in k[t]$, or $\eta \cdot f = g$. Multiplying by (non-zero) h, we have

$$h \cdot \eta \cdot f = hg = f \underset{\text{domain}}{\implies} h \cdot \eta = 1.$$

So h is a unit with inverse η. ⊠

Remark 16.2. All of this is valid in any PID. In general, it's difficult to stare at a polynomial and tell whether it's irreducible or not. In degree zero and one this is trivial, and for degree two plug it into the quadratic formula and find the discriminant.

Lemma 16.2. *Let $f \in k[t]$ be non-zero. Then there exist $f_1, \cdots, f_n$ irreducible such that $f = \prod_{i=1}^n f_i$.*

Proof 1. This proof is for $k[t]$. If f is not irreducible, then $f = g \cdot h$ for g, h not units. If $\deg f = 0$ then we are done. If $\deg f = 1$ we have f irreducible so we are done. For g, h not units, $\deg(g), \deg(h) < \deg(f)$, which implies $g = g_1, \cdots, g_r$, $h = h_1, \cdots, h_s$ with g_i, h_j irreducible. So f is a product of irreducibles and we are done. ☒

Proof 2. This proof is valid for any PID. Given f non-zero, by last time there exists some maximal ideal $\mathfrak{m}_1 \supseteq (f)$. We have $\mathfrak{m}_1 = (f_1)$ for f_1 irreducible, which implies $f_1 \mid f$. If $\frac{f}{f_1}$ is a unit, then we are done. Otherwise, we can take the ideal $\left(\frac{f}{f_1}\right) \subseteq \mathfrak{m}_2 = (f_2)$ for f_2 irreducible. We get that $f_2 \mid \frac{f}{f_1}$- if $\frac{f}{f_1 f_2}$ is a unit we are done, otherwise we repeat. If the process $f = f_1 \cdots f_n \cdot \frac{f}{f_1 \cdots f_n}$ doesn't terminate (for all $n > 0, f_i$ irreducible), $f \in (f_1), f \in (f_1 f_2) \subseteq (f_1)$. Eventually,

$$(f_1) \supsetneq (f_1 f_2) \supsetneq \cdots$$

which is a strict inclusion since f_2 is not a unit, and so on. For $I = \bigcap_{n>0} (f_1 \cdot \cdots \cdot f_n)$, we want to show that $I = (0)$. This gives a contradiction since $f \in I$ with f non-zero. Since we are in a PID, this implies $I = (g) \subseteq (f_1 \cdots f_n)$ for all $n > 0$. We can then form $\frac{g}{f_1 \cdot \cdots \cdot f_n}$, where

$$(g) \subsetneq \left(\frac{g}{f_1}\right) \subsetneq \left(\frac{g}{f_1 f_2}\right) \subsetneq \cdots$$

Decreasing sequences of ideals are more subtle than increasing sequences of ideals, which we have transformed our increasing sequence into by the fact that we live in a PID. Form $J = \bigcup_{n>0} \left(\frac{g}{f_1 \cdots f_n}\right)$, and $J = (h)$. But this is a union, so $h \in \left(\frac{g}{f_1 \cdots f_n}\right)$ for some $n > 0$. Moving some symbols around,

$$\begin{aligned}
\frac{g}{f_1 \cdots f_{n+1}} &\in J = (h), \\
\frac{g}{f_1 \cdots f_{n+1}} &\in \left(\frac{g}{f_1 \cdots f_n}\right), \\
\frac{g}{f_1 \cdots f_{n+1}} &= \eta \cdot \frac{g}{f_1 \cdots f_n}.
\end{aligned}$$

Since we live in a domain, $1 = f_{n+1} \cdot \eta$, so f_{n+1} is a unit, a contradiction. ☒

That was a lot of manipulation, how do we set up the argument? There is some sort of built in "finiteness", the fact that we can't be divisible by an infinite amount of irreducible polys. So for ideals, the union eventually stabilizes, and the increasing sequence eventually stops.

17 October 6, 2021

Let's continue with polynomials.

Definition 17.1. If k is a field, then a **field extension** of k is a field K with a (necessarily injective) homomorphism $k \to K$. We denote K/k to mean that K is a field extension over k.

Example 17.1. $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$ are all field extensions.

Claim. *Given a field k and a polynomial $f \in k[t]$, there exists a field extension K/k such that f has a* root *in K, i.e., there exists $\lambda \in K$ such that $f(\lambda) = 0$.*

Example 17.2. If $k = \mathbb{R}$ and $f(t) = t^2 + 1$, then $K = \mathbb{C}$.

Proof. Choose some irreducible polynomial $g \in k[t]$ such that g divides f. Take $K := k[t]/g$. Note that we have a homomorphism $k \to k[t] \xrightarrow{\pi} k[t]/g = K$. Also note that K is a field, since $(g) \subseteq k[t]$ is maximal. Take $\lambda := \pi(t)$.Then $g(\lambda) = g(\pi(t)) = \pi(g(t)) = 0$. So $f = g \cdot h$ implies $f(\lambda) = g(\lambda) \cdot h(\lambda) = 0$. ☒

Example 17.3. Say $k = \mathbb{R}$ and $f(t) = t^2 + 1$. Then $K := \mathbb{R}[t]/t^2 + 1$. Let $i \in K$ be the image of t (what we just called λ). On the homework it was shown that every element of K can be written uniquely as $\alpha + \beta i$ for $\alpha, \beta \in \mathbb{R}$. Then

$$(\alpha + \beta i)(\gamma + \delta i) = \alpha\gamma + (\alpha\delta + \beta\gamma)i + \beta\delta(i^2).$$

Note that $i^2 = -1$ by construction since i solves $t^2 + 1 = 0$, so $K = \mathbb{C}$.

Example 17.4. Why do we need an irreducible polynomial in our proof? Take $f(t) = t^2 - 1 = (t-1)(t+1)$, and by the homework there is a natural map

$$\mathbb{R}[t]/(t-1)(t+1) \xrightarrow[\text{homework}]{\simeq} \underbrace{\mathbb{R}}_{\mathbb{R}[t]/t-1} \times \underbrace{\mathbb{R}}_{\mathbb{R}[t]/t-1},$$

which is not a field.

Given a polynomial $f \in [t]$ of degree n, does there exist an extension K/k such that f has n roots? The answer appears to be yes, but consider $f(t) = t^2$.

Proposition 17.1. *Given $f(t) \in k[t]$ monic of degree $n > 0$, there exists a field extension K/k and elements $\lambda_1, \cdots, \lambda_n \in K$ such that $f = \prod_{i=1}^n (t - \lambda_i)$.*

Remark: maybe the λ_i's are not all distinct.

Lemma 17.1. *Suppose k is a commutative ring, $f \in k[t]$, and $\lambda \in k$ is a root of f, i.e., $f(\lambda) = 0 \in k$. Then there exists a unique $g \in k[t]$ such that $g(t) \cdot (t - \lambda) = f(t)$.*

Proof. Define $\widetilde{f}(t) := f(t+\lambda)$, i.e., if $f(t) = a_n t^n + \cdots + a_0$, then $\widetilde{f}(t) = a_n(t-\lambda)^n + \cdots + a_0$ which we expand by the binomial theorem. Write $\widetilde{f}(t) = \widetilde{a}_n t^n + \widetilde{a_{n-1}} t^{n-1} + \cdots + \widetilde{a}_0$. By assumption, $\widetilde{a}_0 = \widetilde{f}(0) = f(\lambda) = 0$. Take $\widetilde{g}(t) := \widetilde{a}_n t^{n-1} + \widetilde{a_{n-1}} t^{n-2} + \cdots + \widetilde{a}_1$, where $\widetilde{g} \cdot t = \widetilde{f}$. Then $g := \widetilde{g}(t - \lambda)$, and

$$f = \widetilde{f}(t-\lambda) = \widetilde{g}(t-\lambda) \cdot (t-\lambda) = g \cdot (t - \lambda). \qquad \boxtimes$$

Proof of Proposition 17.1. We prove this by induction on degree, with the case deg 0 being trivial. By what we did earlier, there exists K_0/k and $\lambda_1 \in K_0$ such that $f(\lambda_1) = 0$. So we have this embedding $k[t] \subseteq K_0[t]$. By Lemma 17.1, $f(t) = (t - \lambda_1) \cdot g(t) \in K_0[t]$, where $\deg g = \deg f - 1 = n - 1$. By induction, suppose there exists K/K_0 with $\lambda_2, \cdots, \lambda_n \in K$ such that $g_9 t) = \prod_{i=2}^n (t - \lambda_i)$. Then $k \subseteq K_0 \subseteq K$, and $f(t) = \prod_{i=1}^n (t - \lambda_i)$ in $K[t]$. $\boxtimes$

Question: given f of degree n, when does f have n *distinct* roots?

Definition 17.2. We say $f \in k[t]$ of degree n is **separable** if there exists some field extension K/k such that f has n distinct roots in K.

Example 17.5. Let $k = \mathbb{Q}$.

(1) $t^2 + 1$ is separable.
(2) $t^2 - 1$ is separable.
(3) t^n for $n > 1$ is not separable.
(4) $t^3 + 2t^2 + t = t(t+1)^2$ is not separable.

18 October 8, 2021

Last time we ended with a question: given a field k and a polynomial $f \in k[t]$ of degree n, when is f *separable*, i.e., when does f have exactly n distinct roots in some extension field K/k?

Example 18.1. $t(t-1)$ or t^2+1 are (usually separable). $t^2, (t-1)^2, (t-1)^2(t^2+1)$ are not separable.

Definition 18.1. Given $f = a_n t^n + \cdots + a_0 \in k[t]$, define the **derivative** of f as $f'(t) := n a_n t^{n-1} + (n-1)a_{n-1}t^{n-2} + \cdots + a_1$.

Note that $(fg)' = f'g + fg'$.

Proposition 18.1. *For $f \in k[t]$ with $\deg(f) = n > 0$, the following are equivalent:*

(1) f is separable (has n distinct roots in some K/k),

(2) For every extension field K/k and $\lambda \in K$, $(t-\lambda)^2$ does not divide f.

(3) The ideal generated by f and f' is equal to the whole ring $k[t]$, or $(f, f') := k[t]f + k[t]f' = k[t]$. In other words, there exist $\alpha, \beta \in k[t]$ such that $\alpha f + \beta f' = 1$.

(4) There exists an extension field K/k such that $K[t]f + K[t]f' = K[t]$. In other words, there exist $\alpha, \beta \in K[t]$ such that $\alpha f + \beta f' = 1$.

Proof. We know (1) is equivalent to (2) because we know there exists some K/k and $c \in k^\times$, $\lambda_1, \cdots, \lambda_n \in K$ such that $f = c \cdot \prod_{i=1}^n (t-\lambda_i) \in K[t]$. Assuming (2), all roots must be distinct, so (2) implies (1). Assuming (1), if f is divisible by $(t-\lambda)^2$, this implies that $f = c(t-\lambda)^2 \cdot \prod_{i=1}^{n-2}(t-\lambda_i)$. The better way to say this is, by induction on degree, factorization into monic irreducible factors is unique.

Tautologically, the two halves of (3) and (4) are equivalent. (3) implies (4) because take the field extension in (4) to be k. Now we want to show that (2) implies (3). Now $(f, f') = (g)$ for some $g \in k[t]$ as $k[t]$ is a PID. WLOG, g is monic. If $g = 1$, we are done. Otherwise, $\deg(g) > 0$, so there exists some extension field K/k where g has a root by last time. The claim is that $(t-\lambda)^2$ divides f in $K[t]$ in this case, giving a contradiction. We know $(t-\lambda) \mid g \mid f$, which implies that $(t-\lambda) \mid f$. Let $\widetilde{f} := \frac{f}{(t-\lambda)}$, we want to see that λ is a root of $\widetilde{f}$. In other words, $f = \widetilde{f} \cdot (t-\lambda)$. By the product rule, $f' = (\widetilde{f})'(t-\lambda) + \widetilde{f} \cdot 1$. Then $(t-\lambda) \mid f'$, and

$$0 = f'(\lambda) = (\widetilde{f})'(\lambda) \cdot (\lambda - \lambda) + \widetilde{f}(\lambda).$$

This implies $\widetilde{f}(\lambda) = 0$, and $(t-\lambda) \mid \widetilde{f}$. Multiplying through, $(t-\lambda)^2 \mid f$. So (2) implies (3). Now we want to show that (3) implies (2), which is the same kind of idea. Suppose $\alpha f + \beta f' = 1$, and suppose that K/k and $\lambda \in K$ such that $(t-\lambda)^2 \mid f$. Then $f = (t-\lambda)\widetilde{f}$ with $\widetilde{f}(\lambda) = 0$. Then $f' = 1\widetilde{f} + (t-\lambda)\widetilde{f}$ which implies $f'(\lambda) = \widetilde{f}(\lambda) = 0$. This implies that $\alpha(\lambda)f(\lambda) + \beta(\lambda)f'(\lambda) = 1$, so $0 = 1$, a contradiction.

It remains to show that (4) implies (2), here is the sketch. The idea is that given some K and $\alpha f + \beta f' = 1$ in $K[t]$, in (2), given $\widetilde{K}$, $\lambda \in \widetilde{K}(t-\lambda)^2 \mid f$. The claim is that there exists a non-zero commutative ring A and embeddings

$$\begin{tikzcd}
& A & \\
K \arrow[ur] & & \widetilde{K} \arrow[ul] \\
& k \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

We skip showing that $K \otimes_k \widetilde{K} = A$. Define $\widetilde{\widetilde{K}} := A/$ a maximal ideal means that $\widetilde{\widetilde{K}}$ is a field, so we have embeddings

$$\begin{tikzcd} & \widetilde{\widetilde{K}} \arrow[dl] \arrow[dr] & \\ K \arrow[ur] \arrow[dr] & & \widetilde{K} \arrow[ul] \arrow[dl] \\ & k \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Run (3) implies (2) in $\widetilde{\widetilde{K}}$, and we are done. $\boxtimes$

Given a field k, there is an important invariant $\mathrm{char}(k)$, the **characteristic** of k. Either $\mathrm{char}(k) = 0$, or $\mathrm{char}(k)$ is some prime number. The construction is as follows: for every A a ring, there exists a unique ring homomorphism $\mathbb{Z} \xrightarrow{i_A} A$, where $0 \mapsto 0, 1 \mapsto 1$, $2 \mapsto 2 := 1 + 1$ ($\mathbb{Z}$ is the initial object for Ring). If k is a field, then $\ker(i_k) = (p) \subseteq \mathbb{Z}$, which is sprime because $\mathbb{Z}/\ker(i_k) \hookrightarrow k$. This p is the characteristic of k. For $\mathbb{F}_p := \mathbb{Z}/p$, this has characteristic p. $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ have characteristic 0, since $\mathbb{Z}$ maps injectively into these fields.

19 October 11, 2021

I missed this class so I'm transcribing John's notes. Fix k a field of characteristic $p \geq 0$. Recall that a field of characteristic 0 means that repeated addition of any non-zero element is nonzero. For example, $\mathbb{R}, \mathbb{Q}$, and $\mathbb{C}$ are fields of characteristic 0, while $\mathbb{F}_p = \mathbb{Z}/p$ has characteristic p.

Definition 19.1. For k a field and $n \geq 1$, define $\mu_n(k) := \{\zeta \in k \mid \zeta^n = 1\}$ to be the set of n**th roots of unity** of k.

Note that $\mu_n(k)$ is a group, since for $\zeta, \widetilde{\zeta} \in \mu_n(k)$ implies $\zeta\widetilde{\zeta} \in \mu_n(k)$, similarly $\zeta^{-1} \in \mu_n(k)$.

Definition 19.2. A group is **cyclic** if there is an isomorphism $G \simeq \mathbb{Z}/n$ for some $n \geq 0$.

Example 19.1. Let $k = \mathbb{C}$, then $\mu_n(k) = \{e^{2\pi i/n} \mid n \in \mathbb{Z}\}$. In general, $\mu(\mathbb{C}) \simeq \mathbb{Z}/n$ as a group, so $\mu(\mathbb{C})$ is cyclic of order n.

Proposition 19.1. *Let k be a field of characteristic p. Then*

(1) For all $n \geq 1$, $\mu_n(k)$ is cyclic,

(2) Any finite subgroup $G \subseteq k^\times$ is contained in $\mu_n(k)$ for some n,

(3) Any finite subgroup of $k^\times$ is cyclic,

(4) If n is coprime to p (vacuously true for $p = 0$), then there exists a field extension K/k with $|\mu_n(k)| = n$,

(5) If $n = p^r n_0$ where $p \nmid n_0$, $\mu_n(k) = \mu_{n_0}(k)$.

Example 19.2. If k has characteristic $\neq 2$, then $\mu_2(k) = \{-1, 1\}$ (in the characteristic two case, $\mu_2(k) = \{1\}$).

Corollary 19.1. *$\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)$ as a group, i.e., $\mathbb{F}_p^\times$ is cyclic.*

Proof. To show (4), for n coprime to p, let $f(t) := t^n - 1$. Then f and f' are coprime because f is separable, so we have some field extension K/k with f having n distinct roots for $\deg(f) = n$, which implies $|\mu_n(k)| = n$. For (1), assume that $|\mu_n(k)| = n$, we want to show that $\mu_n(k)$ is cyclic. Suppose $d \mid n$, then $(t^d - 1)$ divide $(t^n - 1)$. Then every dth root of unity is an nth root of unity, and $|\mu_d(k)| = d$. $\boxtimes$

20 October 13, 2021

A digression on counting.

Definition 20.1 (Euler's φ-function)**.** For $n \geq 1$, $\varphi(n) = |\{1 \leq m \leq n \mid \gcd(m, n) = 1\}$.

For example, $\varphi(1) = 1$, for $n = p$ a prime, $\varphi(p) = p - 1$, and $\varphi(8) = 4$. Here is why this function is significant:

Lemma 20.1. $\varphi(n) = |(\mathbb{Z}/n)^\times|$.

Proof. If m is coprime to n, then there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha m + \beta n = 1$ which implies m is a unit $\pmod n$. Conversely, if m is a unit $\pmod n$, then there exists an $\alpha \in \mathbb{Z}$ such that $am = 1 \pmod n$, which implies the existence of a $\beta \in \mathbb{Z}$ such that $\alpha m + \beta m = 1$, which implies $\gcd(m, n) = 1$. So

$$\underset{\{m|\gcd(m,n)=1\}}{\overset{\subseteq}{\{1, \cdots, n\}}} \ \underset{\xrightarrow{\sim}}{\xrightarrow{\sim}} \ \underset{(\mathbb{Z}/n)^\times}{\overset{\subseteq}{\mathbb{Z}/n}},$$

and we are done. ⊠

Lemma 20.2. $(\mathbb{Z}/n)^\times = \{m \in \mathbb{Z}/n \mid \operatorname{ord}(m) = n\}$.

Proof. Recall that for G a finite group, the order of an element g is defined as $\operatorname{ord}(g) = \min\{r > 0 \mid g^r = 1\}$. For $m \in \mathbb{Z}/n$, $\operatorname{ord}(m) = d$, $d \mid n, d \neq n$. This implies that $m + \cdots + m$ (d-times) $= m \cdot d = 0$, and $d < n$ implies that $d \neq 0$ so m is not a unit. Conversely, if $\operatorname{ord}(m) = n$, this implies that $d \cdot m \neq 0$ for all $d \mid n$, $d \neq n$. Let $\delta := \gcd(m, n)$. Then $\frac{n}{\delta} \mid n$, OTOH

$$m \cdot \frac{n}{\delta} = \frac{m}{\delta} \cdot \delta \cdot \frac{n}{\delta} = \frac{m}{\delta} \cdot n = 0 \implies \frac{n}{\delta} = n \implies \delta = 1 \implies \gcd(m, n) = 1 \implies m \in (\mathbb{Z}/n)^\times. \qquad ⊠$$

Remark 20.1. What this argument really shows is that $\{m \in \mathbb{Z}/n \mid \operatorname{ord}(m) = d\} = \{m \in \mathbb{Z}/n \mid \gcd(m, n) = \frac{n}{d}\}$.

Corollary 20.1. $\sum_{d|n} \varphi(d) = n$.

Proof. It is equivalent to show that $\sum_{d|n} \varphi\left(\frac{n}{d}\right) = n$ counts $|\{1 \leq m \leq n \mid \gcd(m, nd) = d\}$. ⊠

Example 20.1. If $1 \mid p$ is prime, $\varphi(p) = p - 1$, and $\varphi(1) + \varphi(p) = p$ as stated.

Now we return to roots of unity. For any field k such that $|\mu_n(k)| = n$, $\mu_n(k) \simeq \mathbb{Z}/n$. We'll prove this by induction on n. The case $n = 1$ is vacuous, assume that the claim is true for all $1 \leq m < n$. Last time we showed that $d \mid n$, $|\mu_d(k)| = d$. Note that for any root of unit, $\zeta \in \mu_n(k)$, $\zeta^n = 1$ implies that $\operatorname{ord}(\zeta) \mid |n$.

Claim. *For every $d \mid n$, $d \neq n$, $|\{\zeta \in \mu_n(k) \mid \operatorname{ord}(\zeta) = d\zeta\}| = \varphi\left(\frac{n}{d}\right)$.*

Proof. If $\operatorname{ord}(\zeta) = d \mid n, d \neq n$ implies that $\zeta^d = 1$ which implies $\zeta \in \mu_d(k)$. By induction, $\mu_d(k) \simeq \mathbb{Z}/d$. From before, we know that there are exactly $\varphi(d)$ elements of order exactly d in $\mathbb{Z}/d \simeq \mu_d(k)$. ⊠

Corollary 20.2. *There are exactly $\varphi(n)$ many $\zeta \in \mu_n(k)$ such that* $\operatorname{ord}(\zeta) = n$.

Proof. We have

$$\begin{aligned} n &= \sum_{d|n} |\{\zeta \in \mu_n(k) | \operatorname{ord}(\zeta) = d\}| \\ &= \sum_{\substack{d|n \\ d\neq n}} |\{\operatorname{ord}\zeta = d\}| + |\{\zeta \mid \operatorname{ord}(\zeta) = n\}| \\ &= \underset{d\neq n}{d} \mid n\varphi(d) + \text{ mystery term.} \end{aligned}$$

We showed that $\sum_{d|n} \varphi(d) = n$, which implies that $n - \sum_{d|n, d\neq n} \varphi(d) = \varphi(n) =$mystery term. ⊠

The key point is that there exists a $\zeta \in \mu_n(k)$ such that $\operatorname{ord}(\zeta) - n$, in fact, $\varphi(n)$ such elements. This leads to a map $\mathbb{Z}/n \to \mu_n(k), 1 \mapsto \zeta$. $\operatorname{ord}(\zeta) = n$ implies this map is injective, and therefore bijective. This could be an approach to showing a group is $\mathbb{Z}/n$– list all the divisors and count their orders.

Lemma 20.3. *Let A be a commutative ring with $p = 0$ (with $p > 0$ a prime). Define the Frobenius map $\varphi \colon A \to A$ by $f \mapsto f^p$. Then φ is a homomorphism.*

Proof. Clearly $\varphi(fg) = \varphi(f)\varphi(g)$. To show additivity, we have

$$\varphi(f+g) := (f+g)^p = f^p + \binom{p}{1} f^{p-1} g + \cdots + \binom{p}{p-1} f g^{p-1} + g^p.$$

By a previous homework, $\binom{p}{i} \equiv 0 \pmod{p}$ for $0 < i < p$, so this whole picture is equivalent to $f^p + g^p = \varphi(f) + \varphi(g)$. More on this next time. $\boxtimes$

References

[**Fra03**] John Fraleigh. *A First Course in Abstract Algebra, 7th edition.* 2003.