Math 6310. Algebra

Taught by David Zywina

Notes by Linus Setiabrata

This course is the first semester of the graduate algebra sequence at Cornell University, as it was taught in the Fall semester of 2018. Please let me know if you spot any mistakes! These notes are probably quite far from being typo-free. Most things in [blue font square brackets] are personal comments. Most things in [red font square brackets] are (important) announcements. David Mehrle's wonderful Algebraic Number Theory notes inspired me to do this.

Last edited May 20, 2020. Theorem numbering unchanged since Dec 3, 2018.

Contents

1 Groups

1.1 Aug 24, 2018

This course has a blackboard page with some info on it. You can get some course details if you email Prof Zywina. [There is some homework due every Friday.] The first one will be until September 7, so 14 days from now, and there will be a takehome final (namely, a big homework). There are some "interesting" questions to justify not-having-a-midterm.

The main book is Dummit/Foote, but we won't follow it exactly. There are also a bunch of other books at blackboard that you can get.

This course is "very serious". In particular, it's not aimed at undergraduate students. This is a 2nd course in abstract algebra. [You know: groups, rings, modules, fields.]

We have a TA who has office hours and does other TA things (the TA is Avery St. Dizier).

Group Actions

Let G be a group (multiplicative with 1). A (left) group action of G on a set X is a map $G \times X \to X$, that is, $(g, x) \mapsto g \cdot x = gx$, such that

a) $g_1(g_2x) = (g_1g_2)x$ for $g_1, g_2 \in G$ and $x \in X$.

b) $1 \cdot x = x$ for $x \in X$.

For $g \in G$, define the map $\varphi_g \colon X \to X$ given by $x \mapsto gx$. Using (a) and (b), we have

- $\varphi_{g_1g_2} = \varphi_{g_1} \circ \varphi_{g_2}$
- $\varphi_1 = \mathrm{id}_X$

This defines a map $\varphi\colon G \to S_X$ by $g \mapsto \varphi_g$. Here S_X is the group of permutations of X, which we will sometimes denote $\mathfrak{S}_X$ or Sym_X. One finds that φ is a homomorphism. Conversely, a homomorphism $G \to S_X$ defines a group action (by $g \circ x := \varphi_g(x)$). Sometimes this is useful for succinctness reasons.

Next semester we'll replace S_X with $\mathrm{Aut}(V)$ (automorphisms of a vector space) when we do representations.

Remark 1.1.1. There are right actions (we defined left actions). You can guess what they're going to be:

a) $(xg_1)g_2 = x(g_1g_2)$

b) $x1 = x$.

But the theories are the same because a right action gives rise to a left action by $g * x := xg^{-1}$.

Group actions are intimately linked with the structure of G (we'll get to that on Monday).

The action of G on X (sometimes denoted by $G \circlearrowleft X$) breaks x up into orbits. Say $x \sim y$ if $x = gy$ for $g \in G$. Observe that $\sim$ is an equivalence relation:

- $x \sim x$ (reflexive)
- $x \sim y \iff y \sim x$ (symmetric)
- $x \sim y$ and $y \sim z$ implies $x \sim z$ (transitive)

This equivalence relation breaks X into pieces (these are our orbits):

Definition 1.1.2. The G-orbit (or just orbit, when the group is clear) of G on X containing $x \in X$ is $\{y \in X : x \sim y\} = \{gx : g \in G\} = G \cdot x$ (sometimes called the equivalence class of X).

Definition 1.1.3. Let $G \backslash X$ be the set of G-orbits in X.

We in fact have

$$X = \bigsqcup_{\mathcal{O} \in G \backslash X} \mathcal{O},$$

that is, X is partitioned into disjoint orbits, and each $\mathcal{O}$ has a G-action.

Definition 1.1.4. We say G acts transitively on X if for any $x, y \in X$, we have $y = gx$ for some $g \in G$. Equivalently, $G \backslash X$ has only one orbit.

Each G-orbit has a transitive G-action.

Example 1.1.5. Let $X = G$. Define the group action $g * x = gxg^{-1}$ (conjugation by g). Then $\varphi \colon G \to \operatorname{Aut}(G) \subseteq S_G$. We will define $\operatorname{Inn}(G) := \varphi(G)$ to be the inner automorphisms of G; it turns out $\operatorname{Inn}(G) \trianglelefteq \operatorname{Aut}(G)$. We will define $\operatorname{Out}(G) := \operatorname{Aut}(G)/\operatorname{Inn}(G)$, and it turns out that

$$\operatorname{Out}(S_n) \cong \begin{cases} 1 & \text{if } n \neq 6 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } n = 6 \end{cases}.$$

In homework 2 we'll construct an automorphism of S_6 that is not given by conjugation.

Example 1.1.6. Let $X = G$. Define the group action $g \cdot x := g \cdot x$, ie. let G act on itself by left multiplication. This gives an injective homomorphism $G \hookrightarrow S_G$ (since it sends 1 to the identity in S_G). This is a theorem of Cayley: every finite group is isomorphic to a subgroup of S_n for some n.

Example 1.1.7. Let $G = \{z \in \mathbb{C}^\times : |z| = 1\} = S^1$ and $X = \{z \in \mathbb{C} : |z| \leq 1\}$. Then $G \circlearrowright X$ by rotation.

Example 1.1.8. $S_n \circlearrowright [n] := \{1, 2, \ldots, n\}$ which induces the homomorphism $S_n \to S_{[n]} = S_n$ (given by id_{S_n}).

Example 1.1.9. Take a subgroup H of G. Then G acts by left multiplication on the cosets $G/H = \{gH : g \in G\}$. This will be a key example (and in his mind, the "only" example).

Groups act on many things (at least, they act on themselves, and in practice, they generally naturally act on many other things). Group actions sometimes gives information about the group itself.

Definition 1.1.10. Take $x \in X$. Define

$$G_x := \{g \in G : gx = x\};$$

it is the stabilizer of x.

In fact, G_x is a subgroup of G. Define a (surjective) map $f \colon G \to G \cdot x$ via $g \mapsto g \cdot x$. Take $g, h \in G$. Then

$$f(g) = f(h) \iff gx = hx \iff (h^{-1}g)x = x \iff h^{-1}g \in G_x \iff g \in hG_x \iff gG_x = hG_x$$

so the map $\bar{f} \colon G/G_x \to Gx$ given by $gG_x \mapsto gx$ is a bijection. Also, it respects G-actions: G acts on both G/G_x and Gx, and $\bar{f}(ga) = g\bar{f}(a)$[such maps are sometimes called "G-equivariant"]. So group actions and subgroups are intimately linked. Next time we'll explore the following:

There is a correspondence

$$\{\text{transitive sets with a } G\text{-action}\}/\text{isomorphism} \longleftrightarrow \{\text{subgroups of } G\}/\text{conjugacy}$$

and if we can find interesting actions we can find interesting subgroups, and vice versa. So actions give you a way of attacking group theory.

1.2 Aug 27, 2018

Last time:

Let G be a group acting on a set X (so think $\varphi\colon G \to S_X$).

For $x \in X$, we defined

- $G \cdot x = \{gx \colon g \in G\}[\subseteq X]$ "a G-orbit"
- $G_x = \{g \in G \colon gx = x\} \leq G$ "stabilizer of x"

We have a bijection

$$\begin{aligned} G/G_x &\xrightarrow{\sim} G \cdot x \\ gG_x &\mapsto gx \end{aligned}$$

that respects the G-actions.

The key example is G/H with $H \leq G$, and G acting by left multiplication. Then

$$\begin{aligned} G_{aH} &= \{g \in G \colon g \cdot aH = aH\} \\ &= \{g \in G \colon a^{-1}ga \in H\} \\ &= aHa^{-1}. \end{aligned}$$

Assume X is finite and $x_1, \ldots, x_h$ are representatives of the G-orbits. Then

$$|X| = \sum_{i=1}^{h} |G \cdot x_i|$$

because X is the disjoint union of the $G \cdot x_i$, and also

$$|X| = \sum_{i=1}^{h} [G : G_{x_i}]$$

(and notice that the terms on the right side all divide $|G|$).

Example 1.2.1. Fix integers $0 \leq k \leq n$. Say that

$$X = \binom{[n]}{k} := \{A \subseteq [n] := \{1, 2, \ldots, n\} \colon |A| = k\}.$$

Then $G = S_n$ acts on X transitively. Pick a representative (any element works, since the action is transitive), say $A_0 = [k]$, then $G_{A_0} = S_{[k]} \times S_{[n] \setminus [k]}$. Then

$$|X| = [G \colon G_{A_0}] = \frac{|G|}{|G_{A_0}|} = \frac{n!}{k!(n-k)!}.$$

"Not groundbreaking."

Proposition 1.2.2. *Let H be a subgroup of a finite group G. Suppose that $[G : H]$ is equal to the smallest prime p dividing $|G|$. Then H is a normal subgroup.*

Proof. We have an action $G \circlearrowleft G/H$, and $\varphi\colon G \to S_X \cong S_p$ (since $|X| = [G : H] = p$). Thus the first isomorphism theorem gives

$$G/\ker(\varphi) \hookrightarrow S_p$$

where the cardinality of $G/\ker(\varphi)$ is not divisible by any $q < p$ [because $|G/\ker(\varphi)|$ divides $|G|$, and $|G|$ is not divisible by any $q < p$], and $|S_p| = p! = p(p-1)!$. This implies that $|G/\ker(\varphi)| \in \{1, p\}$. But

$|G/\ker(\varphi)| \neq 1$ because G acts on X transitively. So $|G/\ker(\varphi)| = p$. Notice that $\ker(\varphi)$ consists of the elements of G that act trivially on G/H, so $\ker(\varphi) \subseteq G_{1\cdot H} = H$. Thus

$$\underbrace{\ker(\varphi) \subseteq \overbrace{H \subseteq G}^{\text{index } p}}_{\text{index } p}$$

so $H = \ker(\varphi)$, which is normal in G. □

Proposition 1.2.3 (Burnside's Lemma). *Let G be a finite group acting on a finite set X. For $g \in G$, define $X^g := \{x \in X : gx = x\}$. Then*

$$|G\backslash X| = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Observe that the left side counts the number of G-orbits of X, whereas the right side counts the average number of elements fixed by $g \in G$.

Proof. It suffices to prove this for each orbit of X. So G acts transitively, and without loss of generality $X = G/H$.

$$\begin{aligned}\sum_{g\in G}|X^g| &= \sum_{g\in G}\sum_{\substack{x\in X\\ gx=x}} 1\\ &= \sum_{x\in X}\sum_{\substack{g\in G\\ gx=x}} 1\\ &= \sum_{x\in X}|G_x|\\ &= \sum_{x\in X}|H|\\ &= |X||H| = |G/H|\cdot|H| = |G|\end{aligned}$$

where the fourth equality is true since $G_{aH} = aHa^{-1}$, and in particular $|G_{aH}| = |H|$. □

Corollary 1.2.4 (Jordan's Lemma). *Let G be a finite group acting transitively on a set X with $|X| \geq 2$. Then there exists a $g \in G$ that fixes no points in X.*

(Such $g \in G$ are sometimes called "derangements")

Proof. Suppose not, so $|X^g| \geq 1$ for all $g \in G$. By Burnside,

$$1 = \frac{1}{|G|}\sum_{g\in G}|X^g| \geq \frac{1}{|G|}\sum_{g\in G} 1 = 1$$

but we have $|X^1| = |X| \geq 2$. □

Corollary 1.2.5 ([also] Jordan's Lemma). *Let G be a finite group. If H is a proper subgroup of G, then then there is a conjugacy class C of G such that*

$$H \cap C = \emptyset.$$

Remark 1.2.6. This is false for infinite groups. Also, when Prof Zywina does Galois theory, this is what he uses to show that a subgroup $H \leq G$ is actually equal to G: he shows it hits every conjugacy class.

Proof of Corollary 1.2.5. There exists $g \in G$ that does not fix any points in $X = G/H$. This says that

$$\begin{aligned}&gaH \neq aH \text{ for } a \in G\\ \implies &a^{-1}ga \notin H \text{ for } a \in G\\ \implies &H \cap C = \emptyset,\end{aligned}$$

where C is the conjugacy class of g in G. □

p-groups

Fix a prime p.

Definition 1.2.7. A finite group is a $\underline{p\text{-group}}$ if its cardinality is a power of p.

Some examples include $\mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_r}\mathbb{Z}$, and the matrix group

$$\left\{ \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \right\} \subseteq \mathrm{GL}_3(\mathbb{F}_p),$$

which has order p^3.

Remark 1.2.8. There are 49,487,365,422 groups of order 2^{10} up to isomorphism. Also, there are 11,759,892 groups of order $< 2^{10}$. It's a folklore conjecture that "most" finite groups are 2-groups.

Proposition 1.2.9. *Let G be a p-group acting on a finite set X. Define $X^G := \{x \in X : gx = x, \forall g \in G\}$. Then*

$$|X| \equiv |X^G| \pmod{p}.$$

Remark 1.2.10. Usually $|X^G|$ is mysterious and you use the proposition to show it's not empty by counting $|X| \pmod{p}$.

Proof of Proposition 1.2.9. Take any G-orbit $\mathcal{O} \subseteq X \backslash X^G$ (notice that $G \circlearrowleft X \backslash X^G$). Then

$$|\mathcal{O}| = |G \cdot x| = [G : G_x] = p^k \qquad (G \text{ is a } p\text{-group})$$

Notice that $|\mathcal{O}| > 1$, and $|\mathcal{O}| \equiv 0 \pmod{p}$. We have

$$X \backslash X^G = \bigsqcup_{\mathcal{O} \subseteq X \backslash X^G} \mathcal{O},$$

so

$$|X| - |X^G| = |X \backslash X^G| = \sum_{\mathcal{O} \subseteq X \backslash X^G} |\mathcal{O}| \equiv 0 \pmod{p}$$

□

Proposition 1.2.11 (Cauchy)**.** *Let G be a finite group and let p be a prime dividing $|G|$. Then G has an element of order p.*

Proof. Define

$$X = \{(g_1, \ldots, g_p) \in G^p : g_1 \ldots g_p = 1\}$$

and observe that $\mathbb{Z}/p\mathbb{Z} \circlearrowleft X$ by $[1] * (g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1})$ since

$$g_p g_1 \ldots g_{p-1} = g_p \underbrace{(g_1 \ldots g_p)}_{=1} g_p^{-1} = 1.$$

Then $|X| = |\mathbb{Z}/p\mathbb{Z}|^p \equiv 0 \pmod{p}$, and $X^{\mathbb{Z}/p\mathbb{Z}} = \{(g, \ldots, g) : g \in G, g^p = 1\}$. Then

$$\{g \in G : g^p = 1\} = |X^{\mathbb{Z}/p\mathbb{Z}}| \equiv |X| \equiv 0 \pmod{p}.$$

Since $X^{\mathbb{Z}/p\mathbb{Z}}$ is nonempty (it contains $(1, 1, \ldots, 1)$), there is $g \in G \backslash \{1\}$ such that $g^p = 1$. □

1.3 Aug 29, 2018

[There are Office Hours, on Thursdays at 12:30-2:30 in his office.]

Last time, we discussed:

Theorem 1.3.1 (Cauchy)**.** *For a finite group G and a prime p dividing $|G|$, there is a $g \in G$ of order p.*

A major tool to prove this theorem is the following

Proposition 1.3.2. *Let G be a p-group acting on a finite set X. Then $|X| \equiv |X^G| \pmod{p}$.*

There are some generalizations of these, called the three Sylow Theorems.

Sylow Theorems

We begin with

Proposition 1.3.3 (Lagrange)**.** *Let $H \leq G$, where G is a finite group. Then $|H|$ divides $|G|$.*

The converse is false: given $n \geq 1$ dividing $|G|$, there need not be a subgroup H with $|H| = n$.

Anyways, fix a prime p. Let G be a finite group. Define

Definition 1.3.4. A p-Sylow subgroup (sometimes called a Sylow p-subgroup) of G is a subgroup $H \leq G$ such that H is a p-group and $p \nmid [G : H]$ (that is, if $|G| = p^\alpha m$ with $p \nmid m$, then $|H| = p^\alpha$).

We fix the notation $\mathrm{Syl}_p(G)$ to denote the set of p-Sylow subgroups.

Example 1.3.5. Say $G = \mathbb{Z}/N\mathbb{Z}$, where $N = p^\alpha m$ with $p \nmid m$. It has a p-Sylow subgroup (the one generated by $[m]$). Alternatively, you can recall the Chinese Remainder Theorem, which asserts

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Example 1.3.6. Say $G = \mathrm{GL}_n(\mathbb{F}_p)$, the $n \times n$ invertible matrices with entries in $\mathbb{F}_p$. Consider the p-group

$$H = \left\{ \begin{bmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \right\} \leq G$$

and observe that

$$|H| = p^{1+2+\dots+(n-1)} = p^{n(n-1)/2}$$

We can also compute $\#GL_n(\mathbb{F}_p)$: observe that this is the number of bases of the $\mathbb{F}_p$ vector space $\mathbb{F}_p^n$, since $A \in M_n(\mathbb{F}_p)$ is invertible if and only if its columns form a basis of $\mathbb{F}_p^n$. But this is just

$$(p^n - 1)(p^n - p)(p^n - p^2)\dots(p^n - p^{n-1}) = p^{1+2+\dots+(p-1)} \underbrace{\prod_{i=1}^{n}(p^i - 1)}_{\not\equiv 0 \pmod{p}}$$

so H is actually a p-Sylow subgroup.

There are three Sylow theorems; the first shows p-Sylow subgroups exist, the second tells you how to find other ones given one, and the third gives a count on how many there are. We have the following:

Proposition 1.3.7. *Let H be a subgroup of G. Suppose that G has a p-Sylow subgroup S. Then $H \cap (gSg^{-1})$ for some $g \in G$ is a p-Sylow subgroup of H. In particular, $\mathrm{Syl}_p(G) \neq \emptyset \implies \mathrm{Syl}_p(H) \neq \emptyset$*

Proof. Define $X = G/S$. The group G, and hence the subgroup H, acts on X by left multiplication. Now take $x := gS \in X$. What is H_x? Well,

$$\begin{aligned} H_x &= H \cap G_x \\ &= H \cap \underbrace{(gSg^{-1})}_{p\text{-group}}. \end{aligned}$$

We want to show that for some $x \in X$, we have $p \nmid [H : H_x]$. So suppose not, ie. $p \div [H : H_x]$ for all $x \in X$. Then

$$|X| = \sum_{i=1}^{h} |Hx_i| = \sum_{i=1}^{h} \underbrace{[H : H_{x_i}]}_{\equiv 0 \pmod p}$$

where the x_i represent the H-orbits in X. But now p divides $|X| = |G/S| = [G : S]$, which can't happen since $S \in \mathrm{Syl}_p(G)$. □

Theorem 1.3.8 (Sylow I)**.** *Every finite group has a p-Sylow subgroup, ie.* $\mathrm{Syl}_p(G) \neq \emptyset$.

Proof. We want to embed G into a bigger group, which we know has p-Sylow subgroups (and then apply Proposition 1.3.7). Cayley's theorem says that $G \hookrightarrow S_n$ for some $n \geq 1$. Furthermore, there is an injective homomorphism

$$S_n \hookrightarrow \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_p^n) \cong \mathrm{GL}_n(\mathbb{F}_p)$$

given by $S_n \circlearrowleft \mathbb{F}_p^n$: fix a basis $e_1, \ldots, e_n$ of $\mathbb{F}_p^n$ and $\sigma(e_i) = e_{\sigma(i)}$. Now we are done, because we showed $\mathrm{GL}_n(\mathbb{F}_p)$ has a p-Sylow subgroup. □

Remark 1.3.9. This is a nonstandard proof; it's not a bad idea to look at the book for the standard one too. Prof Zywina mentioned that he got this proof from a class with Serre.

Now observe that if $S \in \mathrm{Syl}_p(G)$, then $gSg^{-1} \in \mathrm{Syl}_p(G)$ for $g \in G$, since conjugation doesn't change the cardinality of a group. The second Sylow theorem says that all p-Sylow subgroups arise in this manner:

Theorem 1.3.10 (Sylow II)**.** *The p-Sylow subgroups of G are conjugate to each other. Moreover, every p-subgroup of G is contained in a p-Sylow subgroup.*

(So the p-Sylow subgroups are those which are maximal with respect to cardinality, but Sylow II guarantees that they are those which are maximal with respect to inclusion.)

Proof. Fix $S \in \mathrm{Syl}_p(G)$ (this uses Sylow I (Theorem 1.3.8)). Take any p-subgroup $H \subseteq G$. By Proposition 1.3.7 there is a $g \in G$ such that $H \cap gSg^{-1}$ is a p-Sylow subgroup of H. But $H = H \cap gSg^{-1}$ since H is already a p-subgroup, so the unique p-Sylow subgroup is itself. Thus, $H \subseteq gSg^{-1} \in \mathrm{Syl}_p(G)$.

Also, take any $H \in \mathrm{Syl}_p(G)$. Then $H \subseteq gSg^{-1}$ for some $g \in G$. But they have the same cardinality for some $g \in G$, so $H = gSg^{-1}$. □

Define $n_p(G)$ to be the number of p-Sylow subgroups.

Theorem 1.3.11 (Sylow III)**.** *We have $n_p(G) \equiv 1 \pmod p$ and $n_p(G)$ divides m, where $|G| = p^\alpha m$ with $p \nmid m$.*

We'll prove this next lecture. For now, here's an example of the power of this theorem:

Example 1.3.12. There is no simple group of order $200 = 2^3 \cdot 5^2$. Here's a proof:

Sylow III (Theorem 1.3.11) says that $n_5(G) \equiv 1 \pmod 5$ and $n_5(G)$ divides 8. Then $n_5(G) = 1$ and $|S| = 25$. So when you conjugate S with any element, you still have S, that is, $gSg^{-1} = S$ for all $g \in G$, so S is a nontrivial normal subgroup of G. Thus, G is not simple.

1.4 Aug 31, 2018

Last time:

Let G be a finite group and p be a prime. Denote by $\mathrm{Syl}_p(G)$ to be the set of p-Sylow subgroups of G, that is, a p-group $H \leq G$ such that $p \nmid [G : H]$. We had three big theorems:

Theorem 1.4.1 (Sylow I)**.** *We have* $\mathrm{Syl}_p(G) \neq \emptyset$.

Theorem 1.4.2 (Sylow II)**.** *The action of G on $\mathrm{Syl}_p(G)$ by conjugation is transitive.*

Theorem 1.4.3 (Sylow III, to be proven)**.** *Let $n_p(G)$ be the number of p-Sylow subgroups. Then $n_p(G) \equiv 1 \pmod p$ and $n_p(G)|m$, where $n = p^\alpha m$ and $p \nmid m$.*

As an application of the theorems, we have:

Example 1.4.4. Let G be a group of order pq with p, q primes so that $p < q$ and $q \not\equiv 1 \pmod p$. Then G is cyclic.

Proof. Recall (from Example 1.3.12) that if $S \in \mathrm{Syl}_p(G)$, we have $n_p(G) = 1 \iff S \trianglelefteq G$. Let

$$n_p := n_p(G) \equiv 1 \pmod p$$

and note that $n_p|q$. Since q is prime we have $n_p = 1$ or $n_p = q$. But $q \not\equiv 1 \pmod p$ so $n_p = 1$. Let P be the unique p-Sylow subgroup of G, so $P \trianglelefteq G$.

Choose $Q \in \mathrm{Syl}_q(G)$. Notice that Q acts on P by conjugation, that is, there's a map

$$\varphi\colon Q \to \mathrm{Aut}(P) \cong (\mathbb{Z}/p\mathbb{Z})^\times$$

If $\ker\varphi = 1$, then $|\varphi(Q)| = q|p-1$, which contradicts $p < q$. So $\varphi = 1$, ie. P and Q commute. This implies that G is abelian of order pq. It follows that G is cyclic. □

Let's now prove Sylow III.

Proof of Theorem 1.3.11. Recall that G acts transitively on $\mathrm{Syl}_p(G)$ via conjugation. Fix $S \in \mathrm{Syl}_p(G)$. Then

$$n_p(G) = \#\mathrm{Syl}_p(G) = [G : G_S],$$

where $G_S = \{g \in G \colon gSg^{-1} = S\} =: N_G(S)$ is the normalizer of S in G. In other words, $n_p(G) = [G : N_G(S)]$. Note that $S \subseteq N_G(S)$. This implies that

$$n_p(G) \text{ divides } [G : N_G(S)][N_G(S) : S] = [G : S] = m.$$

Also, observe that S acts on $\mathrm{Syl}_p(G)$ by conjugation. But $n_p(G) = \#\mathrm{Syl}_p(G) \equiv \#\mathrm{Syl}_p(G)^S \pmod p$, by Proposition 1.2.9 (recall that $\mathrm{Syl}_p(G)^S = \{S' \in \mathrm{Syl}_p(G) \colon gS'g^{-1} = S', \forall g \in S\}$).

Fix an $S' \in \mathrm{Syl}_p(G)$ such that $gS'g^{-1} = S'$ for all $g \in S$. This is the same as saying $S \subseteq N_G(S')$. Also note that $S' \trianglelefteq N_G(S')$ (so that $n_p(N_G(S')) = 1$). So $S, S' \in \mathrm{Syl}_p(N_G(S'))$, that is, $S = S'$. It follows that the unique element in $\mathrm{Syl}_p(G)^S$ is S itself (we fixed S' and showed it was S). In other words,

$$n_p(G) \equiv \mathrm{Syl}_p(G)^S = 1 \pmod p.$$

□

Now we can do something a little more serious.

Example 1.4.5. We will show that A_5 is the only simple group of order 60.

Define $X = \mathrm{Syl}_5(G)$, where G is simple of order 60. Then G acts by conjugation on X; it is transitive by Sylow II (Theorem 1.3.10). This gives a map $\varphi\colon G \to S_X$. Let's compute $|X| = n_5(G)$. By Sylow III (Theorem 1.3.11), we have $n_5(G) \equiv 1 \pmod 5$ and $n_5(G)$ divides 12. So $n_5(G) = 1$ or $n_5(G) = 6$, but G is simple so $n_5(G) = 6$ (since $n_5(G) = 1$ would imply that G has a normal subgroup of order 5).

Since G is simple, $\ker\varphi = 1$ or G. But the action is transitive, so $\ker\varphi \neq G$. So $\ker\varphi = 1$, and $G \subseteq S_6$. In fact, $G \subseteq A_6$, since $G \subseteq S_6 \twoheadrightarrow \{\pm 1\}$ is given by the sign map, and if G contains an element not in A_6, the kernel of the sign map restricted to G would yield an index 2 normal subgroup.

Now recall that G acts on A_6/G by left multiplication (observe that $|A_6/G| = 6$). Note that G fixes $1 \cdot G$. So G acts on $Y := (A_6/G)\backslash\{1 \cdot G\}$, where $|Y| = 5$. Now we have

$$\psi\colon G \to S_Y$$

and G simple implies that the kernel is trivial or G. We claim that the kernel is trivial:

Suppose not; let $\ker(\psi) = G$. So $g \cdot aG = aG$ for all $a \in A_6, g \in G$. So $a^{-1}ga \in G$ for all $a \in A_6$. This means that $G \trianglelefteq A_6$. But A_6 is simple! So

$$\psi\colon G \hookrightarrow S_Y$$

So $G \subseteq S_5$. As before, $G \subseteq A_5$, that is, $G \cong A_5$.

Remark 1.4.6. We don't actually need that A_6 is simple; we just need that A_6 has no order 6 subgroups (we won't prove this so we can end lecture on time). Later in the course we'll meet the alternating groups again, anyways.

1.5 Sep 5, 2018

[A reminder that homeworks are due on Friday]

Recall that G acts on itself by conjugation, which gives a homomorphism $\varphi\colon G \to \mathrm{Aut}(G) \subseteq S_G$. The image is denoted $\mathrm{Inn}(G)$, called the "inner automorphisms". One can check $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$:

Proof. Let $f \in \mathrm{Aut}(G)$, and $g \in G$. We want to show that $f \circ \varphi(g) \circ f^{-1}$ is an inner automorphism: indeed,

$$\begin{aligned}(f \circ \varphi(g) \circ f^{-1})(x) &= (f \circ \varphi(g))(f^{-1}(x)) \\ &= f(gf^{-1}(x)g^{-1}) \\ &= f(g)xf(g)^{-1} \\ &= \varphi(f(g)).\end{aligned}$$

□

Thus we can define $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

Observe that $G/Z(G) \hookrightarrow \mathrm{Aut}(G)$, where $Z(G) = \ker(\varphi) = \{x\colon xg = gx \, \forall g \in G\}$ is the center of G. We have $Z(G) \trianglelefteq G$. In fact, $Z(G)$ is a characteristic subgroup of G:

Definition 1.5.1. Let $H \leq G$. We say H is characteristic if $f(H) \subseteq H$ for all $f \in \mathrm{Aut}(G)$.

Of course, $H \leq G$ is normal if $f(H) \subseteq H$ for all $f \in \mathrm{Inn}(G)$. Examples of characteristic subgroups include $H = 1, H = G$, and any $H \leq \mathbb{Z}/m\mathbb{Z}$. Maybe a more nontrivial characteristic subgroup is the commutator subgroup of G, that is

$$[G, G] := \langle \{\underbrace{g^{-1}h^{-1}gh}_{:=[g,h]}\colon g, h \in G\} \rangle$$

Lemma 1.5.2. *Let $N \trianglelefteq G$. Then G/N is abelian if and only if $N \supseteq [G, G]$. In particular, $G/[G, G]$ is the largest abelian quotient of G.*

Proof. The quotient G/N is abelian if and only if

$$gNhN = hNgN \iff g^{-1}h^{-1}gh \in N \iff [G, G] \subseteq N. \quad \square$$

Proposition 1.5.3. *Let $G \neq 1$ be a p-group. Then $Z(G) \neq 1$.*

Proof. We have an action $G \circlearrowright X = G$ by conjugation. So $|X| \equiv |X^G| \pmod{p}$ (this is Proposition 1.2.9). In particular,

$$0 \equiv |G| \equiv |Z(G)| \pmod{p}$$

so p divides $|Z(G)|$. □

Recall that a group G is simple if $G \neq 1$ and its only normal subgroups are 1 and G.

For example, $\mathbb{Z}/p\mathbb{Z}$ is simple for p prime (Proposition 1.5.3 says that these are the only finite simple p-groups). Also, A_n is simple for $n \geq 5$, and so is

$$\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/Z(\mathrm{SL}_n(K)) = \mathrm{SL}_n(K)/\{aI\colon a \in K^\times, a^n = 1\}$$

for $n \geq 2$, and K a field with $|K| > 3$ if $n = 2$ (and of course, $\mathrm{SL}_n(K)$ denotes $n \times n$ matrices with entries in K and det $= 1$). Also, there are the sporadic groups (Monster, Baby Monster, ...).

Here's some archaic terminology, (Prof Zywina prefers "filtrations", or something):

Definition 1.5.4. A series of a group G is a sequence of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$$

with G_{i+1} normal in G_i. The integer n is called the length of the series. Since the G_i are normal, we can consider the quotients $G_0/G_1, \ldots, G_{n-1}/G_n$. Such a series is a composition series of G if all these quotients are simple.

Series always exist (take $G_0 = G, G_1 = 1...$), but it's not clear that composition series always exist. In fact, for infinite groups, this is not always true. But:

Lemma 1.5.5. *Every finite group G has a composition series.*

Proof. We induct on $|G|$. If $|G| = 1$, then $G = 1$. Then it is true with $n = 0$.

Take G with $|G| > 1$ and assume the lemma is true for smaller groups. If G is simple then then we are done. So assume G is not simple. Then there is a normal subgroup $N \trianglelefteq G$, and can assume there is no larger normal subgroup. By our choice of N, we have G/N is simple (otherwise, there would be a larger normal subgroup of G). But $|N| < |G|$, so N has a composition series $N = N_0 \supset N_1 \cdots \supset N_r = 1$. Then $G \supset N \supset N_1 \supset \cdots \supset N_r = 1$ is a composition series of G. □

The integers $\mathbb{Z}$ do not have a composition series, so this lemma is false for infinite groups. This is because nontrivial subgroups of $\mathbb{Z}$ are isomorphic to $\mathbb{Z}$ itself, and $\mathbb{Z}$ is not simple, so you could never end a chain.

Theorem 1.5.6 (Jordan-Hölder)**.** *Let $G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$ be a composition series of a group G. Then the simple quotients $G_0/G_1, G_1/G_2, \ldots, G_{n-1}/G_n$ are unique up to isomorphism and reordering (i.e., regardless of the choice of composition series), counted with multiplicities. The length does not depend on the composition series either.*

This is really powerful. As an example, consider $G = \mathbb{Z}/6\mathbb{Z}$ and observe that

$$\mathbb{Z}/6\mathbb{Z} = G_0 \supset G_1 = \langle 2 \rangle \supset G_2 = 1$$

induces $G_0/G_1 \cong \mathbb{Z}/2\mathbb{Z}$ and $G_1/G_2 \cong \mathbb{Z}/3\mathbb{Z}$, whereas

$$\mathbb{Z}/6\mathbb{Z} = G_0 \supset G_1 = \langle 3 \rangle \supset G_2 = 1$$

induces $G_0/G_1 \cong \mathbb{Z}/3\mathbb{Z}$ and $G_1/G_2 \cong \mathbb{Z}/2\mathbb{Z}$.

Example 1.5.7. Consider $G = S_5$. Notice that $S_n \supset A_n \supset 1$ (recall that A_n is simple so this is a composition series). But there is no $N \trianglelefteq S_n$ such that $S_n/N \cong A_n$ and $N \cong \mathbb{Z}/2\mathbb{Z}$. This is because A_n acts by conjugation on $N \cong \mathbb{Z}/2\mathbb{Z}$ so A_n commutes with N, which implies $Z(A_n) \neq 1$ (which is false, apparently!).

Example 1.5.8. Let $|G| = 1024$. The quotients that appear in the composition series are just $\mathbb{Z}/2\mathbb{Z}$, since all quotients that would appear are 2-groups, so if they were simple they would have to be $\mathbb{Z}/2\mathbb{Z}$.

1.6 Sep 7, 2018

[The new homework is up.]

Last time, we stated a very miraculous theorem. Recall:

A composition series for a group G is a series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$$

where G_{i+1} is normal in G_i, and G_i/G_{i+1} are simple. In general, groups don't have composition series, but finite groups do. There may be multiple composition series; last class we saw the following (miraculous) theorem:

Theorem 1.6.1 (Jordan-Hölder)**.** *Take any composition series as above. Then the simple groups*

$$G_0/G_1, \ldots, G_{n-1}/G_n$$

depend only on G up to isomorphism and reordering.

As a remark, this theorem also holds for infinite groups which have a composition series. We defined the length of G, denoted by $\ell(G) := n$, and define $\ell(G) = \infty$ if G does not have a composition series.

Example 1.6.2. Fix an integer $m \geq 2$. Consider $G = \mathbb{Z}/m\mathbb{Z}$. Factor $m = p_1 \ldots p_r$ into primes. We have the composition series

$$\mathbb{Z}/m\mathbb{Z} \supset p_1\mathbb{Z}/m\mathbb{Z} \supset p_1p_2\mathbb{Z}/m\mathbb{Z} \supset \cdots \supset \underbrace{p_1 \ldots p_r}_{=m}\mathbb{Z}/m\mathbb{Z} = 0$$

which gives quotients $\mathbb{Z}/p_1\mathbb{Z}, \mathbb{Z}/p_2\mathbb{Z}, \ldots, \mathbb{Z}/p_r\mathbb{Z}$ with cardinalities $p_1, \ldots, p_r$. Jordan-Hölder says that these primes are unique up to reordering; the uniqueness amounts to the Fundamental Theorem of Arithmetic.

Let's prove Jordan-Ḧ(Theorem 1.5.6)

Proof. Take any simple group S. Define the number $e(G, G_\bullet, S)$ to be the number of factors G_i/G_{i+1} with $0 \leq i < n$ that are isomorphic to S. We need to show that $e(G, G_\bullet, S)$ does not depend on $G_\bullet$. We prove this by induction on n.

The $n = 0$ case is easy: we have $G = G_0 = 1$ and hence $e(G, G_\bullet, S) = 0$. So assume $n \geq 1$, and that the theorem is known for composition series of length strictly less than n. If G is simple, then $G = G_0 \supset G_1 = 1$ and $e(G, G_\bullet, S) = 1$ if $S \cong G$ and 0 otherwise. If G is not simple, then it has a normal subgroup N. For $0 \leq i < n$, define $N_i := N \cap G_i$ and observe that we have the chain of inclusions

$$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n = 1$$

which is not necessarily a composition series. Similarly, for $0 \leq i < n$, define $(G/N)_i := G_iN/N$, and similarly observe that we have the chain of inclusions

$$G/N = (G/N)_0 \supseteq (G/N)_1 \supseteq \cdots \supseteq (G/N)_n = 1.$$

This gives short exact sequences

$$\begin{tikzcd} 1 \arrow[r] & N_i \arrow[r, hook] & G_i \arrow[r, two heads] & G_iN/N \arrow[r] & 1, \end{tikzcd}$$

which in turn give short exact sequences ("this is a good exercise to check if you know your isomorphism theorems well")

$$\begin{tikzcd} 1 \arrow[r] & N_i/N_{i+1} \arrow[r, hook] & G_i/G_{i+1} \arrow[r, two heads] & (G/N)_i/(G/N)_{i+1} \arrow[r] & 1. \end{tikzcd}$$

Since G_i/G_{i+1} is simple, exactly one of N_i/N_{i+1}, and $(G/N)_i/(G/N)_{i+1}$ is simple and isomorphic to G_i/G_{i+1}, and the other is 1. So we have

$$e(G, G_\bullet, S) = e(N, N_\bullet, S) + e(G/N, (G/N)_\bullet, S),$$

where we abuse notation a little because $N_\bullet$ and $(G/N)_\bullet$ are not composition series, but they still mean what they should mean (number of quotients which are isomorphic to S). We want to show that both these numbers are strictly less than $e(G, G_\bullet, S)$, so that we can apply the induction hypothesis.

The quotient N_i/N_{i+1} is simple or equal to 1 for all $0 \leq i < n$. In fact, $N_i/N_{i+1} = 1$ for some $0 \leq i < n$ (otherwise, we have $(G/N)_i = (G/N)_{i+1}$ and we get $G/N = (G/N)_0 = \cdots = (G/N)_n = 1$, which implies $G = N$). So we can obtain a composition series of length strictly less than n by removing some N_i. The inductive hypothesis implies $e(N, N_\bullet, S)$ depends only on N and S. Similarly, $(G/N)_i = (G/N)_{i+1}$ for some i (otherwise, $N_i = N_{i+1}$ for all $0 \leq i < n$, so $N = N_0 = \cdots = N_n = 1$ implies $N = 1$), so $e(G/N, (G/N)_\bullet, S)$ depends only on G/N and S. So since

$$e(G, G_\bullet, S) = e(N, N_\bullet, S) + e(G/N, (G/N)_\bullet, S),$$

we conclude that $e(G, G_\bullet, S)$ depends on $N, G/N$, and S (and not $G_\bullet$). □

Remark 1.6.3. In the proof, we actually showed that for $N \trianglelefteq G$, we have $\ell(G) = \ell(N) + \ell(G/N)$. This is true when G doesn't even have a composition series (so if G doesn't have a composition series, then either N or G/N doesn't have one!)

Remark 1.6.4. There is a Hölder program for classifying finite groups. It has two ridiculously hard steps. The idea is:

1. Classify finite simple groups
2. Find all ways to "put simple groups together".

Composition series are related to the second part, i.e. the study of how can we put simple groups together.

Part 1 was solved* in the '80s. Maybe not everything was published and some people are still reproving things. There are:

- Infinite families: $\mathbb{Z}/p\mathbb{Z}, A_n$, for $n \geq 5$
- 16 families of Lie types (such as $\mathrm{PSL}_n(\mathbb{F}_q) = \mathrm{SL}_n(\mathbb{F}_q)/Z(\mathrm{SL}_n(\mathbb{F}_q))$, for $n \geq 2$ and $q > 3$ if $n = 2$).
- 26 sporadic groups (Monster, Baby Monster, Thompson, Janko,...)

There's some overlap in these families. For example $\mathrm{PSL}_2(\mathbb{F}_4)$ and $\mathrm{PSL}_2(\mathbb{F}_5)$ are simple of order 60, so they're both isomorphic to A_5.

1.7 Sep 10, 2018

Today, we're going to show A_n is simple for $n \geq 5$. We're going to prove this by induction; the base case was the homework. There are a lot of proofs of this; this will be one that is hopefully not "magical" (that is, we won't have to appeal to any random facts about cycles)

Definition 1.7.1. Fix $n \geq 1$. A group G acts $\underline{n\text{-transitively}}$ on a set X if $|X| \geq n$ and G acts transitively on $\{(x_1, \dots, x_n) \colon x_i \in X \text{ distinct}\}$, where $g \cdot (x_1, \dots, x_n) = (gx_1, \dots, gx_n)$.

For example, S_n acts n-transitively on $[n] = \{1, 2, \dots, n\}$. A slightly less trivial example is the following:

Example 1.7.2. The gorup A_n acts $(n-2)$-transitively on $[n]$. Indeed, pick distinct $a_1, \dots, a_{n-2} \in [n]$ and distinct $b_1, \dots, b_{n-2} \in [n]$. There are two $\sigma \in S_n$ such that $\sigma(a_i) = b_i$ for $1 \leq i \leq n-2$; they differ by a transposition. So one of the σ is in A_n.

Note that if σ is n-transitive, then it's k-transitive for $1 \leq k \leq n$.

Lemma 1.7.3. *Let G be a group acting 2-transitively on X. Then G_x (the stabilizer of $x \in X$) is a maximal subgroup of G for any x.*

This will be a nice way of generating large subgroups.

Proof. If not, then $G_x < M < G$ for some M. Recall that there is a natural bijection $G/G_x \to X$.

$$G/G_x = \bigsqcup_{C \in G/M} \{\kappa \colon \kappa \in G/G_x, \kappa \subseteq C\}$$

so that

$$X = \bigsqcup_{C \in G/M} X_C$$

where $[G : M] > 1$, and $|X_C| = [M : G_x] > 1$. Furthermore, G permutes the X_C amongst themselves. Here X_C denotes the image of $\{\kappa \colon \kappa \in G/G_x, \kappa \subseteq C\}$ under the bijection $G/G_x \to X$.

This will contradict 2-transitivity on $G \circlearrowleft X$: take distinct x_1, x_2 in the same X_C and distinct y_1, y_2 *not* in the same set X_C. There is no g such that $gx_1 = y_1$ and $gx_2 = y_2$. Otherwise, G does not permute $\{X_C\}$. □

We now prove A_n is simple. "It's not an easy proof".

Theorem 1.7.4. *The group A_n is simple for $n \geq 5$.*

Proof. Let $n \geq 6$ and assume that A_{n-1} is simple. By abuse of notation, we identify A_{n-1} with a subgroup of A_n in the following way: for a $\sigma \in A_{n-1}$, define $\tau \in A_n$ by $\tau(i) = \sigma(i)$ for $i \leq n-1$, and $\tau(n) = n$. In his notation, $A_{n-1} = (A_n)_n = \{\sigma \in A_n \colon \sigma(n) = n\}$, that is, it's the stabilizer of $n \in [n]$ under the action $A_n \circlearrowleft [n]$. Note that A_n acts 2-transitively on $[n]$, so $A_{n-1} \subseteq A_n$ is a maximal subgroup, by Lemma 1.7.3.

Suppose $N \neq 1$ is a normal subgroup of A_n. We need to show that $N = A_n$. Consider $N \cap A_{n-1} \trianglelefteq A_{n-1}$. Since A_{n-1} is simple we have $N \cap A_{n-1} = 1$ or A_{n-1}. We have two cases:

Case 1. We have $N \cap A_{n-1} = A_{n-1}$. Since A_{n-1} is maximal either $N = A_n$ (and we're done) or $N = A_{n-1}$. But A_{n-1} is not normal in A_n: conjugate any element by the transposition $(1, n)$ and we no longer fix n, so we're not in A_{n-1}.

Case 2. We have $N \cap A_{n-1} = 1$. So the only element of N that fixes n is the identity. Thus, observe $N \cdot A_{n-1} \supset A_{n-1}$, since $N \neq 1$ and $N \cap A_{n-1} = 1$; since A_{n-1} is maximal we have $N \cdot A_{n-1} = A_n$. We conclude $|N| = n$, e.g. because there is a surjective map $A_{n-1} \twoheadrightarrow A_{n-1} \cdot N/N = A_n/N$, whose kernel is $N \cap A_n = 1$. Consider the map $\varphi \colon N \to [n]$ which sends $g \mapsto g \cdot n$. We claim that φ is bijective: There is $\sigma \in A_n$ so that $\sigma(n) = i$, and since $A_n = N \cdot A_{n-1}$ we can decompose $\sigma = gh$ for $g \in N, h \in A_{n-1}$, so

$i = \sigma(n) = g(h(n)) = g(n)$ so that φ is surjective.

We claim that φ is A_{n-1}-equivariant, where $A_{n-1} \circlearrowright N$ by conjugation and $A_{n-1} \circlearrowright [n]$ as usual (i.e., "these actions are compatible"). That is, we should show that for any $g \in N, h \in A_{n-1}$, we have $\varphi(hgh^{-1}) = h\cdot\varphi(g)$. But

$$\varphi(hgh^{-1}) = hgh^{-1} \cdot n = hg \cdot n,$$

since $h^{-1} \in A_{n-1}$. Notice also that $h \cdot \varphi(g) = h(g \cdot n)$, so that $\varphi(hgh^{-1}) = h \cdot \varphi(g)$.

By factoring through φ, we get an action $A_{n-1} \circlearrowright N - \{1\}$ by conjugation that is 3-transitive (using the fact that $A_{n-1} \circlearrowright [n-1]$ is $(n-3)$-transitive). So $\operatorname{Aut}(N)$ acts 3-transitively on $N - \{1\}$ and $|N| = n \geq 6$. This will prove to be too good to be true:

Lemma 1.7.5. *There is no finite group G with $|G| \geq 5$ such that* $\operatorname{Aut}(G)$ *acts 3-transitively on $G - \{1\}$.*

Proof. Suppose G exists. Then all $g \in G - \{1\}$ have the same order, since $\operatorname{Aut}(G)$ preserves order. The order must be a prime p, by Proposition 1.2.11.

As always, suppose first that $p > 2$. Since $|G| \geq 5$, there is $x \in G - \{1\}$, and $y \in G - \{1, x, x^{-1}\}$. We have two pairs (x, x^{-1}) and (x, y). There is no $f \in \operatorname{Aut}(G)$ such that $f(x) = x$ and $f(x^{-1}) = y$, since $1 = f(xx^{-1}) = xy$ but $y \neq x^{-1}$. So $G \circlearrowright X$ is not 2-transitive. On the other hand, if $p = 2$, then G is abelian (for $a, b \in G$, we have $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$). So $G = \mathbb{F}_2^r$ with $r \geq 3$. Then $\operatorname{Aut}(G) = \mathrm{GL}_r(\mathbb{F}_2)$. One can check that $\mathrm{GL}_r(\mathbb{F}_2) \circlearrowright \mathbb{F}_2^r - \{0\}$ is not 3-transitive. □

This proves that A_n is simple for $n \geq 5$. □

1.8 Sep 12, 2018

Let K be a field, and $n \geq 2$. Recall that

$$\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/Z(\mathrm{SL}_n(K)) = \mathrm{SL}_n(K)/\{aI \colon a^n = 1\}.$$

We're going to prove today that $\mathrm{PSL}_n(K)$ is simple for all $n \geq 2$ and fields K, where $|K| > 2$ if $n = 2$. The techniques we use for this group will apply to the groups of Lie type, so except for the sporadic groups we'll have everything. Note that $\mathrm{PSL}_2(\mathbb{F}_2) \cong S_3$ and $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$.

Here's a theorem, due to Iwasawa:

Theorem 1.8.1. *Let G be a group acting 2-transitively on a set X. Suppose that:*

a) G is "perfect", that is, G has no nontrivial abelian quotients (equivalently, we have $G = [G, G]$).

b) for some $x \in X$, the stabilizer G_x has a normal subgroup A that is abelian and $\cup_{g \in G} gAg^{-1}$ generate G.

Then G/H is simple, where H is the kernel of the action of $G \circlearrowleft X$

(Recall that $G \circlearrowleft X$ gives $\varphi \colon G \to S_X$; the kernel of the action is H.)

The conditions seem very restrictive, but it apparently applies to most of the groups of Lie type. In our case, G is SL_n; this is easier to work with.

Proof. Take a normal subgroup N of G, with $N \supsetneq H$. We need to show that $N = G$, since G/H is simple if and only if G has no normal subgroup containing H except H and G.

Take $x \in X$. Define $M := G_x$; it is a maximal subgroup of G (this was proven in Lemma 1.7.3; we used $G \circlearrowleft X$ is 2-transitive). So $M = G_x \supseteq H$, because elements of H fix all elements (it's the kernel of the action), whereas elements of G_x fix only x. Since M is maximal, $N \cdot M$ is equal to M or G.

Suppose that $N \cdot M = M$, i.e. that $N \subseteq M$. Take $g \in G$ and $n \in N$; since $N \trianglelefteq G$ we have $g^{-1}ng \in N \subseteq M$. So $n \cdot gM = gM$, that is, n fixes $G/M = G/G_x = X$, so $n \in H$. But this says $N \subseteq H$, even though we assumed $N \supsetneq H$.

So $G = N \cdot M$. Define $\tilde{G} := G/N$. Let $\tilde{A}$ be the image of A in $\tilde{G}$. The homomorphism

$$M \hookrightarrow G \twoheadrightarrow \hat{G}$$

is surjective because $G = N \cdot M$. Observe that we're trying to show that $\hat{G}$ is trivial; we showed that it's a quotient of M. Note that $\tilde{A} \trianglelefteq \tilde{G}$, since $A \trianglelefteq M$ and $M \twoheadrightarrow \tilde{G}$. Because $\cup_{g \in G} gAg^{-1}$ generates G, we conclude that $\cup_{g \in \tilde{G}} g\tilde{A}g^{-1}$ generate $\tilde{G}$.

So $\tilde{A} = \tilde{G}$, because $\cup_{g \in \tilde{G}} g\tilde{A}g^{-1} \subseteq \tilde{A}$ (we have $\tilde{A}$ is normal), and $G = \langle \cup_{g \in \tilde{G}} g\tilde{A}g^{-1} \rangle \subseteq \tilde{A}$. This means that $\tilde{G}$ is abelian. But G is perfect, so if $\tilde{G} = G/N$ is abelian we must have $G/N = 1$, that is, $N = G$. □

Example 1.8.2. Let $G = \mathrm{SL}_n(K)$, where K is a field, $n \geq 2$, and $|K| > 3$ when $n = 2$. Observe that G acts on $X = \{$1-dimensional subspaces of $K^n\}$; we chose this action so that the kernel is $H = \{aI \colon a^n = I\} = Z(\mathrm{SL}_n(K))$. Sometimes X is denoted $\mathbb{P}^{n-1}(K)$, called projective space. Indeed, $G/H = \mathrm{PSL}_n(K)$. We want to apply Theorem 1.8.1.

We should verify that $G \circlearrowleft X$ is 2-transitive. The idea is the following: given a basis $v_1, \ldots, v_n$ of K^n and $w_1, \ldots, w_n$ of K^n, there is a $B \in \mathrm{SL}_n(K)$ such that $Bv_1 = w_1, \ldots, Bv_n = cw_n$, where $c \in K^\times$.

We should also verify that condition b) holds. Indeed, take $x := K \cdot e_1 \in X$, so that $x = (*, 0, \ldots, 0)$. Now

$$G_x = \left\{ \begin{bmatrix} a & * & \cdots & * \\ 0 & b_{11} & \cdots & b_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{(n-1)1} & \cdots & b_{(n-1)(n-1)} \end{bmatrix} : a \in K^\times, b \in \mathrm{GL}_{n-1}(K), a \det B = 1 \right\}$$

has a normal subgroup

$$A = \left\{ \begin{bmatrix} a & * & \dots & * \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \cong K^{n-1} \right\}$$

which is abelian. Now for $1 \leq i, j \leq n$ distinct, let $E_{i,j} \in M_n(K)$ with 1 at the (i, j)th coordinate and 0 elsewhere. Then note that $I + cE_{i,j} \in SL_n(K)$ for any $c \in K$, and it is conjugate in $\mathrm{SL}_n(K)$ to an element in A.

Observe that $\mathrm{SL}_n(K)$ is generated by such $I + cE_{i,j}$, for $1 \leq i, j \leq n$ distinct, and $c \in K$. The idea is the following: Multiplying by $I + cE_{i,j}$ is doing an elementary row operation, that is, adding c times row j and leaving other rows the same. Any $B \in \mathrm{SL}_n(K)$ can be put in the form I using these operations.

We should also verify that condition a) holds. Indeed, it suffices to show that $I + cE_{i,j}$ are commutators: since they generate $\mathrm{SL}_n(K)$, this will imply that $G = [G, G]$. The idea is as follows. If $n \geq 3$, then

$$\begin{bmatrix} 1 & c & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \left[\begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \right]$$

and if $n = 2$ then

$$\begin{bmatrix} 1 & -b(a^2-1) \\ 0 & 1 \end{bmatrix} = \left[\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \right]$$

where we note that $-b(a^2 - 1)$ can be anything in K if $a \notin \{0, 1, -1\}$, which holds since $|K| > 3$.

1.9 Sep 14, 2018

We'll begin by talking about a concept that's falling out of fashion; they're not really in the newer books. We'll talk about groups with operators. The idea is to generalize group theory in the following way. Begin by fixing a set Ω.

Definition 1.9.1. An Ω-group (or a group with operator set Ω) is a group $(G, \cdot)$ such that for all $x \in \Omega$ and $g \in G$, we have a $g^x \in G$ satisfying $(gh)^x = g^x h^x$ for all $g, h \in G$.

So if $\Omega = \emptyset$, then we just have a usual group, and we could redo group theory!

Definition 1.9.2. An Ω-subgroup H of G is a subgroup stable under the Ω-action.

For a normal Ω-subgroup $N \trianglelefteq G$, we have that G/N is an Ω-group, given by $(gN)^x = g^x N$.

Definition 1.9.3. $G \neq 1$ is a simple Ω-group if it has no normal Ω-subgroups.

And you say "hey, most of this still works". For eample, the Jordan-Hölder theorem works with Ω-groups. Let's look at an example that's not $\Omega \neq \emptyset$.

Example 1.9.4. Let R be a commutative ring. Then an R-module M is an "R-group": for $a \in R, m \in M$, define $m^a := am$. An R-subgroup is just a submodule, and so on. We say an R-module $M \neq 0$ is simple if the only submodules are 0 and itself. With this, we get a Jordan-Hölder theorem. In particular:

A composition series for an R-module M is a chain of submodules

$$M = M_0 \subset M_1 \subset \cdots \subset M_n = 0$$

such that M_i/M_{i+1} are simple for all $0 \leq i < n$. So Jordan-Hölder says that up to reordering and isomorphism, the simple R-modules

$$M_0/M_i, \ldots, M_{n-1}/M_n$$

are independent of composition series. The length of M is defined to be $\ell(M) := n$.

This is somewhat important in algebraic geometry, when one tries to figure out intersection properties; it's sometimes a good generalization of dimension (when $R = K$ is a field then it is exactly the dimension of the vector space).

Okay, let's move on.

Solvable Groups

Let G be a group, and recall $[G, G]$, called the commutator subgroup of G, denotes the subgroup of G generated by commutators $[g, h] = g^{-1}h^{-1}gh$. We showed that $[G, G]$ is characteristic subgroup of G. We also saw that $G/[G, G]$ is the (unique) largest abelian quotient of G, which shouldn't be too surprising.

Let $G^{(0)} = G$, and $G^{(1)} = [G, G] = [G^{(0)}, G^{(0)}]$. Inductively, define $G^{(i+1)} = [G^{(i)}, G^{(i)}]$, so that

$$G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \ldots.$$

We say that G is solvable if $G^{(n)} = 1$ for some $n \geq 0$. The British call these soluble groups. The smallest such $n \geq 0$ is called the derived length.

For example, when G is abelian, then $[G, G] = G^{(1)} = 1$, and in fact, G is abelian if and only if its derived length is 1.

Example 1.9.5. Let

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in \mathbb{R}^\times, b \in \mathbb{R} \right\}$$

and observe that

$$[G,G] = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{R} \right\} \cong \mathbb{R}$$

so that $G/[G,G] \xrightarrow{\sim} \mathbb{R}^\times$, given by

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mapsto a.$$

Observe that $[G,G]$ is abelian and so is $G/[G,G]$, but G itself is not abelian. This will come up again later. The group G is solvable, with derived length 2.

Some nonexamples include $A_5 = [A_5, A_5]$, and more generally perfect groups, and also S_5. Sometimes infinite groups G are also not solvable even though $G^{(i+1)} \subset G^{(i)}$ for all i. We have the following lemma:

Lemma 1.9.6. *The group G is solvable if and only if $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ is a series with G_i/G_{i+1} abelian.*

Proof. The forwards direction is easy: define $G_i := G^{(i)}$; recall that

$$G_0 \supseteq G_1 \supseteq \cdots \supseteq \underbrace{G_n}_{=G^{(n)}} = 1$$

for n large enough; we have $G^{(i)}/G^{(i+1)} = G^{(i)}/[G^{(i)}, G^{(i)}]$ is abelian, as desired.

For the backwards direction, we claim that $G^{(i)} \subseteq G_i$; roughly, at each step G_i removes something so that the quotient is abelian, whereas $G^{(i)}$ removes the largest thing possible so that the quotient is abelian. We will prove this claim by induction. For $i = 0$, of course we have $G^{(0)} = G = G_0$, we are done. Suppose that $G^{(i)} \subseteq G_i$ for $i \geq 0$. Then

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1}.$$

□

Lemma 1.9.7. *Suppose G is solvable.*

1. *Any subgroup of G is solvable.*
2. *Any quotient of G is solvable.*

Proof. For part i), we take $H \leq G$. Note that $H^{(i)} \subseteq G^{(i)}$ for all i, so eventually $H^{(i)}$ is trivial. This also implies that the derived length of H is at most the derived length of G.

For part ii), we take $N \trianglelefteq G$. Note that

$$(G/N)^{(i)} = G^{(i)}N/N$$

for $i \geq 0$. Then $G^{(n)} = 1$ implies $(G/N)^{(n)} = 1$, so G/N is solvable. □

Proposition 1.9.8. *Fix a group G. Let N be a normal subgroup. Then G is solvable if and only if N and G/N are solvable.*

Remark 1.9.9. Recall Example 1.9.5, which says that Proposition 1.9.8 is not true if we replace "solvable" with "abelian"; this makes proving things about solvable groups with induction much easier. Solvable groups are the smallest class of groups with this property.

Proof. The forward direction is just Lemma 1.9.7. For the backwards direction recall that $(G/N)^{(i)} = G^{(i)}N/N$. So for n large enough, $(G/N)^{(n)} = 1$, so $G^{(n)} \subseteq N$, and for m large enough, $N^{(m)} = 1$. Then $G^{(m+n)} = (G^{(n)})^{(m)} \subseteq N^{(m)} = 1$, that is, G is solvable. □

1.10 Sep 17, 2018

Last time, we defined solvable groups:

The group G is solvable if and only if there exists a series

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 0$$

such that $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is abelian.

It suffices to consider $G^{(i)}$, where $G^{(0)} := G$ and $G^{(k+1)} := [G^{(k)}, G^{(k)}]$, for $k \geq 0$. Solvable groups had some nice properties: subgroups and quotients of solvable groups are solvable. Also, if $N \trianglelefteq G$, then G is solvable if and only if N and G/N are solvable. This should be thought of as the key property of solvable groups.

Historical Aside

Consider an irreducible polynomial $f \in \mathbb{Q}[x]$. What are its roots?

For example, when $f = ax^2 + bx + c$ with $a \neq 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Can we find similar solutions to other polynomials, where "similar" means "in terms of radicals"? This motivates the following definition:

Definition 1.10.1. We say f is solvable in radicals if its roots are in a finite extension $L/\mathbb{Q}$, with $L \subseteq \mathbb{C}$, and $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ such that $\alpha_i^{n_i} \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ for $i = 1, \ldots, n$ for some $n_i \geq 1$.

As an example, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3 + \sqrt{5}})$ is a field that satisfies the above conditions.

Example 1.10.2. Let $f = x^4 + x^3 + x^2 + x + 1 = \frac{x^5-1}{x-1}$. One solution is $x = e^{2\pi i/5}$, that is,

$$x = \left(\frac{\sqrt{5}}{2} - \frac{1}{4}\right) + \frac{1}{2}\left(\sqrt{\frac{5}{4} + \frac{\sqrt{5}}{2}} + \sqrt{\frac{5}{4} - \frac{\sqrt{5}}{2}}\right) i.$$

So f is solvable in radicals.

Let $K \subseteq \mathbb{C}$ be the extension of $\mathbb{Q}$ generated by the roots of f.

Definition 1.10.3. The Galois group of f is $G := \mathrm{Aut}(K)$, that is, the group of field automorphisms of K. That is, if $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ are the roots of f, then we get a homomorphism

$$\varphi \colon G \hookrightarrow S_d$$

given by $\sigma(\alpha_i) = \alpha_{\varphi(\sigma) \cdot i}$.

We have

Theorem 1.10.4. *The polynomial f is solvable in radicals if and only if $G = \mathrm{Aut}(K)$ is solvable.*

For example, if $f = x^4 + x^3 + x^2 + x + 1$ then $G \cong (\mathbb{Z}/5\mathbb{Z})^\times$ (because elements σ of G correspond to integers $a \in (\mathbb{Z}/5\mathbb{Z})^\times$, where the correspondence comes from $\sigma(e^{2\pi i/5}) = e^{2\pi i a/5}$).

As another example, if $d = \deg f \leq 4$, then $G \hookrightarrow S_d$, where S_d is solvable (for $d \leq 4$). So G is solvable because it is a subgroup, and so f is solvable in radicals.

Finally, if $f = x^5 - x - 1$, then $G \cong S_5$, which is not solvable, so f is not solvable in radicals.

This is foreshadowing; we'll see more of this in 6320, and more of field theory in 6310.

By the way, we have two major results on solvable groups:

Theorem 1.10.5 (Burnside)**.** *If $|G| = p^a q^b$, for p, q prime, then G is solvable.*

The proof isn't so bad, it's in Dummit/Foote, but one needs some representation theory to do it.

Theorem 1.10.6 (Feit-Thompson)**.** *If $|G|$ is odd, then G is solvable.*

The proof of *this* one lasts more than 250 pages. It was a pivotal first step in the classification of finite simple groups.

Let's reset.

Nilpotent Groups

We begin with a definition:

Definition 1.10.7. The lower central series of G is the series defined by

$$C^0G := G, C^{i+1}G = [G, C^iG]$$

for $i \geq 0$.

We should observe that

$$G = C^0G \supseteq C^1G \supseteq \cdots \supseteq C^nG \supseteq \dots$$

The book apparently uses G^i, and the previous professor of this class used $G^{[i]}$; we'll use C^i, where C is the "central" in "lower central series".

Definition 1.10.8. We say G is nilpotent if $C^nG = 1$ for some $n \geq 0$. The number n is the nilpotency class.

As an example, if G is abelian, then $C^1G = [G, G] = 1$.

Proposition 1.10.9. *If G is nilpotent, then G is solvable.*

Proof. Just observe that

$$C^iG/C^{i+1}G = C^iG/[G, C^iG],$$

but also notice that $[G, C^iG] \supseteq [C^iG, C^iG]$, so the quotient is abelian (see Lemma 1.5.2). □

Definition 1.10.10. We say G is a central extension of a group Γ by an abelian group A if there is an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] & G \arrow[r] & \Gamma \arrow[r] & 1 \end{tikzcd}$$

with $A \subseteq Z(G)$.

Proposition 1.10.11. *The group G is nilpotent of nilpotency class at most n if and only if G is a central extension of a nilpotent group Γ of nilpotency class at most $n-1$.*

The idea is that this proposition gives us a way to induct (similar to the case of solvable groups). Let's prove this:

Proof. Let's first prove the forward direction: we have $C^nG = 1$, so $C^{n-1}G \subseteq Z(G)$ since $[G, C^{n-1}G] = C^nG = 1$: recall that by definition $[G, C^{n-1}G] = \langle g^{-1}h^{-1}gh \rangle$ for $g \in G, h \in C^{n-1}G$ and $g^{-1}h^{-1}gh = 1$; this says $gh = hg$ and so $h \in Z(G)$.

So we define

$$A = C^{n-1}G, \quad \Gamma = G/A$$

and since

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] & G \arrow[r] & \Gamma \arrow[r] & 1 \end{tikzcd}$$

is a short exact sequence, we have $C^{n-1}\Gamma = A/A = 1 \subseteq \Gamma$, so Γ is nilpotent, with nilpotency class at most $n-1$.

Conversely, if we have a short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] & G \arrow[r] & \Gamma \arrow[r] & 1 \end{tikzcd}$$

such that $C^{n-1}\Gamma = 1$, then $C^{n-1}G \subseteq A$ and $C^nG = [G, C^{n-1}G] \subseteq [G, A] = 1$ since $A \subseteq Z(G)$. So G is nilpotent of nilpotency class at most n. □

We get a different way of building up groups: if we considered short exact sequences

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] & G \arrow[r] & \Gamma \arrow[r] & 1 \end{tikzcd}$$

with $A \trianglelefteq G$ and solvable, then G itself was solvable; if now we insist that $A \leq G$ is abelian, then the G we construct will be nilpotent.

Example 1.10.12. Let G be a p-group. We claim that G is nilpotent.

Proof. We'll induct on $|G|$. For the base case, we have $|G| = 1$, which is nilpotent. We want to find subgroups of the center, but we showed that p-groups have nontrivial center (in fact, we showed that p divides $Z(G)$, see Proposition 1.5.3).

Suppose $G \neq 1$ and smaller p-groups are nilpotent. Also, $Z(G) \trianglelefteq G$, so we have that $G/Z(G)$ is nilpotent (by the inductive hypothesis).

$$\begin{tikzcd} 1 \arrow[r] & Z(G) \arrow[r] & G \arrow[r] & G/Z(G) \arrow[r] & 1 \end{tikzcd}$$

□

Next time we'll talk about some of the key properties of nilpotent groups and begin finishing up group theory.

1.11 Sep 19, 2018

Today, we'll talk just a little bit more about nilpotent groups and then we'll move on.

Recall that we had an exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

and that if N and G/N are solvable, then G itself was also solvable. Also, all abelian groups are solvable. "These are basically what solvable groups are": you start with abelian groups and build up, that is, you can deconstruct solvable groups into abelian groups.

We also had nilpotent groups, which are what you get when the exact sequences above are more restricted. That is, we talked about central extensions

$$1 \longrightarrow A \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$$

where $A \subseteq Z(G)$. We have that abelian groups are nilpotent, and if Γ is nilpotent, then so is G. In this setup it's clear that nilpotent groups are solvable.

These families of groups are nice for inductive proofs. Here's an example:

Proposition 1.11.1. *Let G be nilpotent, and $H < G$ a proper subgroup. Then $H \subsetneq N_G(H)$.*

As an example of the power of this, this implies that maximal subgroups are normal.

Proof. We induct on the nilpotency class n of G (recall we had the sequence $C^0G = G$ and $C^{i+1}G = [G, C^iG]$, and n is the smallest integer such that $C^nG = 1$). If $n = 0$ then $G = 1$, so it's vacuously true. For $n = 1$, then G is abelian, which means $N_G(H) = G$, as desired. Now we can do the inductive step.

Let $A = Z(G)$. Last time we showed that $G/Z(G) = G/A$ is nilpotent with nilpotency class at most $n - 1$. We have two cases:

If $A \subseteq H$ then $H/A < G/A$; the inductive hypothesis says that

$$H/A \subsetneq N_{G/A}(H/A) = N_G(H)/A$$

where the equality follows because $A \subseteq H$. So this implies $H \subsetneq N_G(H)$, as desired.

If $A \not\subseteq H$, then $A = Z(G) \subseteq N_G(H)$, and so $N_G(H) \supsetneq H$. □

There is the following result, which is not so nice to present:

Theorem 1.11.2. *Let G be a finite group. The following are equivalent:*

1. *G is nilpotent*
2. *G is a product of p-groups for some primes p (you can have different primes appearing)*
3. *For every prime p, G has a unique p-Sylow subgroup*
4. *Any two elements of G of relatively prime order commute.*

Remark 1.11.3. It's not hard to show that the product of two nilpotent groups is nilpotent, and last time we showed that p-groups are nilpotent. So 2 is not so hard, and 3 is not so hard either (the p-Sylow subgroup is the product of the p-groups for a fixed p).

Remark 1.11.4. Number theory is full of theorems where one "fights their way up" from abelian groups to nilpotent/solvable groups. Often the abelian case is well understood and the nonabelian case is harder, but you can scrape the abelian things together and say something about the nonabelian things.

Free Groups

Fix a set S. We will define a group F_S and a map $i\colon S \hookrightarrow F_S$. Intuitively, S is a set of generators for F_S with no relations except those imposed by the group axioms (so for example, $ac = abb^{-1}c$ is imposed by the group axiom, but $ab = ba$ is not). We will prove:

Theorem 1.11.5 (Universal property of free groups)**.** *For any map $\varphi\colon S \to G$, where G is a group, then there is a unique group homomorphism $\Phi\colon F_S \to G$ such that $\Phi \circ i = \varphi$, that is,*

$$\begin{tikzcd}
S \arrow[r, hook, "i"] \arrow[dr, "\varphi"'] & F_S \arrow[d, "\exists!\Phi"] \\
& G
\end{tikzcd}$$

commutes.

Remark 1.11.6. Suppose there is $i'\colon S \to F'_S$ has the same property. Then the universal property for F_S and again for $F_{S'}$ gives

$$\begin{tikzcd}
& F_S \arrow[dd, bend right, "f"'] \\
S \arrow[ur, "i"] \arrow[dr, "i'"'] & \\
& F_{S'} \arrow[uu, bend right, "g"']
\end{tikzcd}$$

We claim that f and g are inverses. Indeed,

$$\begin{tikzcd}
S \arrow[r, "i"] \arrow[dr, "i"'] & F_S \arrow[d, "g\circ f"] \\
& F_S
\end{tikzcd}$$

commutes, but uniqueness of the homomorphism says that $g \circ f = \mathrm{id}_{F_S}$. For exactly the same reason, $f \circ g = \mathrm{id}_{F_{S'}}$. So the moral is that F_S is determined (with $i\colon S \hookrightarrow F_S$ up to natural isomorphism).

Let us construct F_S. We first choose a set S^{-1} such that it is that is disjoint from S and that there is a bijection $S \to S^{-1}$, given by $s \mapsto s^{-1}$, and $s^{-1} \leftarrow\!\shortmid s$. (this are just some symbols, this isn't a group yet). Let $T = S \cup S^{-1}$, which you can think of $T = \{(s,i)\colon s \in S, i \in \{\pm 1\}\}$.

A <u>word</u> in T is a finite sequence $w = (a_1, \dots, a_n)$ with $a_n \in T$. Alternatively, we can concatenate these to form some string $a_1 \dots a_n$. The word is <u>reduced</u> if $a_{i+1} \neq a_i^{-1}$ for all i.

Let F_S be the set of all reduced words in T, with the following group structure $(a_1 \dots a_n) \cdot (b_1 \dots b_m)$ is the reduced word of the concatenation $a_1 \dots a_n b_1 \dots b_m$. There are things to check: associativity is pedantic, the identity is the empty word (which we still denote by 1), and the inverse of $a_1 \dots a_n$ is $a_n^{-1} \dots a_1^{-1}$.

Also, $i\colon S \hookrightarrow F_S$ is the inclusion $s \mapsto s$. Now the universal property holds if we define Φ to be the map $\Phi(a_1^{e_1} \dots a_n^{e_1}) = \varphi(a_1)^{e_1} \cdot \varphi(a_n)^{e_n}$. Here are some results about free groups:

1. Up to isomorphism, F_S depends only on the cardinality of S (will be on the next homework).
2. (Nielsen-Schreier) A subgroup of a free group is free.

The second result is not as easy as one might expect: for $|S| = 2$, we have $[F_S, F_S] \cong F_{S'}$ with S' infinite.

1.12 Sep 21, 2018

Last time, we fixed a set S and constructed a free group F_S with $S \subseteq F_S$ generating the group. The main property was that any map $\varphi\colon S \to G$ extends to a unique homomorphism $\Phi\colon F_S \to G$.

Consider the wedge of n circles, as a topological space its fundamental group is $\pi_1(X,P) \cong F_{[n]}$ [here $[n] = \{1, 2, \ldots, n\}$], so sometimes one can use algebraic topology to understand free groups (see Nielsen-Schreier; the proof uses algebraic topology).

Presentations

[Prof Zywina thought that the previous 6310 had *group presentations*, and then realized that they were talking about presentations of groups.]

Let S be a set, and consider again F_S the free group on S generators. Let R be a set of words in $S \cup S^{-1}$, and define the group

$$\langle S|R\rangle := F_S/N,$$

where N is the smallest normal subgroup of F_S containing R. This is called a presentation of the group $\langle S|R\rangle$.

Remark 1.12.1. Any group is of the form $\langle S|R\rangle$. Indeed, choose generators S of G, and get a $\varphi\colon S \twoheadrightarrow G$, so it induces a unique $\Phi\colon F_S \twoheadrightarrow G$, and the kernel of this map can be chosen to be N.

We say G is finitely presented if $G \cong \langle S|R\rangle$ with both S and R finite.

Example 1.12.2. Consider $\langle \{a\}|\{a^n\}\rangle = \langle a|a^n\rangle$ (forget about the brackets); this is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ (via the isomorphism $a \mapsto 1$).

Example 1.12.3. Consider $\langle a, b|b^3, a^{-1}b^{-1}ab\rangle = \langle a, b|b^3 = 1, ab = ba\rangle$. We let a, b be the image of a, b in G. Then $G \cong \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, given by the map $a \mapsto (1, 0)$ and $b \mapsto (0, 1)$.

Example 1.12.4. We have $D_{2n} \cong \langle r, s|r^n = 1, s^2 = 1, s^{-1}rs = r^{-1}\rangle$. Since $rs = sr^{-1} = sr^{n-1}$ we can write elements of $\langle r, s|r^n = 1, s^2 = 1, s^{-1}rs = r^{-1}\rangle =: G$ as $\{s^i r^j : i = 0, 1, 0 \le j < n\}$, so $|G| \le 2n$. This gives the isomorphism to D_{2n}.

Example 1.12.5. Let $G := \langle a, b|a^2 = b^3 = 1\rangle$. It's a fact that

$$G \cong \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}.$$

The isomorphism is given by

$$a \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad b \mapsto \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}$$

and there is some work to show that the images of a, b generate $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ and even more work to show that this really does give an isomoprhism.

In general, it is undecidable to determine if $\langle S|R\rangle$ is finite (or trivial, or abelian) when S and R is finite (where "undecidable" is in the precise computer science sense). So just given a presentation it can be very mysterious what the group is. More generally, given a word g, there is no algorithm to determine if it is trivial in $\langle S|R\rangle$.

In general, it is a challenge to show that there is a homomorphism out of the presentation into the group you think it should be; thankfully usually there is some extra information (like in the case of D_{2n}, we knew its size). On the other hand a homomorphism from the group you think it should be into the presentation isn't so hard.

Direct Products

We'll talk about direct products and next lecture we'll also talk about semidirect products and that'll basically be the end of our group theory.

Fix groups H and K. This gives a group $H \times K$ (endowed with component-wise multiplication). The relevant question to ask is: Given a group G, how does one detect whether or not it is a direct product?

By abuse of notation, we let $H := H \times 1 \subseteq G$ and $K := 1 \times K \subseteq G$ (where $G = H \times K$). There are some properties we knew about H and K: we have

- $H \trianglelefteq G, K \trianglelefteq G$
- $HK = \{hk \colon h \in H, k \in K\} = G$
- $H \cap K = 1$.

The claim is that these properties are sufficient, in the following sense:

Proposition 1.12.6. *Fix a group G. Suppose H and K are normal subgroups of G such that $HK = G$ and $H \cap K = 1$. Then*

$$\begin{aligned} H \times K &\to G \\ (h,k) &\mapsto hk \end{aligned}$$

is an isomorphism.

Proof. We first show that H and K commute. Let $h \in H$ and $k \in K$, and consider the commutator $h^{-1}k^{-1}hk = (kh)^{-1}hk$. Now we have

$$h^{-1}k^{-1}hk = h^{-1}\underbrace{(k^{-1}hk)}_{\in H} \in H, \quad \text{and} \quad h^{-1}k^{-1}hk = \underbrace{(h^{-1}k^{-1}h)}_{\in K} k \in K$$

so $h^{-1}k^{-1}hk \in H \cap K = 1$, and hence $hk = kh$. Knowing this it is easier to check that $\varphi \colon H \times K \to G$ given by $(h,k) \mapsto hk$ is a homomorphism. Notice that φ is surjective since $HK = G$. To see that φ is injective, notice that if $\varphi(h,k) = 1$ we have $hk = 1$, and hence $h = k^{-1} \in H \cap K = 1$. So $(h,k) = (1,1)$, as desired. □

Semidirect Products

Now we want to loosen the assumptions:

Let H and K be subgroups of G such that $H \trianglelefteq G$ and $H \cap K$ and $G = HK$. Note that without the assumption $G = HK$, we still have that HK is always a subgroup of G.

As before, $\varphi \colon H \times K \to HK = G$ given by $(h,k) \mapsto hk$ is still a bijection, though it need not be a homomorphism. To define $H \rtimes K$ (the semidirect product), we'll understand how multiplication works in HK and pull the multiplication over to $H \times K$ (as a set) to give it a group structure.

So let $h_1, h_2 \in H$, and $k_1, k_2 \in K$. Then

$$\begin{aligned} (h_1k_1)(h_2k_2) &= h_1k_1h_2(k_1^{-1}k_1)k_2 \\ &= (h_1 \underbrace{k_1h_1k_1^{-1}}_{\in H\ (H \trianglelefteq G)}) \cdot \underbrace{k_1k_2}_{\in K} \end{aligned}$$

and since φ was a bijection this is the unique way of writing $(h_1k_1)(h_2k_2)$ as an element of HK. Note that K acts on H by conjugation. So this will define a multiplication on $H \times K$.

1.13 Sep 24, 2018

We're going to finish up semi-direct products and then begin rings.

Last time, we had a group G with two subgroups H and K such that

- $H \trianglelefteq G$
- $HK = G$
- $H \cap K = 1$.

We saw that there was a map $H \times K \to G$ given by $(h, k) \mapsto hk$ is a bijection, but not a homomorphism. In particular, we had, for $h_1, h_2 \in H, k_1, k_2 \in K$,

$$(h_1k_1)(h_2k_2) = \underbrace{(h_1k_1h_2k_1^{-1})}_{\in H} \cdot \underbrace{(k_1k_2)}_{\in K}$$

and since $H \times K \to G$ is a bijection this is the unique way of writing $(h_1k_1)(h_2k_2)$ as a product of two elements $h'k'$ for some $h' \in H, k' \in K$. Note that K acts on H by conjugation, that is, there is a $\varphi \colon K \to \mathrm{Aut}(H)$.

Let's do a reset. Let H and K be groups, and let K be an action on H such that $\varphi \colon K \to \mathrm{Aut}(H)$. We define

$$H \rtimes_\varphi K = H \rtimes K$$

to be the group consisting of the set $H \times K$ with the multiplication

$$(h_1, k_1) \cdot (h_2, k_2) := (h_1(k_1 \cdot h_2), k_1k_2) = (h_1 \cdot \varphi_{k_1}(h_2), k_1k_2).$$

We say that $H \rtimes K$ is the semidirect product of H and K. This is a group.

The triangle in $\rtimes$ points in the direction it would in the above setup (we had $H \trianglelefteq G$). The identity in this group is $(1, 1)$. We have $\varphi \colon K \to \mathrm{Aut}(H)$ is a homomorphism into the automorphism group, $\varphi_1 = \mathrm{id}_H$, so

$$(1, 1) \cdot (h, k) = (1 \cdot (1 \cdot h), 1 \cdot k) = (h, k).$$

Also since φ_k is an automorphism of H, we have $\varphi_k(1) = 1$, and so

$$(h, k) \cdot (1, 1) = (h \cdot (k \cdot 1), k \cdot 1) = (h, k).$$

We have $(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$, since

$$(h, k) \cdot (k^{-1} \cdot h^{-1}, k^{-1}) = (h \cdot k \cdot (k^{-1} \cdot h^{-1}), k \cdot k^{-1}) = (1, 1).$$

We can identify H and K with $H \times 1 \subseteq H \rtimes_\varphi K$ and $1 \times K \subseteq H \rtimes_\varphi K$. We can also check that H and K are subgroups of $H \rtimes_\varphi K$, with $HK = H \rtimes_\varphi K$ and $H \cap K = 1$ and $H \trianglelefteq H \rtimes_\varphi$.

Furthermore, for $h \in H$ and $k \in K$, we have $k \cdot h = khk^{-1}$ (where on the left side $k \in K$ is acting on $h \in H$, giving an element of $H \hookrightarrow H \times 1$, whereas on the right side we are multiplying in $H \rtimes_\varphi K$ [the claim is that this will land inside $H \times 1$ and in particular *is* the element $k \cdot h \in H \times 1$]).

Example 1.13.1. For $\varphi = 1$, we have $H \rtimes_\varphi K = H \times K$ as groups!

Example 1.13.2. For $H = \mathbb{R}$, and $K = \mathbb{R}^\times$, we have $K \circlearrowright H$ by $k \cdot h = kh$ (multiplication as a real number). From this, we get a group $H \rtimes K$. It turns out that

$$H \rtimes K \cong G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in \mathbb{R}^\times, b \in \mathbb{R} \right\}.$$

Inside G we have $H_1 \trianglelefteq G$ given by

$$H_1 = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{R} \right\} \cong \mathbb{R}$$

and

$$K_1 = \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} : a \in \mathbb{R}^\times \right\} \cong \mathbb{R}^\times.$$

We can also verify that

$$\begin{aligned} &\underbrace{\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}}_{:=k} \underbrace{\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}}_{:=h} \underbrace{\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}^{-1}}_{:=k^{-1}} \\ &= \begin{bmatrix} a & ab \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a^{-1} & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & ab \\ 0 & 1 \end{bmatrix} \end{aligned}$$

so that $khk^{-1} = k \cdot h$, as claimed earlier.

Example 1.13.3. Let $H = \langle r \rangle$ and $K = \langle s \rangle$, where H is the cyclic group of order n, and K is the cyclic group of order 2. We have $\varphi \colon K \to \operatorname{Aut}(H)$ given by $\varphi_s \colon H \to H$ sending $x \mapsto x^{-1}$. We have $H \rtimes_\varphi K \simeq D_{2n}$.

Remark 1.13.4. If $G = H \rtimes K$ then we actually have a split exact sequence

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r] & G \arrow[r] & K \arrow[r] \arrow[l, bend right, dashed] & 1 \end{tikzcd}$$

since G has a copy of K sitting inside it.

2 Rings

2.13 Sep 24, 2018

[We should read chapter 7 of Dummit/Foote]. Everybody should know what a ring is.

Definition 2.13.1. A ring is a set R with two binary operations $+$ and $\cdot$ (ie. addition and multiplication) such that the following hold:

a) $(R, +)$ is an abelian group (with additive identity denoted by 0)

b) Multiplication is associative, that is, $a(bc) = (ab)c$ for $a, b, c \in R$.

c) There is a distributive law, that is, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for $a, b, c \in R$.

d) There is an element $1 \in R$ such that $1a = a = a1$ for all $a \in R$.

As a warning, Dummit and Foote do not include d). But to Prof Zywina, these are called rngs (there's no identity).

We say that R is commutative if $ab = ba$ for all $a, b \in R$. It's noncommutative otherwise. Some examples include $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $R[x]$, $M_n(R)$, $R[[x]]$, $C(\mathbb{R})$, and $R = \{0\}$ (though some people assume an axiom $0 \neq 1$).

We also have the ring RG (called a group ring) for G a finite group and R a ring, defined to be the set of formal sums $\sum_{g \in G} a_g \cdot g$ with $a_g \in R$, given by

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

and

$$\sum_{g \in G} a_g g \cdot \sum_{g \in G} b_g g = \sum_{g, h \in G} a_g b_h gh = \sum_{g \in G} \left(\sum_{\substack{h_1, h_2 \in G \\ h_1 h_2 = g}} a_{h_1} b_{h_2} \right) g.$$

It turns out that the group ring $\mathbb{C}G \cong \Pi_{i=1}^r M_{n_i}(\mathbb{C})$, and this is linked to the representation theory of G (take 6320!).

Under his definition, $2\mathbb{Z}$ is not a ring, though it is a rng (and is hence a ring under Dummit/Foote convention).

Definition 2.13.2. A subring of a ring R is a subset $S \subseteq R$ such that

- $a + b \in S$ for $a, b \in S$
- $-a \in S$ for $a \in S$
- $ab \in S$ for $a, b \in S$
- $1 \in S$.

We have S is a ring with $+, \cdot, 1$ inherited from R.

We say an element $a \in R$ is a unit if $ab = 1 = ba$ for some $b \in R$. The set of units in R is denoted by $R^\times$. This can be given a group structure via multiplication from elements of R.

For example, $\mathbb{Z}^\times = \{\pm 1\}$ and $\mathbb{R}^\times = \mathbb{R} - \{0\}$ and $M_n(\mathbb{R})^\times =: \mathrm{GL}_n(\mathbb{R})$ and $\mathbb{R}[x]^\times = \mathbb{R}^\times$.

For a wild example, for a commutative ring R we have

$$R[x]^\times = \{a_0 + a_1 x + \cdots + a_n x^n : a_0 \in R^\times, a_i \text{ nilpotent }, i \geq 1\},$$

where nilpotent elements $a \in R$ are those such that $a^k = 0$ for some $k \geq 1$. This would need some proof, which is omitted.

Of course, this means that for R a field, we have $R[x]^\times = R^\times$.

2.14 Sep 26, 2018

Let R be a ring. Recall that a (left) ideal of R is a nonempty $I \subseteq R$ such that

- $a + b \in I$ for $a, b \in I$
- $ra \in I$ for $r \in R, a \in I$.

In other words, I is an R-submodule of R (where R acts on itself by left multiplication). Right ideals also exist; when R is commutative this distinction does not matter.

Example 2.14.1. Let $f\colon R \to S$ be a ring homomorphism, that is, a map f such that

- $f(a + b) = f(a) + f(b)$
- $f(ab) = f(a)f(b)$
- $f(1) = 1$

Then $\ker f = \{r \in R\colon f(r) = 0\}$ is an ideal of R.

Example 2.14.2. Let $a_1, \ldots, a_n \in R$ be elements of R. One can consider the ideal generated by $a_1, \ldots, a_n$, given by

$$\langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n \colon r_i \in R\}.$$

You can have infinitely many a_i's but the ideal generated by them will be the set of finite linear combinations of the a_i.

Let $I \subseteq R$ be an ideal of a commutative ring R. We can look at the cosets

$$R/I := \{r + I \colon r \in R\}$$

where $r + I = \{r + a \colon a \in I\}$. We have that R/I is a ring with operations $(a+I)+(b+I) = (a+b)+I$ and $(a + I) \cdot (b + I) = ab + I$. There is a homomorphism $R \to R/I$ given by $r \mapsto r + I$; its kernel is precisely I.

Example 2.14.3. Let $R = \mathbb{Z}$ and fix $n \geq 1$ consider the ideal $\langle n \rangle = n\mathbb{Z}$. The homomorphism $\mathbb{Z}/n\mathbb{Z}$ is the familiar ring of integers mod n.

Example 2.14.4. Consider $R = \mathbb{R}[x]/\langle x^2 + 1\rangle$. We have $R \cong \mathbb{C}$ because there is a ring homomorphism $\mathbb{R}[x] \to \mathbb{C}$ given by $f(x) \mapsto f(i)$ that is surjective and has kernel $\langle x^2 + 1\rangle$.

Let R be a commutative ring.

Definition 2.14.5. An element $a \in R$ is a zero divisor if $ab = 0$ for some nonzero $b \in R$.

As an example, $[2] \in \mathbb{Z}/6\mathbb{Z}$ is a zero divisor.

Definition 2.14.6. We say $R \neq 0$ is an integral domain if it has no nonzero zero divisors.

Definition 2.14.7. We say $R \neq 0$ is a field if every $a \in R - \{0\}$ has a multiplicative inverse (that is, $ab = 1$ for $b \in R$). Equivalently, R is a field if it has exactly two ideals.

To see the equivalence, notice that $\langle a \rangle \supseteq \langle 1 \rangle = R$, so $\langle a \rangle = R$.

Fix an ideal $I \subseteq R$.

Definition 2.14.8. We say I is a prime ideal if $ab \in I$ with $a, b \in R$, then $a \in I$ or $b \in I$. Equivalently, I is prime if and only if R/I is an integral domain.

Definition 2.14.9. We say I is a maximal ideal if $I \subsetneq R$ and there are no ideals between I and R (wrt inclusion). Equivalently, I is maximal if and only if R/I is a field.

Observe that maximal ideals are prime (since fields are integral domains).

Theorem 2.14.10. *Let $R \neq 0$ be a commutative ring (with 1). Then R has a maximal ideal.*

Proof. Use Zorn's lemma. Let $\mathcal{P}$ be the set of proper ideals of R, and say that $P \neq \emptyset$ (and $0 \in \mathcal{P}$). Then $\mathcal{P}$ with $\subseteq$ is a partially ordered set. Take any nonempty chain $\mathcal{C} \subseteq \mathcal{P}$, that is, for $A, B \in \mathcal{C}$, we have $A \subseteq B$ or $B \subseteq A$. We want to find an upper bound for all the elements in this chain, but

$$J := \bigcup_{I \subseteq \mathcal{C}} I \subseteq R.$$

We claim that J is an ideal. It's nonempty because:

- It's nonempty, since $0 \in J$
- Take $a, b \in J$. Then $a \in A$ or $b \in B$; either $A \subseteq B$ or $B \subseteq B$ so $a + b \in A$ or $a + b \in B$. In either case, $a + b \in J$
- Take $a \in J, r \in R$. Then $a \in A$ for some $A \in \mathcal{C}$, so $ra \in A$, and so $ra \in J$.

We also need to show that J is a proper ideal of $\mathcal{P}$. But notice that if $J = R$, then $1 \in J$, and hence $1 \in A$ for some $A \in \mathcal{C}$, which is a contradiction because then $A = R$ and so $A \notin \mathcal{P}$. So $J \subsetneq R$ and $J \in \mathcal{P}$. In particular, J is an upper bound of $\mathcal{C}$.

By Zorn's lemma, $\mathcal{P}$ has a maximal element with respect to inclusion, that is, R has a maximal ideal. □

Remark 2.14.11. There are some crazy rings out there (especially the ones from analysis). This theorem in its full generality is equivalent to Zorn's lemma. On the other hand, for Noetherian rings, one can avoid using any big hammers.

Remark 2.14.12. This theorem fails for commutative rings without an identity.

Localization

This is in Dummit and Foote, in section 15.4. It's only a little fancier than the field of fractions construction, which is in Dummit and Foote 7.5.

Let R be a commutative ring with 1, and let $S \subseteq R$ be a multiplicatively closed set, that is, if $a, b \in S$ then $ab \in S$ (we don't assume any other structure). Assume that $1 \in S$ (you can replace S by $S \cup \{1\}$).

Theorem 2.14.13. *There is a commutative ring $S^{-1}R$ with a ring homomorphism $\pi\colon R \to S^{-1}R$ such that $\pi(b) \in (S^{-1}R)^\times$ for $b \in S$ and for any ring homomorphism $\varphi\colon R \to A$ with $\varphi(b) \in A^\times$ for all $b \in S$, then there is a unique ring homomorphism $\Phi\colon S^{-1}R \to A$ such that $\Phi \circ \pi = \varphi$. This is expressed in the commutative diagram*

$$\begin{tikzcd}
R \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & S^{-1}R \arrow[d, dashed, "\exists!\Phi"] \\
& A
\end{tikzcd}$$

Loosely, $S^{-1}R$ is the ring you obtain from R when you "invert" all elements of S. As an example, let $R = \mathbb{Z}$, and $S = \mathbb{Z} - \{0\}$, then the construction $S^{-1}R$ should produce $\mathbb{Q}$.

We call $S^{-1}R$ the localization of P at S, or sometimes the ring of fractions of R with respect to S.

Remark 2.14.14. The idea is that you want to invert some elements of R which may not be units, but we can homomorph into an A such that elements of S get sent to units. The construction says that "$S^{-1}R$" is the "best ring" to which we should send S to units (it's a fact that $\pi(b) \in (S^{-1}R)^\times$ for all $b \in S$).

Remark 2.14.15. The theorem gives a universal property that determines $S^{-1}R$ and $\pi\colon R \to S^{-1}R$ up to a uniquely determined isomorphism.

2.15 Sep 28, 2018

Let R be a commutative ring $S \subseteq R$ multiplicatively closed, with $1 \in S$. We had this theorem last time stated without proof:

Theorem 2.15.1. *There is a commutative ring $S^{-1}R$ with a homomorphism $\pi\colon R \to S^{-1}R$ such that $\pi(b) \in (S^{-1}R)^\times$ for all $b \in S$. Moreover, for any ring homomorphism $\varphi\colon R \to A$ with $\varphi(b) \in A^\times$ for $b \in S$, there is a unique homomorphism $\Phi\colon S^{-1}R \to A$ such that $\varphi = \Phi \circ \pi$, that is,*

$$\begin{tikzcd}
R \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & S^{-1}R \arrow[d, dashed, "\exists!\Phi"] \\
 & A
\end{tikzcd}$$

commutes.

We say $S^{-1}R$ is the localization of R at S.

Proof. Define a relation on $R \times S$ given by $(a, b) \sim (c, d)$ if and only if $x(ad - bc) = 0$ for some $x \in S$. Of course, if S has no zero divisors then this is true if and only if $ad - bc = 0$.

We claim that this is an equivalence relation. Obviously we are reflexive and symmetric. We are transitive: if $(a, b) \sim (c, d)$, so that $x(ad - bc) = 0$ for some $x \in S$, and $(c, d) \sim (e, f)$, so that there is y so that $y(cf - ed) = 0$ for some $y \in S$, then

$$0 = fyx(ad - bc) + bxy(cf - de) = xyd(af - be)$$

so that $(a, b) \sim (e, f)$. We let $\frac{a}{b}$ be the equivalence class of (a, b); we can now define

$$S^{-1}R := \left\{ \frac{a}{b} \colon a \in R, b \in S \right\}.$$

As an exercise, show that $S^{-1}R$ is a ring with

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

This not worth doing in lecture.

We have identities in $S^{-1}R$; the multiplicative one is $1 = \frac{1}{1}$ and the additive one is $0 = \frac{0}{1}$. We also have a canonical homomorphism

$$\pi\colon R \to S^{-1}R$$

that maps $r \mapsto \frac{r}{1}$. If S has no zero divisors (of R), then π is injective. Also, for $b \in S$, we have $(\frac{b}{1})^{-1} = \frac{1}{b}$, so elements in S have inverses.

Finally, take any map $\varphi\colon R \to A$ such that $\varphi(b) \in A^\times$ for $b \in S$. Then $\Phi\colon S^{-1}R \to A$ given by $\frac{a}{b} \mapsto \varphi(a)\varphi(b)^{-1}$ is a homomorphism such that $\Phi \circ \pi = \varphi$. □

The key example is the following:

Example 2.15.2. Let R be an integral domain and $S = R - \{0\}$. We have that S is multiplicatively closed (because R is integral domain) and contains 1. So we can consider $S^{-1}R$: it is called the fraction field or quotient field of R. Since S has no zero divisors $R \hookrightarrow S^{-1}R$ by $r \mapsto \frac{r}{1}$.

We understand these well: this construction maps $\mathbb{Z} \to \mathbb{Q}$ and $\mathbb{R}[x] \to \mathbb{R}(x)$.

Example 2.15.3 (Localization at a prime)**.** Let R be a commutative ring, and $\mathfrak{p} \subseteq R$ prime ideal, and $S := R\backslash\mathfrak{p}$; notice that S is multiplicatively closed since if $a, b \in S$ such that $ab \in \mathfrak{p}$ (that is, $ab \notin S$), but this means that either a or b is also in $\mathfrak{p}$, which is not true (they were both in S). So $ab \in S$.

The localization $S^{-1}R$ is sometimes denoted $R_{\mathfrak{p}}$. For example, we have $\mathbb{Z}_{\langle p\rangle} = \{\frac{a}{b} \colon p \nmid b\}$. You can also consider $\mathbb{C}[x,y]_{\langle x,y\rangle}$, where $\langle x,y\rangle = \{f \in \mathbb{C}[x,y] \colon f(0,0) = 0\}$. Thus,

$$\mathbb{C}[x,y]_{\langle x,y\rangle} = \left\{\frac{f}{g} \colon f, g \in \mathbb{C}[x,y], g(0,0) \neq 0\right\};$$

that is, we have functions that make sense in a neighborhood of $(0,0)$, so in this sense things are "local".

Example 2.15.4. Let $R = \mathbb{Z}/6\mathbb{Z}$ and $S = \{1,2,4\}$ (so we are trying to invert zero divisors). Then one can show that $S^{-1}R \cong \mathbb{Z}/3\mathbb{Z}$, and$S^{-1}R$ is *smaller* than R, and $\pi \colon R \to S^{-1}R$ is not injective.

Theorem 2.15.5. *There is an inclusion preserving bijection*

$$\begin{aligned}\left\{\text{prime ideals } \mathfrak{p} \text{ of } R \text{ with } \mathfrak{p} \cap S = \emptyset\right\} &\longleftrightarrow \left\{\text{prime ideals of } S^{-1}R\right\} \\ \mathfrak{p} &\longmapsto S^{-1}\mathfrak{p} := \left\{\frac{a}{b} \colon a \in \mathfrak{p}, b \in S\right\} \\ \pi^{-1}(\mathfrak{q}) &\longleftarrow\!\shortmid \mathfrak{q}\end{aligned}$$

Let R be a commutative ring with 1. We can do some operations: for $I, J \subseteq R$ ideals, we have

- $I \cap J$ is an ideal (largest ideal in I and J)
- $I + J = \{a + b \colon a \in I, b \in J\}$ is an ideal (smallest ideal containing I and J)
- $IJ = \langle\{ab \colon a \in I, b \in J\}\rangle = \{\sum_{i=1}^{n} a_i b_i \colon a_i \in I, b_i \in J\}$

We say I and J are coprime (some people say comaximal) if $I + J = \langle 1\rangle = R$. Observe that if $R = \mathbb{Z}$, and $a, b \in \mathbb{Z}$ not both 0, then $\langle a\rangle + \langle b\rangle = \langle \gcd(a,b)\rangle$, so $\langle a\rangle$ and $\langle b\rangle$ are coprime if and only if $\gcd(a,b) = 1$.

Fix ideals $I_1, \ldots, I_n$ of R. Define a map by

$$\begin{aligned}\varphi \colon R &\to \prod_{i=1}^{n} R/I_i \\ r &\mapsto (r + I_1, \ldots, r + I_n).\end{aligned}$$

It is a homomorphism.

Theorem 2.15.6 (Chinese Remainder Theorem)**.** *Suppose the ideals I_i, I_j are coprime for $i \neq j$. Then φ is surjective, and the kernel is $I_1 \cap \cdots \cap I_n = I_1 \ldots I_n$.*

2.16 Oct 1, 2018

Let R be a commutative ring. For ideals $I, J \subseteq R$, we have new ideals $I + J$, $I \cap J$, and IJ; they satisfy the inclusions

$$\begin{tikzcd}
& I + J \arrow[dl, dash] \arrow[dr, dash] & \\
I \arrow[dr, dash] & & J \arrow[dl, dash] \\
& I \cap J \arrow[d, dash] & \\
& IJ &
\end{tikzcd}$$

We say that I and J are coprime if $I + J = R$. For $R = \mathbb{Z}$, the above picture looks like

$$\begin{tikzcd}
& \langle \gcd(a,b) \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle a \rangle \arrow[dr, dash] & & \langle b \rangle \arrow[dl, dash] \\
& \langle \operatorname{lcm}(a,b) \rangle \arrow[d, dash] & \\
& \langle ab \rangle &
\end{tikzcd}$$

Lemma 2.16.1. *If I and J are coprime, then $I \cap J = IJ$.*

Proof. We just need to show $I \cap J \subseteq IJ$.

Take $a \in I \cap J$. Recall I and J are coprime, so that $x + y = 1$ for some $x \in I, y \in J$. So $a = ax + ay$, but $a \in J$ and $x \in I$, whereas $a \in I$ and $y \in J$, so $ax + ay \in IJ$. □

Let $I_1, \ldots, I_n$ be ideals of R such that I_i and I_j are coprime for $i \neq j$ (that is, they're pairwise coprime). We define the usual ring homomorphism

$$\varphi \colon R \to \prod_{i=1}^{n} R/I_i,$$

that is, $\varphi(r) = (r + I_1, \ldots, r + I_n)$.

Theorem 2.16.2 (Chinese Remainder Theorem)**.** *With assumptions as above, φ is surjective. Furthermore,*

$$\ker(\varphi) = I_1 \cap \cdots \cap I_n = I_1 \ldots I_n.$$

Remark 2.16.3. There is content in the second equality. It also gives the immediate consequence that

$$R/(I_1 \ldots I_n) \xrightarrow{\sim} R/I_1 \times \cdots \times R/I_n.$$

So you can use the Chinese Remainder Theorem in two ways: you can break up a ring into simpler rings (by the above isomorphism), or you can generate some interesting elements (because φ above is surjective) which are useful in proofs.

Example 2.16.4. Let $n = p_1^{e_1} \ldots p_r^{e_r}$. Then

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \prod_{i=1}^{r} \mathbb{Z}/p_i^{e_i}\mathbb{Z}.$$

Proof. Let's first show that $I_1 \cap \dots \cap I_n = I_1 \dots I_n$. The proof is by induction; for $n = 1$ this is obvious, and $n = 2$ is Lemma 2.16.1. So assume $n > 2$ and that the result is known for smaller n.

We have

$$\begin{aligned} I_1 \cap \dots \cap I_n &= I_1 \cap (I_2 \cap \dots \cap I_n) \\ &= I_1 \cap (I_2 \dots I_n) \end{aligned}$$

by induction; we need only show that I_1 and $I_2 \dots I_n$ are coprime (this will imply that $I_1 \cap (I_2 \dots I_n) = I_1 \dots I_n$, as desired).

For each $2 \leq i \leq n$ there is $x_i \in I_1, y_i \in I_i$ so that $1 = x_i + y_i$. So

$$1 = \prod_{i=2}^{n}(x_i + y_i) \equiv \prod_{i=2}^{n} y_i \pmod{I_1},$$

where we define $a \equiv b \pmod{I_1}$ if and only if $a - b \in I_1$. This means

$$1 = \underbrace{\left(\prod_{i=2}^{n}(x_i + y_i) - \prod_{i=2}^{n} y_i\right)}_{\in I_1} + \underbrace{\prod_{i=2}^{n} y_i}_{I_2 \dots I_n}$$

and so $1 \in I_1 + I_2 \dots I_n$.

Now we show that φ is surjective. It suffices to show that there is $r \in R$ so that $\varphi(r) = (1, 0, \dots, 0)$ (and every other standard basis element of $R/I_1 \times \dots \times R/I_n$), because φ is linear.

Recall that $I_1 + I_i = R$. Then $1 = x_i + y_i$ with $x_i \in I_1$ and $y_i \in I_i$. Take $r := y_2 \dots y_n = \prod_{i=2}^{n} y_i$. This says that $r \in I_i$ for $i \geq 2$, since $y_i \in I_i$. On the other hand,

$$r = \prod_{i=2}^{n} y_i = \prod_{i=2}^{n}(1 - x_i) \equiv \prod_{i=2}^{n}(1 - 0) = 1 \pmod{I_1}$$

since $x_i \in I_1$. This completes the proof. □

Definition 2.16.5. We say that a commutative ring R is Noetherian if one of the following (equivalent) conditions hold:

(a) R satisfies the *Ascending Chain Condition (ACC)*: If we have an ascending chain

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

for ideals I_n of R, then for some n, it stabilizes, that is,

$$I_n = I_{n+1} = I_{n+2} = \dots.$$

(b) Every nonempty set of ideals in R has a maximum (with respect to inclusion).

(c) All ideals are finitely generated.

Remark 2.16.6. Condition (b) allows us to avoid Zorn's lemma in some proofs (unfortunately, we'd have to restrict to Noetherian rings...)

Proof. We first show (a) implies (b).

Let Σ be a nonempty set of ideals with no maximum. Choose $I_1 \in \Sigma$. Inductively define $I_2, I_3, \dots$ by observing that for $n \geq 2$, I_{n-1} is not maximal in Σ, so there is $I_n \in \Sigma$ such that $I_{n-1} \subsetneq I_n$. Thus

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots,$$

contradicting (a).

Now we prove (b) implies (c).

Take any ideal $I \subseteq R$. We define the set

$$\Sigma := \{J \colon J \subseteq I, J \text{ finitely generated ideal of } R\}.$$

Take a maximal set $J \subseteq \Sigma$. If $J = I$ we're done because I is finitely generated. If $J \subsetneq I$, then take $a \in I - J$, and observe that the finitely generated ideal $J + \langle a \rangle \supsetneq J$, so J could not have been maximal.

Finally we should show (c) implies (a). Given an ascending chain

$$I_1 \subseteq I_2 \subseteq \dots$$

we consider the ideal

$$I := \bigcup_{i=1}^{\infty} I_i \subseteq R,$$

which is finitely generated, so $I = \langle a_1, \dots, a_r \rangle$. But there is an N such that $a_i \in I_n$ for all $n \geq N$; this says that

$$\langle a_1, \dots, a_r \rangle \subseteq I_n \subseteq I$$

so that $I_n = I$ for all $n \geq N$. □

Remark 2.16.7. It's quite terrifying when one encounters a non-Noetherian ring, because they're so ubiquitous.

Theorem 2.16.8 (Hilbert's Basis Theorem)**.** *If R is Noetherian, then $R[x]$ is Noetherian.*

We'll prove this next time.

Corollary 2.16.9. *If R is Noetherian, then $R[x_1, \dots, x_n]$ is Noetherian.*

Of course, this follows from repeatedly applying Hilbert's Basis Theorem. This was a controversial theorem at that time, because the proof was very nonconstructive. Apparently, this is false if we replace "Noetherian" with PID and other good adjectives.

Lemma 2.16.10. *If R is Noetherian and I is an ideal, then R/I is Noetherian.*

Proof. Recall that there is an inclusion preserving bijection:

$$\left\{\text{ideals of } R \text{ containing } I\} \leftrightarrow \left\{\text{ideals of } R/I\right\}\right.$$
$$J \mapsto J/I$$

Now the Lemma is clear, because if R satisfies ACC, then R/I now satisfies ACC. □

Remark 2.16.11. Let R be a Noetherian ring. Any finitely generated R-algebra is isomorphic to $R[x_1, \dots, x_n]/I$, which is Noetherian. It's also useful to note that $I = \langle f_1, \dots, f_r \rangle$ is itself finitely generated.

We'll talk about Noetherian rings a lot throughout the second half of the course.

2.17 Oct 3, 2018

We're going to prove the Hilbert Basis Theorem.

Theorem 2.17.1 (Hilbert's Basis Theorem)**.** *If R is Noetherian, then $R[x]$ is Noetherian.*

Proof. Take any ideal $I \subseteq R[x]$. Suppose that I is not finitely generated. We have $I \neq \{0\}$. Choose a nonzero $f_0 \in I$ of minimal degree. We inductively define $f_1, f_2, f_3, \dots \in I$ with $f_n \in I - \langle f_1, \dots, f_{n-1}\rangle$; this set is nonempty since I is not finitely generated. In particular, pick an f_n of minimal degree in $I - \langle f_1, \dots, f_{n-1}\rangle$.

Define $d_n = \deg(f_n)$. Note that $d_0 \leq d_1 \leq d_2 \leq \dots$. Also define a_n to be the leading coefficient of f_n, that is,

$$f_n = a_n x^{d_n} + \dots$$

so that each $a_i \in R - \{0\}$. Consider the ascending chain of ideals of R given by

$$\langle a_0 \rangle \subseteq \langle a_0, a_1 \rangle \subseteq \langle a_0, a_1, a_2 \rangle \subseteq \dots$$

and observe that this chain eventually stabilizes. This says that for some $N \geq 1$, we have

$$\langle a_0, \dots, a_n \rangle = \langle a_0, \dots, a_N \rangle$$

for all $n \geq N$.

Now take any $n > N$, and observe that $a_n \in \langle a_0, \dots, a_N \rangle$. Thus

$$a_n = r_0 a_0 + \dots + r_N a_N$$

with $r_i \in R$. We can define

$$\begin{aligned} g &:= f_n - \left(r_0 x^{d_n - d_0} f_0 + \dots + r_N x^{d_n - d_N} f_N \right) \\ &= \Big(\underbrace{a_n - (r_0 a_0 + \dots + r_N a_N)}_{=0} \Big) x^{d_n} + \text{lower order terms.} \end{aligned}$$

We claim that $g \in I - \langle f_0, \dots, f_{n-1} \rangle$, even though the above computation says that $\deg g < d_n = \deg f_n$. To see that this is true, $g - f_n \in \langle f_0, \dots, f_{n-1} \rangle$ but $f_n \notin \langle f_0, \dots, f_{n-1} \rangle$, so $g \notin \langle f_0, \dots, f_{n-1} \rangle$ either.

This gives a contradiction to the assumption that I is not finitely generated. So $R[x]$ is Noetherian. □

Example 2.17.2. There are non Noetherian rings: rings of continuous (or holomorphic) functions, the ring $\mathbb{R}[x_1, x_2, \dots]$, and $\prod_{i=1}^{\infty} \mathbb{F}_2$.

Let R be an integral domain (a commutative ring with no zero divisors).

We say a divides b if $b = ac$ for some $c \in R$, or if equivalently $\langle b \rangle \subseteq \langle a \rangle$. This is denoted $a|b$.

We say a and b are associates if $a = ub$ for some $u \in R^\times$, or if equivalently $\langle b \rangle = \langle a \rangle$. This is an equivalence class, so sometimes this is denoted $a \sim b$ if there is no confusion.

We say $p \in R$ is irreducible if $p \neq 0$ and p is not a unit, and if $p = ab$, then a or b is a unit.

We say $p \in R$ is prime if $p \neq 0$ and p is not a unit, and if $p|ab$ then $p|a$ or $p|b$, or if equivalently $\langle p \rangle$ is a prime ideal of R.

Lemma 2.17.3. *If $p \in R$ is a prime, then it is irreducible.*

Of course, the point is that the converse does not hold in general.

Proof. If $p = ab$, then since p is prime $p|a$ or $p|b$. Without loss of generality, suppose $p|a$, so that $a = pc$. Then $p = (pc)b = pcb$; since R is an integral domain we have $1 = cb$ and so b is a unit. □

Proposition 2.17.4. *Let R be a Noetherian integral domain. Then for any $a \neq 0$ in R, we have*

$$a = up_1 \dots p_r$$

with $u \in R^\times$ and $p_i \in R$ irreducible.

Proof. Define the set

$$\Sigma := \{\langle x \rangle : x \in R, x \neq 0, x \text{ not a product of irreducibles}\}.$$

Suppose that $\Sigma \neq \emptyset$. Since R is Noetherian, there is a maximal $\langle x \rangle \in \Sigma$. So x cannot be factored into irreducibles, i.e., $x = ab$ with a, b not units where either a or b cannot be factored into irredicubles.

Without loss of generality, suppose a cannot be factored into irreducibles. Then

$$\langle x \rangle \subseteq \langle a \rangle \implies \langle x \rangle = \langle a \rangle$$

and so $a = xy$ with $y \in R$, but as before we now have $x = (xy)b = xyb$ and so $1 = yb$ and b is a unit. □

Remark 2.17.5. The ring $\mathbb{R}[x_1, x_2, \dots]$ is non-Noetherian but has fatorization into irreducibles.

We didn't need the full power of Noetherian rings; we just needed that principal ideal domains satisfy ACC – that weaker assumption is equivalent to the conclusion of the above lemma.

Definition 2.17.6. A Unique Factorization Domain (UFD) is an integral domain R such that

- every non-zero element $a \in R$ satisfies
$$a = up_1 \dots p_r$$
for some unit $u \in R^\times$ and irreducible $p_i \in R$
- such a factorization is unique up to factoring and associates, that is, if
$$a = u' q_1 \dots q_s$$
for U' and unit and q_i irreducible, we have $r = s$ and $\sigma \in S_r$ such that $p_i \sim q_{\sigma(i)}$.

Nonexamples of UFD include: $\mathbb{Z}[\sqrt{-5}]$ (classic example: $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$), $\mathbb{R}[\cos x, \sin x]$ (classic example: $\cos^2 x = (1 + \sin x)(1 - \sin x)$).

Even worse is $\mathcal{H}$ the ring of holomorphic functions $\mathbb{C} \to \mathbb{C}$ is such that elements don't even factor into irreducibles! The classic example is that $\sin(\pi z) = z(z-1)(z-2)\dots(z-n)g(z)$ for some holomorphic g; it's not hard to show that these are all irreducible.

2.18 Oct 5, 2018

Last time, we defined a UFD: an integral domain R such that every $a \in R - \{0\}$ has a factorization

$$a = up_1 \dots p_r$$

with $u \in R^\times$ and p_i irreducible, where the $p_1, \dots, p_r$ are unique up to reordering and scaling by units (associates).

Let $a = up_1^{e_1} \dots p_r^{e_r}$ and $b = u'p_1^{f_1} \dots p_r^{f_r}$ for irreducible p_i (not associates of each other) and $e_i \geq 0$ and $f_i \geq 0$. Then

Definition 2.18.1. A greatest common divisor of a and b is a common divisor that divides all other common divisors. In other words,

$$\gcd(a,b) = p_1^{\min(e_1,f_1)} \dots p_r^{\min(e_r,f_r)}.$$

Note that this is only defined up to a unit, or by the ideal $\langle \gcd(a,b) \rangle$.

Lemma 2.18.2. *Let R be a UFD. Take $p \in R$. Then p is prime if and only if p is irreducible*

Proof. The forward direction was done in Lemma 2.17.3. For the backwards direction, take p irreducible, and suppose $p|ab$ with $a, b \in R$ nonzero, that is,

$$p(u''p_1'' \dots p_t'') = pc = ab = (up_1 \dots p_r)(p_1' \dots p_s')$$

where $u, u', u'' \in R^\times$ and p_i, p_i', p'' irreducible. Then by uniqueness of factorizations both sides are the same up to reordering and units, so p is an associate of p_i or p_i' for some i. In the first case $p|a$ and in the second $p|b$. □

Lemma 2.18.3. *Let R be an integral domain. Suppose all $a \neq 0$ in R can be factored into irreducibles. Then, R is a UFD if and only if all irreducibles of R are prime.*

Proof. The forward direction is the previous lemma. For the backwards direction, take two different factorizations

$$up_1 \dots p_r = q_1 \dots q_s$$

for p_i, q_j irreducible in $R^\times$. Look at p_1: we have $p_1 | q_1 \dots q_s$, and since p_1 is now prime (by assumption), we have $p_1 | q_j$ for some j, and hence p_1 and q_j are associates. So reorder and scale by units to get $p_1 = q_1$. Because we are in an integral domain we can cancel, that is,

$$u'p_2 \dots p_r = q_2 \dots q_s$$

for possibly a different u'. So we can do [lazy man's] induction: keep repeating so that $u = q_{s-r} \dots q_s$ (we have $s \geq r$ because for each p_i there must be at least one q_i on the right side). Since

$$1 = u^{-1} q_{s-r} \dots q_s$$

we have $s = r$ and $p_i = q_i$ for all i. □

Definition 2.18.4. An integral domain is a principal ideal domain (abbreviated PID) if it is a domain and if all ideals of R are principal.

Standard examples are $\mathbb{Z}, F[x], F$ for F a field. Nonexamples include $F[x,y]$ and the ideal $\langle x, y \rangle$, and $\mathbb{Z}[x]$ and the ideal $\langle 5, x \rangle$. But these are still UFDs (we'll prove this next time: if R is a UFD then so is $R[x]$).

Proposition 2.18.5. *All PIDs are UFDs.*

Proof. Let R be a PID. Any $a \neq 0$ has a factorization into irreducibles (since R is Noetherian!). Take any irreducible $p \in R$; we need to show it is prime.

Observe that $\langle p \rangle \subsetneq R$ since p is not a unit. It follows that there is a maximal ideal $\mathfrak{m} \supseteq \langle p \rangle$ (and we do not need Zorn here, because R is Noetherian). Then $\mathfrak{m} = \langle \pi \rangle$ because R is a PID. So $\langle p \rangle \subseteq \langle \pi \rangle$ and $\pi | p$. Note that π is not a unit, and so $p = u\pi$ for some $u \in R^\times$ (because p is irreducible). It follows that $\langle p \rangle = \langle \pi \rangle = \mathfrak{m}$, so $\langle p \rangle$ is a maximal ideal and hence a prime ideal. So p is now prime. □

This proof also gives the corollary

Corollary 2.18.6. *All nonzero prime ideals of a PID are maximal.*

Definition 2.18.7. A Euclidean domain is an integral domain R such that there is a function $N\colon R-\{0\} \to \mathbb{Z}$ such that $N(a) \geq 0$ for $a \neq 0 \in R$ and for any $a, b \in R$, with $b \neq 0$, we have $a = qb + r$ with $q, r \in R$ such that $r = 0$ or $N(r) < N(b)$.

Secretly N above stands for norm. Examples of Euclidean domains include $\mathbb{Z}$ with $N(b) = |b|$, and $F[x]$ with $N(f) = \deg f$. More nontrivial is

Example 2.18.8. Let $R = \mathbb{Z}[i] \subseteq \mathbb{C}$. We have $N(a + bi) = |a + bi|^2 = a^2 + b^2$. To see that we can divide, take any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Note that $\alpha/\beta = x + yi$ is not necessarily in $\mathbb{Z}[i]$; we can only conclude $x, y \in \mathbb{R}$. But we can take $a, b \in \mathbb{Z}$ such that $|x - a| \leq 1/2$ and $|y - b| \leq 1/2$; define $q := a + bi \in \mathbb{Z}[i]$, and observe that

$$\left|\frac{\alpha}{\beta} - q\right| \leq \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2}$$

so that

$$|\underbrace{\alpha - q\beta}_{:=r}|^2 \leq \frac{1}{2}|\beta|^2$$

so that $\alpha = q\beta + r$, with $N(r) < N(\beta)$.

As an exercise, what goes wrong with $R = \mathbb{Z}[\sqrt{-5}]$?

Proposition 2.18.9. *A Euclidean domain R is a PID.*

Proof. Let I be any ideal of R; we wish to show it's principal. We can assume $I \neq \langle 0 \rangle$. Take any $b \in I - \{0\}$ with $N(b)$ minimal (recall that $N(\cdot)$ is an integer, so we can actually take this minimum). Note that $\langle b \rangle \in I$; we claim that the other inclusion is true. Indeed, take any $a \in I$ so that $a = qb + r$ with $q, r \in R$ and $r = 0$ or $N(r) < N(b)$. But we have $r = a - qb \in I$ so $r = 0$ (otherwise $N(r) < N(b)$, contrary to assumption on b). So $a = qb \in \langle b \rangle$ so $I = \langle b \rangle$. □

Remark 2.18.10. Euclidean domains have a nice Euclidean algorithm, that is, if $a = qb + r$ you can prove $\gcd(a, b) = \gcd(b, r)$. So these are important computationally. They're also useful for proving certain rings are PIDs.

2.19 Oct 10, 2018

Last week, we considered several classes of rings. In particular, we have the chain of inclusions

$$\text{Integral domains} \supsetneq \text{UFDs} \supsetneq \text{PIDs} \supsetneq \text{Euclidean Domains} \supsetneq \text{Fields}.$$

Fix an integral domain R. Take $a, b \in R$, not both 0.

- If R is a UFD, then there is a $\gcd(a, b) \in R$, defined up to a unit (or equivalently defined up to the ideal $\langle \gcd(a, b) \rangle$).
- If R is a PID, then this ideal $\langle \gcd(a, b) \rangle$ is just the (principal) ideal $\langle a, b \rangle$. Thus there are $x, y \in R$ such that $ax + by = \gcd(a, b)$.
- If R is Euclidean, with norm map $N \colon R - \{0\} \to \mathbb{Z}_{\geq 0}$, then if $b \in R - \{0\}$, for $a \in R$ we have $a = qb + r$ with $q, r \in R$ and $r = 0$ or $N(r) < N(b)$. Then any d divides both a and b if and only if it divides both b and r. So $\langle \gcd(b, r) \rangle = \langle \gcd(a, b) \rangle$.

Let's do an example of the Euclidean algorithm, which says that we should use $a = qb + r$ over and over until we get 0 as the remainder. Let $R = \mathbb{Z}$ with $N(b) = |b|$; say that $a = 46391, b = 4301$. Then

$$\begin{aligned}
& && \gcd(46391, 4301) \\
46391 &= 10 \cdot 4301 + 3381 && = \gcd(4301, 3381) \\
3381 &= 3 \cdot 920 + 621 && = \gcd(3381, 920) \\
920 &= 1 \cdot 621 + 299 && = \gcd(621, 299) \\
621 &= 2 \cdot 299 + 23 && = \gcd(299, 23) \\
299 &= 13 \cdot 23 + 0 && = \gcd(23, 0) \\
& && = 23
\end{aligned}$$

Today we'll focus on the Gaussian integers $R = \mathbb{Z}[i]$ and do some computations with it. We showed that it was a Euclidean domain with $N(a+bi) = a^2+b^2$; this was Example 2.18.8. Observe that $N(\alpha\beta) = N(\alpha)N(\beta)$ respects multiplication.

Lemma 2.19.1. *We have $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ with $(\pm 1)^{-1} = \pm 1$ and $(\pm i)^{-1} = \mp i$. Furthermore, each prime π of $\mathbb{Z}[i]$ divides a unique prime $p \in \mathbb{Z}$, with $N(\pi) = p$ or $N(\pi) = p^2$.*

Proof. Let $\alpha \in \mathbb{Z}[i]^\times$, so that there is $\beta \in \mathbb{Z}[i]$ with $\alpha\beta = 1$. Thus

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$$

so $N(\alpha) = 1$. Now $\alpha = a + bi$ where $a^2 + b^2 = 1$ and a, b are integers. So $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$, and $\alpha = \pm 1$ or $\alpha = \pm i$.

For the second part, let $N(\pi) = p_1 \dots p_r$. Then since $\pi\bar{\pi} = N(\pi)$, then since π is prime we have π divides some $p_i =: p$. We can factor p into primes in $\mathbb{Z}[i]$, say $p = \pi\pi_2 \dots \pi_s$, and hence

$$p^2 = N(p) = N(\pi)N(\pi_2) \dots N(\pi_s)$$

so that $N(\pi) = p$ or $N(\pi) = p^2$. □

In fact, this proof says that if $N(\pi) = p^2$ then $\pi = p$ up to a unit, and if $N(\pi) = p$ then $p = \pi\bar{\pi}$. In other words, we saw that any prime $\pi \in \mathbb{Z}[i]$ divides a unique p. When we factor p in $\mathbb{Z}[i]$, we either have p prime in $\mathbb{Z}[i]$ or $p = \pi\bar{\pi}$ for primes $\pi, \bar{\pi}$ conjugate to each other, both of norm p. We want to understand which case happens.

We should deal with the case $p = 2$ separately: we have $2 = (1 + i)(1 - i) = -i(1 + i)^2$, and so up to units, $1 + i$ is the unique prime dividing 2.

Now consider p odd. We have isomorphisms

$$\mathbb{Z}[i]/\langle p\rangle \xleftarrow{\sim} \mathbb{Z}[x]/\langle x^2+1, p\rangle \xrightarrow{\sim} \mathbb{F}_p[x]/\langle x^2+1\rangle$$

Notice that $x^2+1 \in \mathbb{F}_p[x]$ is separable since $p \neq 2$. If $x^2+1 \in \mathbb{F}_p[x]$ is irreducible, then $\mathbb{F}_p[x]/\langle x^2+1\rangle$ is a field, which means that $\mathbb{Z}[i]/\langle p\rangle$ is a field, and hence p is prime in $\mathbb{Z}[i]$. On the other hand, if $x^2+1 \in \mathbb{F}_p[x]$ factors, say $x^2+1 = (x+\alpha)(x-\alpha)$, then

$$\mathbb{F}_p[x]/\langle x^2+1\rangle \xrightarrow{\sim}_{\text{CRT}} \mathbb{F}_p[x]/\langle x+\alpha\rangle \times \mathbb{F}_p[x]/\langle x-\alpha\rangle \cong \mathbb{F}_p \times \mathbb{F}_p.$$

This is not an integral domain, so p is not prime in $\mathbb{Z}[i]$ and $p = \pi\overline{\pi}$.

It remains to answer when -1 is a square in $\mathbb{F}_p^\times$.

Proposition 2.19.2. *The group $\mathbb{F}_p^\times$ is cyclic. Moreover, any finite subgroup G of $F^\times$, with F a field, is cyclic.*

Proof. The second part implies the first part, so we'll prove that. We have that G is finite and cyclic, so it is isomorphic to the direct product of its p-Sylow subgroups [we technically aren't allowed to use the structure theorem for finite abelian groups yet]. So without loss of generality assume G is a p-group, and suppose that G is not cyclic. Since $|G| = p^e$, we have $g^{p^{e-1}} = 1$ for all $g \in G$ (otherwise we'd have a generator). So $x^{p^{e-1}} - 1$ has at least $|G| = p^e$ roots in F. However, $\deg(x^{p^{e-1}} - 1) < p^e$, which is a contradiction. □

So when p is odd, we have -1 a square in $\mathbb{F}_p^\times$, that is, $x^2 = -1$ for some $x \in \mathbb{F}_p^\times$, if and only if we have an element of order 4 in $\mathbb{F}_p^\times$, which means that $p - 1 = |\mathbb{F}_p^\times|$ is divisible by 4.

So to summarize, if $p = 2$, then $1+i$ is the unique prime dividing 2. If $p \equiv 3 \pmod 4$, then p is prime in $\mathbb{Z}[i]$ and it is the unique prime dividing itself. If $p \equiv 1 \pmod 4$ then $p = \pi\overline{\pi}$, where if we write p as a sum of two squares $p = a^2 + b^2$ then $\pi = a + bi$. Hence $a+bi, a-bi$ are the primes that divide p.

Theorem 2.19.3 (Fermat)**.** *Let p be an odd prime. Then $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$.*

Proof. We just did the backwards direction, which is the hard one. To get the forward direction, notice that $x^2 \equiv 0, 1 \pmod 4$ for every x, and so $p \equiv 0, 1, 2 \pmod 4$ but p is odd. □

2.20 Oct 12, 2018

We'll begin with an example:

Example 2.20.1. Find all solutions of $y^2 = x^3 - 1$ with $x, y \in \mathbb{Z}$.

Proof. We fix a solution $(x, y) \in \mathbb{Z}^2$. Notice that

$$x^3 = y^2 + 1 = (y + i)(y - i) \quad \text{ in } \mathbb{Z}[i].$$

We claim that $y + i$ and $y - i$ are relatively prime: suppose not, and take a prime $\pi \in \mathbb{Z}[i]$ dividing both $y + i$ and $y - i$. So π divides their difference, and up to a unit, $\pi | 2$ so $\pi = 1 + i$ (we characterized the primes dividing 2 last class). Also, π divides $x^3 = (y + i)(y - i)$, but $2 = N(\pi)|N(x^3) = x^6$ so x is even. But then $y^2 = x^3 - 1 \equiv 7 \pmod 8$, a contradiction. So $y + i$ and $y - i$ are relatively prime.

So $x^3 = (y + i)(y - i)$ for some relatively prime $y + i$ and $y - i$. It follows that $y + i$ and $y - i$ are themselves cubes: take π a prime dividing $y + i$, and let e be such that $\pi^e | y + i$ and $\pi^{e+1} \nmid y + i$. It follows that $\pi^e | x^3$ and $\pi^{e+1} \nmid x^3$, and so e must be divisible by 3. So

$$y + i = u\pi_1^{3e_1} \dots \pi_r^{3e_r}$$

where u is a unit and π_i are nonassociate primes. Then

$$y + i = (a + ib)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i$$

with $a, b \in \mathbb{Z}$. So we have integers $a, b \in \mathbb{Z}$ satisfying

$$\begin{aligned} y &= a^3 - 3ab^2 \\ 1 &= 3ab^2 - b^3 \end{aligned}$$

The second equation says $b = \pm 1$. When $b = 1$ then $3a^2 - 1 = 1$, which is impossible, and when $b = -1$ then $3a^2 + 1 = 1$, which has the unique solution $a = 0$. Then the first equation says $y = 0$ and hence $x = 1$.

The only solution (x, y) is $(1, 0)$. □

Last time, we showed that if p is an odd time, then p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$. So take such a $p \equiv 1 \pmod 4$, and define

$$N := \#\{(a, b) \in \mathbb{Z}^2 : p = a^2 + b^2\}.$$

What is N? We have at least 8 solutions: $(\pm a, \pm b)$ and $(\pm b, \pm a)$. We claim that these are precisely all of the solutions: note that

$$N = \#\{\pi \in \mathbb{Z}[i] : N(\pi) = p\}$$

but then $p = \pi\bar{\pi}$ is the prime factorization of p, so the primes that divide p are $u\pi, u\bar{\pi}$ with $u \in \mathbb{Z}[i]^\times$.

Consider $n = 2^{32} + 1 = 4294967297$. Observe that $n = (2^{16})^2 + 1^2 = 62264^2 + 20449^2$ is a sum of two squares in at least two ways. Hence n is not prime!

We can find integer factors of n in the following way: write

$$(2^{16} + i)(2^{16} - i) = n = (62264 + 20449i)(62264 - 20449i).$$

We can compute $\gcd(2^{16} + i, 62264 - 20449i)$ via the Euclidean Algorithm (steps are suppressed, the point is that it's doable). The gcd happens to be $-4 - 25i$. So in particular

$$N(-4 - 25i)|N(2^{16} + 1)$$

and since $N(-4 - 25i) = 641$ and $N(2^{16} + 1) = n$, we see that $641|n$.

And more specifically $n = 641 \cdot 6700417$ (this factorization was originally due to Euler).

Let R be an integral domain. We defined $F \supseteq R$ the field of fractions of R.

Definition 2.20.2. We say that R is integrally closed if all $\alpha \in F$ that is a root of a monic polynomial in $R[x]$ is actually in R.

Proposition 2.20.3. *A UFD is integrally closed.*

For example, $\mathbb{Z}$ is integrally closed, since $\mathbb{Z}$ is a UFD. We can conclude that $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ (if not it has a root $\alpha \in \mathbb{Q}$, but by the proposition we have $\alpha \in \mathbb{Z}$, and obviously there is no $\alpha \in \mathbb{Z}$ so that $\alpha^3 = 2$). Let's prove the above proposition:

Proof. Take

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$$

such that $f(\alpha) = 0$ with $\alpha \in F$. Then $\alpha = \frac{c}{d}$ with $c, d \in R, d \neq 0$. Since R is a UFD, we can assume that c and d are relatively prime (we can "reduce to lowest terms"). Then

$$0 = d^n f(\alpha) = c^n + a_{n-1}dc^{n-1} + \cdots + a_1 d^{n-1} c + a_0 d^n$$

which says that

$$-c^n = d(a_{n-1}c^{n-1} + \cdots + a_1 d^{n-2} c + a_0 d^{n-1})$$

and since $\gcd(c, d) = 1$ we have $d \in R^\times$, and now $\alpha = cd^{-1} \in R$. □

Example 2.20.4. Fix $d \in \mathbb{Z}$ squarefree, $d \neq 1$ so that $d \equiv 1 \pmod 4$. Then $\mathbb{Z}[\sqrt{d}]$ is not a UFD. This is because we can consider the monic polynomial

$$x^2 - x + \frac{1-d}{4} = \left(x - \left(\frac{1+\sqrt{d}}{2}\right)\right)\left(x + \left(\frac{1-\sqrt{d}}{2}\right)\right)$$

with roots in the fraction field $(1 \pm \sqrt{d})/2 \notin \mathbb{Z}[\sqrt{d}]$.

For $d \neq 1$ squarefree, define

$$R_d := \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

The R_d are integrally closed; there is a formal process we'll get to later that gives us integral closures of rings.

Some facts:

- R_d is a UFD if and only if R_d is a PID
- For $d < 0$, we have R_d is a UFD if and only if

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$$

- (Conjecture by Gauss): There are infinitely many $d > 1$ such that R_d is a UFD. We expect about 76% of these to work, by some Cohen-Lenstra heuristics.

The second fact was conjectured by Gauss, and is a theorem due to Stark and Heegner.

2.21 Oct 15, 2018

Last time we defined, for squarefree $d \neq 1$, the ring

$$R_d := \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

and R_d need not be UFD, but it is a Dedekind domain, which is a domain in which every nonzero ideal factors uniquely into prime ideals. These R_d are actually the ring of integers of $\mathbb{Q}(\sqrt{d})$.

Example 2.21.1. Consider $R := R_{-5} = \mathbb{Z}[\sqrt{-5}]$; one can show that $R^\times = \{\pm 1\}$ (by looking at norm maps). We have failure of unique factorization in R, since

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

with every element irreducible in R. We consider the ideals

$$\begin{aligned} \mathfrak{p} &= \langle 2, 1+\sqrt{-5}\rangle \\ \mathfrak{q}_1 &= \langle 3, 1+\sqrt{-5}\rangle \\ \mathfrak{q}_2 &= \langle 3, 1-\sqrt{-5}\rangle. \end{aligned}$$

We claim that these are maximal ideals, for example,

$$R/\mathfrak{q}_1 \cong \mathbb{Z}[x]/\langle 3, x^2+5, 1+x\rangle \xrightarrow{\sim} \mathbb{Z}/\langle 3\rangle$$

where the isomorphism is $x \mapsto -1$.

Observe that

$$\mathfrak{p}^2 = \langle 4, 2(1+\sqrt{-5}), (1+\sqrt{-5})^2\rangle = \langle 4, 2+2\sqrt{-5}, 2\sqrt{-5}\rangle = \langle 4, 2, 2\sqrt{-5}\rangle = \langle 2\rangle.$$

So $\langle 2\rangle = \mathfrak{p}^2$, and similarly one can show that $\langle 3\rangle = \mathfrak{q}_1\mathfrak{q}_2$. One can also do $\mathfrak{p}\mathfrak{q}_1 = \langle 1+\sqrt{-5}\rangle$ and $\mathfrak{p}\mathfrak{q}_2 = \langle 1-\sqrt{-5}\rangle$. So

$$\mathfrak{p}^2 \cdot \mathfrak{q}_1\mathfrak{q}_2 = \langle 2\rangle\langle 3\rangle = \langle 6\rangle = \langle 1+\sqrt{-5}\rangle\langle 1-\sqrt{-5}\rangle = \mathfrak{p}\mathfrak{q}_1 \cdot \mathfrak{p}\mathfrak{q}_2.$$

Thus, although unique factorization fails in R, the nonzero ideal $\langle 6\rangle$ factors uniquely into a product of prime ideals.

Remark 2.21.2. PIDs are both UFDs and Dedekind domains, but not all UFDs are Dedekind domains (and as we saw earlier, not all Dedekind domains are UFDs).

Example 2.21.3. Let's factor $4x^3 + 11x - 6$ in $\mathbb{Q}[x]$. Because it's a cubic we just need to know if it has a root, say $\alpha = \frac{r}{s}$ with $r, s \in \mathbb{Z}$ and $\gcd(r,s) = 1$ and $s \geq 1$.

Thus $4r^3 + 11rs^2 - 6s^3 = 0$. In other words, $r(4r^2 + 11s^2) = 6s^3$ so r divides 6 (because r, s are coprime). So $r = \pm 1, \pm 2, \pm 3$. Similarly, $4r^3 = s(-11rs + 6s^2)$, so s divides 4, and $s = 1, 2, 4$ (we assumed $s \geq 1$, by symmetry).

So we can check all 18 possible α. It turns out that $\alpha = \frac{1}{2}$ is the only root. It follows that

$$4x^3 + 11x - 6 = 4\left(x - \frac{1}{2}\right)\left(x^2 + \frac{1}{2}x + 3\right).$$

In $\mathbb{Z}[x]$, this says $4x^3 + 11x - 6 = (2x-1)(2x^2 + x + 6)$.

Gauss' Lemma tells us how factorizations in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ compare. More generally, let R be a UFD and F be the field of fractions of R; we want to compare factorizations in $R[x]$ with those in R and $F[x]$.

The irreducible elements of degree 0 in $R[x]$ are just the irreducible elements of R. So you can't escape understanding factorization of R if you want to understand factorizations of $R[x]$.

Proposition 2.21.4 (Rational root theorem)**.** *Let R be a UFD. Fix $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, with $a_n \neq 0$. If $\alpha \in F$ is a root, take $\alpha = \frac{r}{s}$ with $r, s \in R$ relatively prime. Then $r | a_0$ and $s | a_n$.*

The proof was Example 2.21.3.

Definition 2.21.5. We say that a nonzero $f \in R[x]$ is primitive if its coefficients are relatively prime (in R). So the only elements of R that divide all coefficients are units.

Take any nonzero $f \in F[x]$. We claim that there is a value $c(f) \in F^\times$ such that $f = c(f) \cdot f_1$ with $f_1 \in R[x]$ primitive.

Proof. We can clear denominators, that is, pick d so that $df \in R[x]$, so without loss of generality $f \in R[x]$. Let g be a gcd of the coefficients of f. Now $f = g \cdot \frac{f}{g}$, and $\frac{f}{g} \in R[x]$ is primitive. □

We also have that $c(f) \in F^\times$ and f_1 are unique up to multiplication by a unit in R:

Proof. Say that $\alpha f_1 = \beta f_2$ with $\alpha, \beta \in F^\times$ and $f_i \in R[x]$ primitive. So $\alpha\beta^{-1} f_1 = f_2$, and if $\alpha\beta^{-1} = \frac{r}{s}$ with $r, s \in R$ relatively prime, we have $rf_1 = sf_2$, and the gcd of the coefficients is r and is s. So $r = su$ for $u \in R^\times$. Now $\alpha\beta^{-1} := u$ is a unit, so $f_2 = uf_1$. □

The element $c(f)$ is called the content of f. Note that if $f \in R[x]$ then $c(f) \in R$.

Lemma 2.21.6 (Gauss' lemma)**.** *Let R be a UFD, and F its fraction field. If $f, g \in F[x]$ are nonzero, then $c(fg) \approx c(f)c(g)$, that is, $c(fg)$ and $c(f)c(g)$ are equal up to a unit. In particular, if $f, g \in R[x]$ are primitive, then fg is also primitive.*

Of course, a polynomial is primitive if and only if its content is a unit.

Let's prove the special case (if $f, g \in R[x]$ are primitive, then so is fg). Suppose fg is not primitive, so there is a prime $\pi \in R$ dividing the coefficients of fg. Now consider

$$\bar{f}\bar{g} = 0 \in (R/\langle\pi\rangle)[x],$$

where $R/\langle\pi\rangle$ is an integral domain (since π is prime). It follows that $(R/\langle\pi\rangle)[x]$ is an integral domain, too. So either $\bar{f} = 0$ or $\bar{g} = 0$ in $(R/\langle\pi\rangle)[x]$. Then either f or g are not primitive (because π divides their coefficients).

We will prove the rest of the lemma next lecture.

2.22 Oct 17, 2018

Last time, we let R be a UFD, and $R \subseteq F$ be its fraction field. We say $f \in R[x]$ is primitive if its coefficients are relatively prime. For nonzero $f \in R[x]$, we have $f = c(f) \cdot f_1$ for some $c(f) \in F^\times$ (the content of f) and primitive $f_1 \in R[x]$. We have that $c(f)$ is unique up to multiplication by a unit $u \in R^\times$. We had the following lemma:

Lemma 2.22.1 (Gauss' Lemma)**.** *If $f, g \in R[x]$ are primitive, then fg is primitive.*

The proof wasn't so bad, we just took fg modulo a prime and got a contradiction. Here's another Gauss' Lemma.

Lemma 2.22.2 (Gauss' Lemma)**.** *If $f, g \in F[x]$ are nonzero, then $c(fg) = u \cdot c(f)c(g)$ for some $u \in R^\times$.*

Proof. We can write $f = c(f)f_1$ and $g = c(g)g_1$ with f_1, g_1 primitive; we now have

$$fg = c(f)c(g)f_1g_1$$

where f_1g_1 is primitive due to the other Gauss' Lemma. Because of uniqueness of c up to multiplication by a unit, we have $c(f)c(g) = c(fg)$ up to a unit. □

Recall that if $f \in R[x]$ is of degree 0, then f is irreducible in $R[x]$ if and only if f is irreducible in R. For example, in $\mathbb{Z}[x]$, the usual primes $p \in \mathbb{Z}$ are irreducible.

Proposition 2.22.3 (Gauss' Lemma?)**.** *Take $f \in R[x]$ of degree ≥ 1. Then f is irreducible in $R[x]$ if and only if f is primitive and f is irreducible in $F[x]$.*

Proof. The backwards direction is easier. Suppose that f is irreducible in $F[x]$ and primitive. Suppose that $f = gh$ for $g, h \in R[x]$ nonunits. Note that $\deg g = 0$ or $\deg h = 0$, otherwise this would be a factorization in $F[x]$. Say that $g \in R - \{0\}$. Now $g|f$ and f is primitive, so g is a unit of R.

To prove the forwards direction, we assume that f is irreducible. Clearly f is primitive. Say that $f = gh$ with $g, h \in F[x]$ of degree at least 1. Then $f = c(g)c(h)g_1h_1$, where $c(g)c(h) \in F^\times$ and $g_1, h_1 \in R[x]$ are primitive. But f is primitive, so $c(f) = 1$ up to a $u \in R^\times$, so in fact $c(g)c(h) \in R^\times$.

It follows that $f = ug_1h_1$ with $u \in R^\times$ and $g_1, h_1 \in R[x]$, but since f is irreducible in $R[x]$ means that either g_1 or h_1 is in $R[x]^\times = R^\times$, which means that g or h is in $F^\times$. This means that f is irreducible in $F[x]$. □

Lemma 2.22.4 (Gauss' Lemma)**.** *Take $f \in R[x]$ nonzero. Suppose $f = gh$ with $g, h \in F[x]$. Then there is a $c \in F^\times$ such that $f = (cg)(c^{-1}h)$ with $cg, c^{-1}h \in R[x]$.*

The proof is exactly the same as the proof above.

Theorem 2.22.5. *Let R be a UFD. Then $R[x]$ is a UFD.*

Hilbert's Basis Theorem is similar (replace UFD with Noetherian), but this is not true for PIDs.

Proof. Take a nonzero $f \in R[x]$. Then $f = df_1$ with f_1 primitive, and $d \in R$. Since R is a UFD we can factor d into irreducibles in R (and hence in $R[x]$). We also have

$$f_1 = p_1 \dots p_r$$

with $p_i \in F[x]$ irreducible, and there are $\tilde{p}_i = c_ip_i \in R[x]$ with $c_i \in F^\times$. We have

$$f_1 = \tilde{p}_1 \dots \tilde{p}_r.$$

Since f_1 is primitive we have $\tilde{p}_i$ are all primitive. Now $\tilde{p}_i$ are primitive and irreducible in $F[x]$, so by Gauss $\tilde{p}_i \in R[x]$ are irreducible.This gives existence of factorizations.

To get uniqueness, we let $f = u\pi_1 \dots \pi_r p_1 \dots p_s$ where $u \in R^\times$, and π_i are degree 0 irreducibles in $R[x]$, and p_i degree ≥ 1 irreducibles in $R[x]$. Since $c(f) \in R$ is, up to a unit, is exactly $\pi_1 \dots \pi_r$, the π_i are unique up to reordering and units since R is a UFD.

So assume $f = p_1 \dots p_s$. Now the p_i are unique up to reordering and units, since $p_i \in F[x]$ is in a PID (and hence a UFD). But also $c(p_i) = 1$ so p_i is unique in $R[x]$. □

Theorem 2.22.6 (Eisenstein's Criterion)**.** *Let R be a UFD, and let $p \in R$ be a prime. Consider*

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$$

with the condition that $p | a_0, a_1, \dots, a_{n-1}$, and $p \nmid a_n$, and $p^2 \nmid a_0$. Then f is irreducible in $F[x]$. If f is primitive (for example, f is monic), it is also irreducible in $R[x]$.

Proof. Suppose $f = gh$ with $g, h \in R[x]$. Reduce this mod p, that is,

$$\bar{f} = \bar{g}\bar{h} \in (R/\langle p \rangle)[x]$$

with $\bar{f} = \bar{a}_n x^n$, and $a_n \neq 0$. Since $R/\langle p \rangle$ is a field, so $\bar{g} = c_1 x^d$ and $\bar{h} = c_2 x^{n-d}$ with $c_i \in (R/\langle p \rangle)^\times$ and $0 \leq d \leq n$. But if $0 < d < n$ then p divides constant terms of g and h, which is contradictory to assumption (that $p^2 \nmid a_0$). So $\deg g$ or $\deg h$ is 0. □

This is the classic example (and the one Eisenstein proved his criterion for):

Example 2.22.7. Let p be a prime, and $f = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$. Then $f(x) = \frac{x^p - 1}{x - 1}$, and

$$f(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{j=1}^{p} \binom{p}{j} x^{j-1}$$

and since $p | \binom{p}{j}$ for $j = 1, \dots, p-1$, $p^2 \nmid \binom{p}{1} = p$, and $p \nmid \binom{p}{p} = 1$, Eisenstein says that f is irreducible in $\mathbb{Z}[x]$ and hence it's irreducible in $\mathbb{Q}[x]$.

3 Modules

3.23 Oct 19, 2018

We saw that if R is a UFD, then $R[x]$ is a UFD. The primes of $R[x]$ are the primes of R and the primitive polynomials in $R[x]$ irreducible in $F[x]$, where F is the fraction field. The story is pretty much the same when one asks for $R[[x]]$; more things become units. In general power series are more complicated but algebraically $R[[x]]$ is easier to work with.

Today we're going to talk about modules; it'll be mostly definitions. Let R be a ring with 1.

Definition 3.23.1. A (left) module over R (or R-module) is a set with with operations

$$\begin{aligned} M \times M &\xrightarrow{+} M \\ (m, n) &\mapsto m + n \end{aligned}$$

and

$$\begin{aligned} R \times M &\xrightarrow{\cdot} M \\ (r, m) &\mapsto r \cdot m \end{aligned}$$

called "addition" and "scalar multiplication" such that the following hold:

- $(M, +)$ is an abelian group, with identity 0;
- $1 \cdot m = m$ for $m \in M$
- $r \cdot (s \cdot m) = (rs) \cdot m$ for $r, s \in R$ and $m \in M$
- $(r + s) \cdot m = r \cdot m + s \cdot m$ for $r, s \in R$ and $m \in M$
- $r \cdot (m + n) = rm + rn$ ro $r \in R$ and $m, n \in M$

Remark 3.23.2. There is a similar definition for right modules, where the multiplication is $M \times R \xrightarrow{\cdot} M$. But if R is commutative, and M is a right R-module, we can define a left module with $r \cdot m := m \cdot r$. Commutativity is required to keep the $r \cdot (s \cdot m) = (rs) \cdot m$ axiom.

Example 3.23.3. If R is a field, then R-modules are precisely vector spaces over F.

Example 3.23.4. Fix an integer $n \geq 0$ and define $R^n := \{(a_1, \ldots, a_n) \colon a_i \in R\}$ with the operations $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$ and $r \cdot (a_1, \ldots, a_n) = (ra_1, \ldots, ra_n)$. This is called the free R-module of rank n.

Example 3.23.5. Let $R = \mathbb{Z}$. Then $\mathbb{Z}$-modules are precisely abelian groups, with the multiplication

$$a \cdot m = \begin{cases} \underbrace{m + \cdots + m}_{a \text{ times}} & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ \underbrace{-m - \cdots - m}_{|a| \text{ times}} & \text{if } a < 0 \end{cases}$$

Example 3.23.6. (Left) ideals $I \subseteq R$ are an R-module: they're closed under addition, and closed under multiplication by R. Similarly, quotients are R-modules with the usual addition and $r(a + I) = ra + I$

Example 3.23.7. Polynomial rings $R[x]$ with the usual addition and multiplication are also an R-module.

Recall that a homomorphism of R-modules is a map $f \colon M \to N$ such that $f(m + n) = f(m) + f(n)$ and $f(rm) = rf(m)$ for $m, n \in M$ and $r \in R$. We also say f is an isomorphism if it is also bijective. The inverse is automatically an isomorphism.

Example 3.23.8. If $f\colon M \to N$ is a homomorphism, then $f(M)$ is an R-module, and $\ker f = \{m \in M\colon f(m) = 0\}$ is also an R-module.

Definition 3.23.9. A submodule of M is a subset $N \subseteq M$ that is an R-module using the operations from the ambient module M.

Observe that if $N \subseteq M$, then N is a submodule of M if and only if $0 \in N$, $m + n \in N$ for all $m, n \in N$, and $rn \in N$ for all $r \in R$, $n \in N$. The other axioms follow in N because they are inherited from M.

Example 3.23.10. Submodules of R are precisely ideals.

Example 3.23.11. We can take quotients: Let M be a module and $N \subseteq M$ be a submodule. The quotient M/N is an abelian group with scalar multiplication defined by $r(m + N) = rm + N$ for $r \in R$ and $m \in M$. This turns M/N into an R-module. We have a natural projection $M \to M/N$ given by $m \mapsto m + N$; it is a homomorphism of R-modules.

There are the four isomorphism theorems as always.

Example 3.23.12. For a set $S \subseteq M$, we have the submodule generated by S:

$$R \cdot S := \left\{ \sum_{s \in S'} r_s \cdot s\colon S' \subseteq S \text{ finite}, r_s \in R \right\},$$

that is, we have finite linear combinations of elements in S. This is the smallest submodule containing S.

Definition 3.23.13. We say M is finitely generated if $M = R \cdot S$ for some finite $S \subseteq M$.

Definition 3.23.14. Let M be an R-module. We say M is Noetherian if any chain

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \dots$$

of submodules stabilizes, ie., $N_n = N_{n+1}$ for n large enough. This agrees with the previous notation, that is, if $M = R$ as an R-modules, then R is Noetherian in the usual sense if and only if it is Noetherian in this sense.

Proposition 3.23.15. *We say that M is Noetherian if and only if all submodules of M are finitely generated.*

The proof is the same as the proof of (the equivalence of) Definition 2.16.5.

Proposition 3.23.16. *Let M be an R-module, and N a submodule of M. Then M is Noetherian if and only if N and M/N are Noetherian.*

Proof. The forward direction is easy: if M is Noetherian then so is N because submodules of N are in particular submodules of M and are hence finitely generated. Also, a submodule of M/N is of the form L/N with $N \subseteq L \subseteq M$ (there's an isomorphism theorem being used here). Since M is Noetherian L is finitely generated as an R module, so L/N is also finitely generated. So M/N is Noetherian.

For the backward direction, we recall that M/N is finitely generated, say with generators $x_1, \dots, x_n \in M$, and N is finitely generated, say with generators $y_1, \dots, y_m \in N$. Take any $m \in M$. Then $m + N = \sum_{i=1}^n r_i(x_i + N)$ for some $r_i \in R$. Now

$$m - \sum_{i=1}^n r_i x_i \in N$$

so we have $n - \sum_{i=1}^n r_i x_i = \sum_{j=1}^m s_j y_j$ with $s_j \in R$. Now we win; M is generated by $x_1, \dots, x_n, y_1, \dots, y_m$. □

Proposition 3.23.17. *Let R be Noetherian. Then if M is an R-module, we have M is Noetherian if and only if M is finitely generated.*

As a special case, we get that R^n is Noetherian, by induction on n (the base case is our assumption on R).

If M is finitely generated, there is a surjective homomorphism $R^n \twoheadrightarrow M$, so M is a quotient of R^n and M is Noetherian. Of course, if M is Noetherian, then M is finitely generated.

3.24 Oct 22, 2018

Last time, for R a commutative ring, we saw that if R is Noetherian, then an R-module M is Noetherian if and only if M is finitely generated.

Today, we let R be a PID. We'll describe modules over a PID.

Let M be a finitely generated R-module, say with generators $m_1, \ldots, m_n \in M$. We have a unique homomorphism of R-modules $\varphi\colon R^n \twoheadrightarrow M$ mapping e_i (the "standard basis" of R^n) to m_i. It's clear what this map should be, since $\varphi(r_1e_1+\cdots+r_ne_n) = r_1m_1+\cdots+r_nm_n$. Also, φ is surjective since $m_1, \ldots, m_n$ generate M.

The first isomorphism theorem says $R^n/\ker\varphi \xrightarrow{\sim} M$. Notice that $\ker\varphi$ is finitely generated, since R^n is Noetherian. So there is another surjective homomorphism $\psi\colon R^m \twoheadrightarrow \ker\varphi$, so we get the short exact sequence

$$\begin{tikzcd} R^m \arrow[r, "\psi"] & R^n \arrow[r, "\varphi"] & M \arrow[r] & 0 \end{tikzcd}$$

Take any $1 \le j \le m$, and observe that

$$\psi(e_j) = \sum_{i=1}^{n} A_{i,j}e_i \qquad \text{for unique } A_{i,j} \in R.$$

If you view R^m and R^n as "columns", then ψ is given by left multiplication by a matrix $A \in M_{n,m}(R)$. So $M \cong R^n/\psi(R^m) = R^n/A(R^m)$.

Some remarks: Let $P \in \mathrm{GL}_n(R)$ and $Q \in \mathrm{GL}_m(R)$. Then because P, Q are isomorphisms

$$R^n/(PAQ)(R^m) = R^n/(PA(R^m)) = R^n/P(A(R^m)) = R^n/A(R^m)$$

given by $\bar{P}v \leftarrow\!\shortmid \bar{v}$.

So to understand modules M over a PID, we want to understand $R^n/A(R^m)$; an idea is to find P and Q so that A is "nice".

In linear algebra, for $R = F$ a field, and a matrix $A \in M_{m,n}(F)$, there are invertible $P \in \mathrm{GL}_m(F)$ and $Q \in \mathrm{GL}_n(F)$ such that

$$D = PAQ = \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

where D is not necessarily a square and there are r 1's, where r is the rank of A (the point is that we'll give a generalization of this result later, for PIDs). Then

$$R^m/D(R^n) \cong \underbrace{R \times \cdots \times R}_{r \text{ times}} \times 0 \times \cdots \times 0 \cong R^{m-r} = F^{m-r}$$

which says that finitely generated vector spaces are free, ie. have a finite basis.

The generalization is called Smith Normal Form: Let R be a PID, and take any matrix $A \in M_{m,n}(R)$. Then there are invertible $P \in \mathrm{GL}_m(R)$ and $Q \in \mathrm{GL}_n(R)$ such that

$$D = PAQ = \begin{bmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

with $a_1, \dots, a_r \in R$ nonzero and $a_1 | a_2, a_2 | a_3, \dots, a_{r-1} | a_r$. Moreover, r is unique and the a_i are unique up to multiplication by $u \in R^\times$.

Theorem 3.24.1 (Structure theorem for finitely generated modules over PIDs)**.** *Let R be a PID, and let M be a finitely generated R-module. Then there are $r, s \geq 0$ and nonzero $a_1, \dots, a_s \in R$ that are not units such that*

$$M \cong R/\langle a_1 \rangle \times \cdots \times R/\langle a_s \rangle \times R^r$$

and $a_1 | a_2, a_2 | a_3, \dots, a_{s-1} | a_s$. Moreover, r and s are unique, and the a_is are unique up to units.

Sometimes people write $a_1 | a_2, a_2 | a_3, \dots, a_{s-1} | a_s$ as "$a_1 | a_2 | \dots | a_s$". The a_i are called invariant factors and r the free rank.

Proof. We first prove existence assuming Smith Normal Form. We saw (with m and n switched) that $M \cong R^m / A(R^n)$ for some $A \in M_{m,n}(R)$, so $M \cong R^m / D(R^n)$ (with the isomorphism coming from Smith Normal Form), where as before

$$D = PAQ = \begin{bmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

with $a_i \in R - \{0\}$ and $a_1 | a_2 | \dots | a_r$. Then

$$R^m / D(R^n) \cong R^m / (a_1 R \times \cdots \times a_r R \times 0 \times \cdots \times 0) \cong R/\langle a_1 \rangle \times \cdots \times R/\langle a_r \rangle \times R \times \cdots \times R$$

where we remove the early a_is that are units (since $R/\langle a_i \rangle = 0$). □

We'll prove Smith Normal Form next time; the proof will be an algorithm, that is, one could actually compute the a_i.

Theorem 3.24.2 (Structure theorem for finitely generated abelian groups)**.** *Let M be a finitely generated abelian group. Then*

$$M \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z} \times \mathbb{Z}^r$$

for unique $r \geq 0$ and unique positive integers $n_1, \dots, n_s \geq 2$ satisfying $n_1 | n_2 | \dots | n_s$.

Observe that if M is well understood, one could compute r and n_i; every step of the proof is constructive.

If $a_i = u\pi_1^{e_1} \dots \pi_t^{e_t}$ with $u \in R^\times$ and $\pi_1, \dots, \pi_t \in R$ primes (not associates) and $e_i \geq 1$, then by CRT we have $R/\langle a_i \rangle \cong R/\langle \pi_1^{e_i} \rangle \times \cdots \times R/\langle \pi_r^{e_t} \rangle$. This gives another description of the modules over a PID.

Next time we'll give the proof of Smith Normal Form, and specialize to $R = F[x]$.

3.25 Oct 24, 2018

Last time, we talked about Smith Normal Form: Let R be a PID, and take a matrix $A \in M_{m,n}(R)$. Then there are invertible matrices $P \in \mathrm{GL}_m(R)$ and $Q \in \mathrm{GL}_n(R)$ such that

$$D = PAQ = \begin{bmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

with $a_i \in R$ nonzero satisfying $a_1|a_2|\dots|a_r$. Moreover, r is unique and a_i is unique up to multiplication by $u \in R^\times$. The matrix D is called the Smith Normal Form of A.

We'll prove the existence of the Smith Normal Form of A. We say $A, B \in M_{m,n}(R)$ are equivalent if $PAQ = B$ for some $P \in \mathrm{GL}_m(R)$ and $Q \in \mathrm{GL}_n(R)$. Of course, this is an equivalence relation on $M_{m,n}(R)$.

Proof. Fix $A \in M_{m,n}(R)$. Our goal is to find an equivalent matrix of the form

$$\begin{bmatrix} a_1 & 0 \\ 0 & B \end{bmatrix}$$

with $B \in M_{m-1,n-1}(R)$, where a_1 divides all entries of B. Doing this is sufficient; we can use induction on the size of the matrix. Notice that a_1 divides all entires equivalent to B, too.

We can assume $A \neq 0$ (otherwise, we are done). We can perform elementary row operations: we can swap rows, add a multiple of one row to another, and scale a row by $u \in R^\times$.

They are reversible by another elementary row operation. Also, each corresponds to left multiplication by a matrix $P \in \mathrm{GL}_m(R)$. We can also perform column operations, corresponding to right multiplication by a matrix $P \in GL_m(R)$. By swapping rows and columns, we can assume $A_{1,1} \neq 0$.

For $2 \leq i \leq n$, we can replace A by an equivalent matrix A' such that $A'_{i,1} = \gcd(A_{1,1}, A_{i,1})$. To see this, say that (without loss of generality, because we can swap rows) that $i = 2$; for $a = A_{1,1}, b = A_{2,1}$, and $g = \gcd(a, b)$, then if R is a PID we have $\langle a, b\rangle = \langle g\rangle$,that is, $ax + by = g$ for some $x, y \in R$.

In step 1, we split into cases. The good case is when $A_{1,1}|A_{i,1}$ for all $2 \leq i \leq m$, say with $A_{i,1} = q_i A_{1,1}$ with $\mathrm{row}_i := \mathrm{row}_i - q_i\mathrm{row}_1$. This turns the first column into the form

$$\begin{bmatrix} a & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{bmatrix}$$

and go to Step 2.

In the bad case, $A_{1,1} \nmid A_{i,1}$ for some $2 \leq i \leq n$. Then replace A by an equivalent matrix A' such that $A'_{1,1} = \gcd(A_{1,1}, A_{1,i-1})$ and restart Step 1 (we'll discuss why this must terminate later).

In step 2, we also split into cases. The good case is when $A_{1,1}|A_{1,j}$ for all $2 \leq j \leq n$, say with $A_{1,j} = q_j A_{1,1}$ with $\mathrm{col}_j := \mathrm{col}_j - q_j\mathrm{col}_1$. This turns A into the form

$$\begin{bmatrix} a & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{bmatrix}$$

and go to Step 3.

In the bad case, $A_{1,1} \nmid A_{1,j}$ for some j. Then replace A by an equivalent matrix A' such that $A'_{1,1} = \gcd(A_{1,1}, A_{1,j})$ and go to step 1.

In step 3, we also split into cases. The good case is when $A_{1,1}$ divides all entries of B. Then we'd be done.

If there is an $2 \leq i \leq m$ such that $A_{1,1}$ does not divide all elements in i-th row, we add the i-th row to the first row, and go to step 2.

To show this is a proof/algorithm, we need to know why it halts. Whenever we were in a bad case, we obtained an equivalent matrix A', such that $A'_{1,1}|A_{1,1}$ and $A_{1,1} \nmid A'_{1,1}$. Let $\alpha_1, \alpha_2, \ldots$ be the $A_{1,1}$ we get over the algorithm. Then

$$\langle \alpha_1 \rangle \subseteq \langle \alpha_2 \rangle \subseteq \ldots$$

and a bad case corresponds to $\langle \alpha_n \rangle \subsetneq \langle \alpha_{n+1} \rangle$. Eventually, we never hit a bad case, so it stops! □

Example 3.25.1. Let $G = \mathbb{Z}^3/\langle (3,3,6), (8,4,0), (0,12,12) \rangle$. Consider

$$A = \begin{bmatrix} 3 & 8 & 0 \\ 3 & 4 & 12 \\ 6 & 0 & 12 \end{bmatrix},$$

and observe that $G = \mathbb{Z}^3/A(\mathbb{Z}^3)$. We want to reduce this matrix. Set $r_2 := r_2 - r_1$ and $r_3 := r_3 - 2r_1$, so that

$$A' = \begin{bmatrix} 3 & 0 & 0 \\ 0 & -4 & 12 \\ 0 & -16 & 12 \end{bmatrix}$$

and then set $c_2 := c_2 - 3c_1$, and set $c_2 := -1c_2$ and swap c_1 and c_2, so that

$$A' = \begin{bmatrix} 1 & 3 & 0 \\ 4 & 0 & 12 \\ 16 & 0 & 12 \end{bmatrix}$$

and set $r_2 := r_2 - 4r_1$ and $r_3 := r_3 - 16r_1$, so that

$$A' = \begin{bmatrix} 1 & 3 & 0 \\ 0 & -12 & 12 \\ 0 & -48 & 12 \end{bmatrix}$$

and set $c_2 := c_2 - 3c_1$ and $r_3 := r_3 - 4r_2$, so that

$$A' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -12 & 12 \\ 0 & 0 & -36 \end{bmatrix}$$

and set $c_3 := c_3 + c_2$, $c_2 := -c_2$, and $c_3 := -c_3$, so that

$$A' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 36 \end{bmatrix}.$$

Thus, A is equivalent to A' as above; we have

$$G \cong \mathbb{Z}^3 / \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 36 \end{bmatrix} \mathbb{Z}^3 \cong (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times 12\mathbb{Z} \times 36\mathbb{Z}) \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}.$$

3.26 Oct 29, 2018

[Homeworks are due Monday for a few weeks, since class was cancelled Friday and Thanksgiving will happen.]

Last time, we talked about Smith Normal Form:

Let R be a PID, and take any $A \in M_{m,n}(R)$. Then there are $P \in \mathrm{GL}_m(R)$ and $Q \in \mathrm{GL}_n(R)$ so that

$$D = PAQ = \begin{bmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

with nonzero $a_1, \ldots, a_r \in R$ satisfying $a_1 | a_2 | \ldots | a_r$. Moreover, the a_i are unique up to units.

We proved the existence of P and Q.

Today we'll set $R = F[x]$, where F is a field. Let V be a finite dimensional vector space over F. Consider a linear operator $T\colon V \to V$. We can turn V into an $F[x]$-module in the following way: elements $c \in F$ act on V as usual, and $x \in F$ acts on V via T, that is, $xv := T(v)$.

The converse is true; if M is an $F[x]$ module then it is a (maybe not necessarily finite dimensional) vector space with a linear operator given by $T(v) := xv$.

Choose a basis $v_1, \ldots, v_n$ of V. We set

$$T(v_j) = \sum_{i=1}^{n} A_{i,j} \cdot v_i$$

with $A_{i,j} \in F$. This gives rise to $A \in M_n(F)$. We can now view F^n as an $F[x]$ module by letting x act as left multiplication by A, and $V \cong F[x]$.

Define $B := xI - A \in M_n(F[x])$. By homework 8, problem 7, we can say

$$V \cong F^n \cong F[x]^n / B(F[x]^n).$$

This is supposed to be a good thing; in the classification of finitely generated modules over a PID we took a finitely generated module and understood $F[x]^n / B(F[x]^n)$.

Consider the Smith Normal Form of B, so

$$B = P \begin{bmatrix} 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 1 & & & & & \\ & & & & a_1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & a_s & & \\ & & & & & & & 0 & \\ & & & & & & & & \ddots \end{bmatrix} Q$$

for $P, Q \in \mathrm{GL}_n(F[x])$ and $a_1, \dots, a_s \in F[x]$ monic of degree at least 1 and $a_1 | a_2 | \dots | a_s$. Moreover, $a_1, \dots, a_s$ are unique polynomials; they are the invariant factors of B or A.

Define the characteristic polynomial of A to be $c_A(x) = \det(xI - A) \in F[x]$, so that $c_A(x)$ is monic of degree n. Because $\det B \neq 0$, we in fact have

$$B = P \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ & & & & a_1 & & \\ & & & & & \ddots & \\ & & & & & & a_s \end{bmatrix} Q$$

that is, we have no zeros. Notice that

$$c_A(x) = \det B = \det P \cdot a_1 \dots a_s \cdot \det Q$$

and furthermore that $\det P, \det Q \in F^\times$ (since $P \cdot P^{-1} = I$, so $\det(P^{-1})$ is an inverse to $\det P$ in $F[x]^\times = F^\times$). Now

$$c_A(x) = (\det P \det Q) a_1 \dots a_s$$

for monic a_i and monic c_A. Since $\det P \det Q \in F$ we have $\det P \det Q = 1$. So $c_A(x) = a_1 \dots a_s$. This could be a determinant-free definition of characteristic polynomials!

Again, by homework 8, we see that (for D the Smith Normal Form of B)

$$\begin{aligned} V &\cong F[x]/B(F[x]^n) \\ &\cong F[x]^n / DF[x]^n \\ &\cong \frac{F[x] \times \dots \times F[x] \times F[x] \times \dots \times F[x]}{F[x] \times \dots \times F[x] \times \langle a_1 \rangle \times \dots \times \langle a_s \rangle} \\ &\cong F[x]/F[x] \times \dots \times F[x]/F[x] \times F[x]/\langle a_1 \rangle \times \dots \times F[x]/\langle a_s \rangle \\ &= F[x]/\langle a_1 \rangle \times \dots \times F[x]/\langle a_s \rangle \end{aligned}$$

As an aside, consider a monic polynomial

$$f = x^d + b_{d-1}x^{d-1} + \dots + b_1 x + b_0 \in F[x]$$

Then $V := F[x]/\langle f \rangle$ has a linear operator T given by multiplication by x: there is a basis $\{1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{d-1}\}$ and $T(1) = \bar{x}$, and $T(\bar{x}) = \bar{x}^2$, and so on; also, $T(\bar{x}^{d-1}) = \bar{x}^d = -b_0 1 - b_1 \bar{x} - \dots - b_{d-1}\bar{x}^{d-1}$.

With respect to this basis, T is given by the matrix

$$C_f := \begin{bmatrix} 0 & 0 & \dots & -b_0 \\ 1 & 0 & \dots & -b_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & -b_{d-1} \end{bmatrix}$$

This is called the companion matrix of f. We have that A is similar to

$$\begin{bmatrix} C_{a_1} & & & \\ & C_{a_2} & & \\ & & \ddots & \\ & & & C_{a_s} \end{bmatrix}.$$

This is painful to prove with classical linear algebra, but in terms of modules and PIDs this is just saying you can put a module structure on vector spaces.

In any case, we had $V \cong F[x]/\langle a_1\rangle \times \cdots \times F[x]/\langle a_s\rangle$. Fix $f \in F[x]$ so that $f(T)v = 0$ for all $v \in V$. This is equivalent to saying that $f(x)v = 0$ for all $v \in V$, and by the isomorphism $f(x)m = 0$ for all $m \in F[x]/\langle a_1\rangle \times \cdots \times F[x]/\langle a_s\rangle$, which happens if and only if $a_s|f$ (because $a_1|a_2|\dots|a_s$), that is, a_s is the minimal polynomial of T (classically, the minimal polynomial is a monic polynomial in $F[x]$ of minimal degree such that $a_s(T) = 0$).

Since $a_s|c_A$, we have $c_A(A) = 0$. This is classically called the Cayley Hamilton theorem.

Example 3.26.1. We fix

$$A = \begin{bmatrix} 13 & 24 & 50 \\ -6 & -11 & -25 \\ 0 & 0 & 1 \end{bmatrix} \in M_n(\mathbb{Q})$$

so that

$$B = xI - A = \begin{bmatrix} x-13 & -24 & -50 \\ 6 & x+11 & 25 \\ 0 & 0 & x-1 \end{bmatrix}$$

To get to Smith Normal Form we can reduce:

$$\begin{bmatrix} x-13 & -24 & -50 \\ 6 & x+11 & 25 \\ 0 & 0 & x-1 \end{bmatrix} \xrightarrow{r_1:=r_2, r_2:=r_1} \begin{bmatrix} 6 & x+11 & 25 \\ x-13 & -24 & -50 \\ 0 & 0 & x-1 \end{bmatrix}$$

$$\xrightarrow{r_2:=6r_2} \begin{bmatrix} 6 & x+11 & 25 \\ 6(x-13) & -144 & -300 \\ 0 & 0 & x-1 \end{bmatrix}$$

$$\xrightarrow{r_2:=r_2-(x-13)r_1} \begin{bmatrix} 6 & x+11 & 25 \\ 0 & -x^2+2x-1 & -25x+25 \\ 0 & 0 & x-1 \end{bmatrix}$$

$$\xrightarrow{\text{column operations}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -x^2+2x-1 & -25x+25 \\ 0 & 0 & x-1 \end{bmatrix}$$

$$\xrightarrow{\text{simplify}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & x-1 & 0 \\ 0 & 25(x-1) & -(x-1)^2 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & (x-1)^2 \end{bmatrix}$$

And so A is similar to

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{bmatrix}$$

3.27 Oct 31, 2018

[I was out of town for this lecture. Cosmo Viola and Yichi Zhang took notes that I borrowed from.]

Recall

Theorem 3.27.1 (Theorem A: Structure Theorem for finitely generated modules over a PID)**.** *Let M be a finitely generated module over a PID R. Then*

$$M \cong R^r \times R/\langle a_1 \rangle \times \cdots \times R/\langle a_s \rangle$$

with $a_i \in R$ nonzero and nonunits such that $a_1 | a_2 | \dots | a_s$. Moreover, $r, s \geq 0$ are unique and $a_1, \dots, a_s$, called the invariant factors of M, are unique up to units.

We will talk about

Theorem 3.27.2 (Theorem B)**.** *Let M be a finitely generated module over a PID R. Then*

$$M \cong R^r \times R/\langle p_1^{e_1} \rangle \times \cdots \times R/\langle p_t^{e_t} \rangle$$

with $p_i \in R$ irreducible and $e_i \geq 1$. Moreover, r and t are unique, and $p_1^{e_1}, \dots, p_t^{e_t}$, called the elementary divisors of M, are unique up to scaling by units and reordering.

Proof. The existence just follows from Theorem A (Theorem 3.27.1) and the Chinese Remainder Theorem: if $a = up_1^{e_1} \dots p_t^{e_t}$ for irreducible and mutually nonassociate then

$$R/\langle a \rangle \cong R/\langle p_1^{e_1} \rangle \times \cdots \times R/\langle p_t^{e_t} \rangle$$

as an isomorphism of rings and R-modules.

To prove uniqueness, we fix an irreducible $p \in R$ dividing a. Without loss of generality, assume $p = p_i$ for some i, where p and p_i are associates. Notice that if $j \geq 1$ then we have an isomorphism

$$\begin{aligned} p^{j-1}R/p^jR &\leftarrow R/pR \\ p^{j-1}x &\leftarrow\!\shortmid x. \end{aligned}$$

Define the field $\mathbb{F} := R/\langle p \rangle$. Notice that

$$p^j \cdot R/\langle p^e \rangle = \begin{cases} \langle p^j \rangle / \langle p^e \rangle & \text{if } j \leq e \\ 0 & \text{if } j \geq e \end{cases}$$

and

$$\frac{p^{j-1} \cdot R/\langle p^e \rangle}{p^j \cdot R/\langle p^e \rangle} \cong \begin{cases} \langle p^{j-1} \rangle / \langle p^j \rangle \cong R/\langle p \rangle = \mathbb{F} & \text{if } j \leq e \\ 0 & \text{if } j \geq e \end{cases}$$

Thus, if $q \in R$ is irreducible and not an associate of p, then there are $a, b \in R$ so that $ap + bq^e = 1$, that is, $\bar{a}\bar{p} = 1$ in $R/\langle q^e \rangle$; this means that $\bar{p}$ has an inverse in $R/\langle q^e \rangle$, and hence

$$p^r R/\langle q^e \rangle \cong R/\langle q^e \rangle.$$

Now we understand

$$\frac{p^{j-1}M}{p^jM} \cong \frac{p^{j-1}(R^r \times R/\langle p_1^{e_1} \rangle \times \cdots \times R/\langle p_t^{e_t} \rangle)}{p^j(R^r \times R/\langle p_1^{e_1} \rangle \times \cdots \times R/\langle p_t^{e_t} \rangle)} \cong \mathbb{F}^r \times \prod_{\substack{1 \leq i \leq t \\ p_i = p \\ j \leq e_i}} \mathbb{F}$$

and in particular the quanitity

$$\dim_{\mathbb{F}} p^{j-1}M/p^jM = r + \#\{i \colon 1 \leq i \leq t, p_i = t, \text{ and } j \leq e_i\}$$

depends only on m, e, and j. By letting j grow arbitrarily large, we find that r depends only on M.

Furthermore, we see that $\#\{i \colon 1 \leq i \leq t, p_i = t, \text{ and } j \leq e_i\}$ depends only on M, p and j. From this, for all j we can recover the sequence of $p_i^{e_i}$ with $p = p_i$ (up to units), and by considering all p we acquire uniqueness. □

Remark 3.27.3. We can use uniqueness in Theorem B (Theorem 3.27.2) to prove uniqueness in Theorem A(Theorem 3.27.1), and uniqueness of the Smith Normal Form.

One application of Theorem B (Theorem 3.27.2) is the following:

Corollary 3.27.4 (Jordan Canonical Form)**.** *Fix a matrix $A \in M_n(F)$, where F is a field. Assume that the characteristic polynomial $c_A(x) = \det(xI - A) \in F[x]$ splits (ie., factors into degree 1 terms).*

For $\lambda \in F$ and $e \geq 1$, we have a Jordan block

$$J_{\lambda,e} = \begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}.$$

Then the matrix A is similar to

$$\begin{bmatrix} J_{\lambda_1,e_1} & & \\ & \ddots & \\ & & J_{\lambda_r,e_r} \end{bmatrix}$$

called the Jordan canonical form of A, with $\lambda_i \in F$ and $e_i \geq 1$. The pairs $(\lambda_1, e_1), \ldots, (\lambda_r, e_r)$ are unique up to reordering.

Let's prove this!

Proof. Let $V := F^n$ be the $F[x]$ module for which multiplication by x is left multiplication by A. We have

$$V \cong F[x]/\langle a_1 \rangle \times \cdots \times F[x]/\langle a_s \rangle$$

for $a_1 | \ldots | a_s$ and a_i monic of degree ≥ 1. Last time we showed that $c_A = a_1 \ldots a_s$, so $a_i \in F[x]$ splits. As before, the Chinese Remainder Theorem says that

$$V \cong F[x]/\langle (x - \lambda_1)^{e_1} \rangle \times \cdots \times F[x]/\langle (x - \lambda_r)^{e_r} \rangle$$

with $c_A = (x - \lambda_1)^{e_1} \ldots (x - \lambda_r)^{e_r}$. Now consider $W := F[x]/\langle (x - \lambda)^e \rangle$ for $\lambda \in F$ and $e \geq 1$. We have a linear map $T \colon W \to W$ given by multiplication by x. Then a basis of W over F is given by $\{\overline{(x - \lambda)}^{e-1}, \ldots, \overline{(x - \lambda)}, \overline{1}\}$. We have

$$T(\overline{(x - \lambda)}^j) = x\overline{(x - \lambda)}^j = (x - \lambda)\overline{(x - \lambda)}^j + \lambda\overline{(x - \lambda)}^j,$$

so with respect to this basis the matrix T is given by

$$T = \begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix} =: J_{\lambda,e}$$

so there is a basis of V such that multiplication by A is given by

$$\begin{bmatrix} J_{\lambda_1,e_1} & & \\ & \ddots & \\ & & J_{\lambda_r,e_r} \end{bmatrix}.$$

□

3.28 Nov 2, 2018

Last time, we proved Jordan canonical form:

Take $A \in M_n(F)$ such that its characteristic polynomial is $c_A(x) = \det(xI - A) \in F[s]$ splits, that is, factors into degree 1 terms. Then A is similar to

$$\begin{bmatrix} J_{\lambda_1,e_1} & & \\ & \ddots & \\ & & J_{\lambda_r,e_r} \end{bmatrix}$$

with $\lambda_i \in F$ and $e_i \geq 1$. Moreover, $(\lambda_1, e_1), \dots, (\lambda_r, e_r)$ are unique up to reordering.

The idea is that $V := F^n$ can be given an $F[x]$-module structure with x acting as multiplication by A. Then as $F[x]$-modules, we have

$$V \cong F[x]/\langle a_1 \rangle \times \cdots \times F[x]/\langle a_s \rangle$$

with $a_i \in F[x]$ monic of degree at least 1, and $a_1 | \dots | a_s$. In this setting, we have $c_A = a_1 \dots a_s$ with a_s the minimal polynomial of A, which we sometimes denote m_A. This implies that c_A and $m_A = a_s$ have the same irreducible factors (because of the divisibility conditions $a_1 | \dots | a_s$). We proved Jordan Canonical Form by using Chinese Remainder Theorem.

Example 3.28.1. Consider $A \in \mathrm{GL}_n(\mathbb{C})$. Let's prove that $B^2 = A$ for some $B \in M_n(\mathbb{C})$. We'll prove this by reducing this to the case where A is a Jordan block, and in this case it's not so hard to prove this.

So let's say J is the Jordan Canonical Form of A, so that $A = PJP^{-1}$ where J is now invertible (since A is invertible). If $B^2 = J$ for some B, then $(PBP^{-1})^2 = PB^2P^{-1} = A$, so A is a square.

So without loss of generality, assume A is in Jordan canonical form, so

$$A = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_r \end{bmatrix}.$$

Notice that if $B_i^2 = J_i$, for some $B_i \in M_n(\mathbb{C})$ then

$$\begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_r \end{bmatrix}^2 = \begin{bmatrix} B_1^2 & & \\ & \ddots & \\ & & B_r^2 \end{bmatrix} = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_r \end{bmatrix} = A$$

so without loss of generality

$$A = \begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}.$$

Recall the (power series) binomial theorem, which states that as formal polynomials

$$\left(\sum_{k=0}^{\infty} \binom{1/2}{k} x^k \right)^2 = 1 + x, \qquad \text{where } \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} \text{ for } n \in \mathbb{Q}.$$

We have $A = \lambda(I + \lambda^{-1}N)$ with

$$N = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}$$

and in particular $N^n = 0$. So

$$B_0 := \sum_{k=0}^{\infty} \binom{1/2}{k} (\lambda^{-1}N)^k = \sum_{k=0}^{n-1} \binom{1/2}{k} \lambda^{-k} N^k$$

and $B_0^2 = I + \lambda^{-1}N$. So $(\sqrt{\lambda}B_0)^2 = \lambda(I + \lambda^{-1}N) = A$, where $\sqrt{\lambda}$ exists because $\lambda \in \mathbb{C}$.

Let's do another example:

Example 3.28.2. Let

$$A = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{bmatrix} \in M_n(\mathbb{Q}).$$

What is its Jordan Canonical Form?

The rank of A is 1, so its nullity is $n-1$, that is, we have eigenvalues $0, \dots, 0, n$. Also, $A^2 = nA$. So m_A has to divide $x^2 - nx = x(x-n)$. Because $\deg m_A > 1$ we must have $m_A = x^2 - nx$. So the Jordan Canonical Form is

$$\begin{bmatrix} n & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{bmatrix}.$$

Alternatively, you could have seen that A was diagonalizable because m_A splits into linear factors.

What about A as a matrix in $M_n(F)$? If $\operatorname{char} F \nmid n$, then the same proof works and we have the same answer. On the other hand, if $\operatorname{char} F | n$, then $m_A = x^2$. Then the Jordan Canonical Form is

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

Example 3.28.3. Let

$$A = \begin{bmatrix} -2 & 2 & 1 \\ -7 & 4 & 2 \\ 5 & 0 & 0 \end{bmatrix} \in M_3(\mathbb{Q}).$$

so that

$$xI - A = \begin{bmatrix} x+2 & -2 & -1 \\ 7 & x-4 & -2 \\ -5 & 0 & x \end{bmatrix}$$

and swapping c_1 and c_2, and then scaling c_1 by -1, gives

$$\begin{bmatrix} 1 & -2 & x+2 \\ 2 & x-4 & 7 \\ -x & 0 & -5 \end{bmatrix}$$

so that swapping $r_2 := r_2 - 2r_1$ and $r_3 := r_3 + xr_1$ gives

$$\begin{bmatrix} 1 & -2 & x+2 \\ 0 & x & -2x+3 \\ 0 & -2x & x^2+2x-5 \end{bmatrix}$$

and cleaning up gives

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & x & -2x+3 \\ 0 & -2x & x^2+2x-5 \end{bmatrix}$$

so that setting $c_3 \colon c_3 + 2c_2$ gives

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & x & 3 \\ 0 & -2x & x^2-2x-5 \end{bmatrix}$$

and swapping c_2 and c_3, and scaling r_2 by 1/3, gives

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & x/3 \\ 0 & x^2-2x-5 & -2x \end{bmatrix}$$

so that with $r_3 := r_3 - (x^2 - 2x - 5)r_2$ gives

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & x/3 \\ 0 & 0 & (-x^3+2x^2-x)/3 \end{bmatrix}$$

and with $c_3 := c_3 - (x/3)c_3$ and scaling r_3 by -3 gives

$$\begin{bmatrix} 1 & & \\ & 1 & \\ & & x^3-2x+x \end{bmatrix}$$

which is the Smith Normal Form of B. So we have $c_A = m_A = a_1 = x^3 - 2x^2 + x = x(x-1)^2$. So the Jordan Canonical Form of A is given by

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

Example 3.28.4. Suppose that $A \in M_{13}(\mathbb{Q})$, with $a_1 = (x-1)^2(x-2)(x-3)^2$, and $a_2 = x(x-1)^2(x-2)^2(x-3)^3$. Then the Jordan Canonical Form of A is given by

$$\begin{bmatrix}
1 & 1 & & & & & & & & & & & \\
 & 1 & & & & & & & & & & & \\
 & & 2 & & & & & & & & & & \\
 & & & 3 & 1 & & & & & & & & \\
 & & & & 3 & & & & & & & & \\
 & & & & & 0 & & & & & & & \\
 & & & & & & 1 & 1 & & & & & \\
 & & & & & & & 1 & & & & & \\
 & & & & & & & & 2 & 1 & & & \\
 & & & & & & & & & 2 & & & \\
 & & & & & & & & & & 3 & 1 & \\
 & & & & & & & & & & & 3 & 1 \\
 & & & & & & & & & & & & 3
\end{bmatrix}.$$

[Today, I learnt that if you want to make a matrix with more than 10 columns, you need to set the counter MaxMatrixCols to however many columns you need]

3.29 Nov 5, 2018

Today we'll talk about free modules and tensor products.

Let R be a commutative ring (we'll talk about noncommutative rings some time in the future; it's useful for next semester) with 1. Let A be a set. We can define

$$F_A := \{f\colon A \to R \text{ with } f(a) = 0 \text{ for all but finitely many } a \in A\}.$$

This is clearly an R-module. For $a \in A$, we have the element

$$\delta_a(b) = \begin{cases} 1 & \text{if } b = a \\ 0 & \text{otherwise} \end{cases}$$

that is, $\delta_a \in F_A$. In fact, F_A is a free module over R with basis $\{\delta_a\colon a \in A\}$. Indeed, take $f \in F_A$, and observe that

$$f = \sum_{\substack{a\in A \\ f(a)\neq 0}} f(a)\delta_a$$

which is a finite sum. This shows that the δ_a span. To show that they are linearly independent, say that

$$\sum_{a\in A'} c_a\delta_a = 0$$

for $A' \subseteq A$ finite and $c_a \in R$. Plugging in $a \in A'$ says that $c_a \cdot 1 = 0$, that is, $c_a = 0$ for all $a \in A'$, so they're linearly independent. This just says that every element of F_A is a unique linear combination (with scalars in R) of the set $\{\delta_a\colon a \in A\}$. We can identify $a \in A$ with δ_a. We can view F_A as a free R-module with basis A.

So this is much less painful than the construction of a free group. Like in that case, we have the universal property that for any $\varphi\colon A \to M$ there is a unique $\Phi\colon F_A \to M$ so that $\varphi = \Phi \circ \iota$, where $\iota\colon A \hookrightarrow F_A$ that is, the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[dr, "\varphi"'] & F_A \arrow[d, dashed, "\exists!\Phi"] \\
 & M
\end{tikzcd}$$

If A is a finite, set that, is $A = \{1, \dots, n\} =: [n]$, then $F_A = R^n$. Let's move on.

Tensor Products

Let R be a commutative ring. For R-modules M, N, P, we say that a map $\varphi\colon M \times N \to P$ is <u>R-bilinear</u> (or just <u>bilinear</u>, if R is clear) if

$$\begin{aligned} M &\to P & \qquad N &\to P \\ m &\mapsto \varphi(m,n) & \qquad n &\mapsto \varphi(m,n) \end{aligned}$$

are homomorphisms of R modules for all $m \in M$ and $n \in N$. Some examples include

Example 3.29.1. For $R = \mathbb{R}$, the dot product $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$,

Example 3.29.2. The map $M_n(R) \times M_n(R) \to M_n(R)$ given by $(A, B) \mapsto AB - BA$,

Example 3.29.3. The map $R \times R \to R$ given by $(a, b) \mapsto ab$,

Example 3.29.4. The map $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ given by $(v, w) \mapsto v \times w$.

We don't want to redo the whole theory of modules and homomorphisms to capture bilinear maps. Bilinear maps are nice: fix a $\varphi\colon M \times N \to P$ bilinear; observe that for any R-module homomorphism $f\colon P \to P'$, the map $f \circ \varphi\colon M \times N \to P'$ is bilinear. So the idea is to find one universal "best" bilinear map and then compose with homomorphisms to get all other bilinear maps. This is captured by

Theorem 3.29.5. *Take R-modules M and N. Then there is an R module $M \otimes_R N$ and a bilinear map $\iota\colon M \times N \to M \otimes_R N$ such that for any bilinear map $\varphi\colon M \times N \to P$, there is a unique homomorphism of R-modules $\Phi\colon M \otimes_R N \to P$ such that $\varphi = \Phi \circ \iota$, that is, the following diagram commutes:*

$$\begin{tikzcd}
M \times N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\exists!\Phi"] \\
 & P
\end{tikzcd}$$

Remark 3.29.6. This universal property characterizes $M \otimes_R N$ and $\iota\colon M \times N \to M \otimes_R N$ up to (canonical) isomorphism.

Remark 3.29.7. The map $\iota\colon M \times N \to M \otimes_R N$ is usually written as $\iota(m, n) = m \otimes n$; first of all, the notation $m \otimes n$ is ambiguous, unless we know what M, R, N are, and secondly, ι need not be surjective.

Proof. Consider $F_{M \times N}$, the free module on the set $M \times N$. Its basis can be identified with $M \times N$. So we have the inclusion map $M \times N \hookrightarrow F_{M \times N}$. This inclusion map is most definitely not bilinear. So we will define

$$M \otimes_R N := F_{M \times N}/K$$

where K is the submodule of $M \times N$ generated by

- $(m + m', n) - (m, n) - (m', n)$
- $(m, n + n') - (m, n) - (m, n')$
- $(rm, n) - r(m, n)$
- $(m, rn) - r(m, n)$

for all $r \in R, m, m' \in M, n, n' \in N$.

Observe that

$$\iota\colon M \times N \to F_{M \times N} \twoheadrightarrow M \otimes_R N$$

is R-bilinear. Now take any bilinear $\varphi\colon M \times N \to P$. Then because $F_{M \times N}$ is a free group we have

$$\begin{tikzcd}
M \times N \arrow[r, hook] \arrow[dr, "\varphi"'] & F_{M \times N} \arrow[d, "\exists!f"] \\
 & P
\end{tikzcd}$$

and observe that $f(K) = 0$, where K is the same K as above (that is, we defined $M \otimes_R N := F_{M \times N}/K$). For example,

$$f((m+m', n) - (m, n) - (m', n)) = f(m+m', n) - f(m, n) - f(m', n) = \varphi(m+m', n) - \varphi(m, n) - \varphi(m', n) = 0$$

because φ is bilinear. For similar reasons all other generators are annihilated by f. So we can factor the inclusion and the f through the projection by K:

$$\begin{tikzcd}
M \times N \arrow[r] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\exists!\Phi"] \\
 & P
\end{tikzcd}$$

as desired. □

Let's do an example:

Example 3.29.8. We have $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$. Indeed, take $a \in \mathbb{Z}/2\mathbb{Z}$ and $b \in \mathbb{Z}/3\mathbb{Z}$. Then we have

$$a \otimes b = (3 \cdot a) \otimes b = 3 \cdot (a \otimes b) = a \otimes (3b) = a \otimes 0 = a \otimes (0 \cdot 0) = 0 \cdot (a \otimes 0) = 0.$$

In general, we'll see at some point that if $a, b \geq 1$ that

$$\mathbb{Z}/\langle a \rangle \otimes_{[\mathbb{Z}?]} \mathbb{Z}/\langle b \rangle \cong \mathbb{Z}/\langle \gcd(a,b) \rangle.$$

Example 3.29.9. We have $R \otimes_R M \cong M$. Indeed, we have $j \colon R \times M \to M$ given by $(r,m) \mapsto rm$. Then if $\varphi \colon R \times M \to P$ is bilinear, we have

$$\begin{tikzcd}
R \times M \arrow[r, "j"] \arrow[dr, "\varphi"'] & M \arrow[d, dashed, "m \mapsto \varphi(1,m)"] \\
& P
\end{tikzcd}$$

and uniqueness gives $R \otimes_R M \cong M$.

The tensor product distributes:

Proposition 3.29.10. *We have* $(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$.

Proof sketch. We have a bilinear map $(M \oplus M') \times N \to (M \otimes_R N) \oplus (M' \otimes_R N)$ given by $((m,m'),n) \mapsto (m \otimes n, m' \otimes n)$ which gives a homomorphism $(M \oplus M') \otimes_R N \to (M \otimes_R N) \oplus (M' \otimes_R N)$.

We also have a bilinear map $M \times N \to (M \oplus M') \otimes_R N$ by $(m,n) \mapsto (m,0),n)$, so we get a homomorphism $M \otimes_R N \to (M \oplus M') \otimes_R N$. Do the same thing with M replaced by M', and check that they are inverses. □

So we get

Corollary 3.29.11. *We have* $R^m \otimes_R R^n \cong (R \otimes_R R^n)^m \cong (R^n)^m \cong R^{nm}$. *n general, we have* $R^m \otimes_R R^n$ *is a free module with basis* $\{e_i \otimes e_j \colon 1 \leq i \leq m \text{ and } 1 \leq j \leq m\}$.

3.30 Nov 7, 2018

Last time, for R a commutative ring and M, N two R-modules, we defined the tensor product $M \otimes_R N$; it is an R-module with an R-bilinear map $\iota\colon M \times N \to M \otimes_R N$, given by $(m, n) \mapsto m \otimes n$. We have the following universal property: for any R-bilinear map $\varphi\colon M \times N \to P$, there is a unique homomorphism $\Phi\colon M \otimes_R N \to P$ of R-modules such that $\varphi = \Phi \circ \iota$. This was expressed in the commutative diagram

$$\begin{tikzcd}
M \times N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\exists!\Phi"] \\
& P
\end{tikzcd}$$

To appreciate this construction we probably need to prove some theorems, but at this point at least the tensor product is turning bilinear maps (mysterious) to homomorphisms (less so).

The elements of $M \otimes_R N$ are called <u>tensors</u>; the element $m \otimes n$ is called a pure, or sometimes simple, or sometimes elementary, tensor. We saw that $R \otimes_R M \cong M$, and $(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$. This isomorphism was given by $((m, m'), n) \to (m \otimes n, m' \otimes n)$ and checking that the universal property gives an inverse. There is also

$$\left(\bigoplus_{i \in I} M_i\right) \otimes_R N \cong \bigoplus_{i \in I} (M_i \otimes_R N).$$

Example 3.30.1. We have $M \otimes_R N \cong N \otimes_R N$. This will use that R is commutative somehow. Obviously, the map will be given by $m \otimes n \leftrightarrow n \otimes n$ but there are details to check:

Consider the map $M \times N \to N \times M$ given by $(m, n) \mapsto (n, m)$; this map is bilinear so it factors to a map $\varphi\colon M \times N \to N \otimes_R M$, that is, we have the diagram:

$$\begin{tikzcd}
& & M \otimes_R N \arrow[d, "\exists!\Phi"] \\
M \times N \arrow[urr, "\iota"] \arrow[r] \arrow[rr, dashed, bend right, "\varphi"'] & N \times M \arrow[r] & N \otimes_R N
\end{tikzcd}$$

and now we have $\Phi(m \otimes n) = \Phi(\iota(m, n)) = \varphi(m, n) = n \otimes m$.

Example 3.30.2. We have for $I \subseteq R$ an ideal, the R-module R/I. If N is an R-module, we have the R-module $IN = \{\sum_{i=1}^{n} a_i n_i \colon a_i \in I, n_i \in N\}$, which is the smallest submodule of n containing all the an with $a \in I, n \in N$. We claim that

$$R/I \otimes_R N \cong N/IN.$$

Indeed, we have a bilinear map

$$\begin{gathered} R/I \times N \xrightarrow{j} N/IN \\ (\bar{r}, n) \mapsto \overline{rn} \end{gathered}$$

and one can check that j is indeed well defined and bilinear. We claim that the universal property holds for j, that is we should verify

$$\begin{tikzcd}
R/I \times N \arrow[r, "j"] \arrow[dr, "\varphi"'] & N/IN \arrow[d, "\exists!\Phi"] \\
& P
\end{tikzcd}$$

But if it exists, then this map sends $\Phi(\bar{n}) = \Phi(j(1, n)) = \varphi(1, n)$. So this is a possible definition of Φ; if Φ exists then it is unique. One should check that Φ is well defined (it is clearly a homomorphism if it's well defined). To see this we compute

$$\Phi\left(\overline{n+\sum_{i=1}^{m} a_i n_i}\right) = \varphi(1,n) + \sum_{i=1}^{m} a_i \varphi(1,n_i) = \varphi(1,n) + \sum_{i=1}^{m} \varphi(\bar{a}_i, n_i) = \varphi(1,n) + \sum_{i=1}^{m} \varphi(0,n_i) = \varphi(1,n).$$

So j satisfies the universal property and proves the claim. Let's do an example of this example:

Set $R = \mathbb{Z}$ and $I = \langle a\rangle$. Furthermore let $N = \mathbb{Z}/\langle b\rangle$ (where $a, b \geq 1$ are integers). We have

$$\mathbb{Z}/\langle a\rangle \otimes_{\mathbb{Z}} \mathbb{Z}/\langle b\rangle \cong \frac{\mathbb{Z}/\langle b\rangle}{a \cdot \mathbb{Z}/\langle b\rangle} = \frac{\mathbb{Z}/\langle b\rangle}{\langle \gcd(a,b)\rangle/\langle b\rangle} \cong \mathbb{Z}/\langle \gcd(a,b)\rangle$$

Let's now consider a (not necessarily commutative) ring R (still with a multiplicative identity). Let M be a right R-module and N a left R-module. We will define an abelian group $M \otimes_R N$ (one needs the $\otimes_R$ to be in the middle, as if it was "connecting two trains"). In this setting, bilinear maps are not quite the right thing:

Definition 3.30.3. Let L be an abelian group (written additively). A map $\varphi\colon M \times N \to L$ is R-balanced if

- $\varphi(m+m', n) = \varphi(m,n) + \varphi(m',n)$
- $\varphi(m, n+n') = \varphi(m,n) + \varphi(m,n')$
- $\varphi(m, rn) = \varphi(rm, n)$

for $m, m' \in M, n, n' \in N, r \in R$. Notice that $r\varphi(m,n)$ doesn't necessarily make sense because L is not (necessarily) an R-module.

One obvious example of an R-balanced map was given last lecture, with $R \times R \to R$ given by $(a,b) \mapsto ab$.

There is a universal R-balanced map $M \times N \xrightarrow{\iota} M \otimes_R N$ such that for any R-balanced map $\varphi\colon M \times N \to L$, there is a unique group homomorphism $\Phi\colon M \otimes_R N \to L$ such that $\Phi \circ \iota = \varphi$. The proof is exactly the same as last time; the commutative diagram is also exactly the same (with P replaced by L).

Definition 3.30.4. Let R, S be rings. An abelian group M is an (S,R)-bimodule if M is a left S-module, and a right R-module such that $s(mr) = (sm)r$ for all $s \in S, r \in R, m \in M$.

Example 3.30.5. The ring R is an (R,R)-bimodule. Dummit/Foote calls this "the standard R-module".

Example 3.30.6. Let R be a commutative ring, and M a left R-module. Then $m \cdot r := rm$ turns M into a (R,R)-module.

Let M be an (S,R)-bimodule and N a left R-module. Then $M \otimes_R N$ is an abelian group, but the S-action on M gives some extra structure: $M \otimes_R N$ is actually an S-module, given by

$$s\left(\sum_{i=0}^{e} m_i \otimes n_i\right) := \sum_{i=0}^{e} (sm_i) \otimes n_i.$$

So if R is commutative and M, N are R-modules, then they're (R,R)-bimodules and $M \otimes_R N$ is an R-module, so it agrees with before.

Example 3.30.7. Let G be a group, and $H \subseteq G$ a subgroup. Say that H acts on a vector space V over F. So this is a map $\varphi\colon H \to \mathrm{Aut}_F(V) = \mathrm{GL}(V)$. We have the induced representation $FG \otimes_{FH} V$, where FH and FG are the group rings. This is an FG-module, that is, a vector space over F with a G-action.

More generally, let M be a left R-module and S an R-algebra (that is, a ring homomorphism $f\colon R \to S$ with $f(R)$ contained in the center of S). Then S is an (S,R)-bimodule, that is, $s \cdot r := sf(r)$. Then we get the left S-module $S \otimes_R M$, called the extension of scalars.

3.31 Nov 9, 2018

[I was out of town for this lecture. Cosmo Viola and Yichi Zhang took notes that I borrowed from.]

Let R, S, T be rings, and M an (S, R)-bimodule and N an (R, T)-bimodule. We defined the $\mathbb{Z}$-module (abelian group) denoted $M \otimes_R N$, and can in fact turn $M \otimes_R N$ into an (S, T)-bimodule.

Take an R-algebra S (that is, a ring homomorphism $f\colon R \to S$ such that $f(R)$ is contained in the center of S; for $r \in R, s \in S$, we have $r \cdot s = f(r)s = sf(r) = s \cdot r$, where the second equality follows because $f(r)$ is in the center). Then, if M is a left R-module, we have $S \otimes_R M$ a left S-module.

Now suppose R is commutative. Then, for R-algebras A and B, we have that $A \otimes_R B$ is also an R-algebra. Multiplication is defined by $(a \otimes b) \cdot (a' \otimes b') = (aa') \otimes (bb')$.

Example 3.31.1. Let S be a commutative R-algebra, with $R \hookrightarrow S$. We claim that $S \otimes_R R[x] \cong S[x]$. Indeed, consider the ($R$-bilinear) map

$$\begin{aligned} S \times R[x] &\xrightarrow{j} S[x] \\ (a, f) &\mapsto af \end{aligned}$$

which induces a unique R-module homomorphism

$$\begin{aligned} S \otimes_R R[x] &\to S[x] \\ a \otimes f &\mapsto af \end{aligned}$$

that is in fact an isomorphism with inverse

$$\begin{aligned} S[x] &\to S \otimes_R R[x] \\ \sum_{i=0}^{m} a_i x^i &\mapsto \sum_{i=0}^{m} a_i \otimes x^i \end{aligned}$$

Now let

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

be an exact sequence of left R-modules. Then, for a right R-module M, we have an exact sequence of $\mathbb{Z}$-modules

$$\begin{tikzcd} 0 \arrow[r] & M \otimes_R A \arrow[r, "f_*"] & M \otimes_R B \arrow[r, "g_*"] & M \otimes_R C \arrow[r] & 0 \end{tikzcd}$$

defined by $f_*(m \otimes a) = m \otimes f(a)$. The failure of surjectivity of g_* leads to functors $\operatorname{Tor}_n^R(M, -)\colon R - \text{mod} \to \mathbb{Z} - \text{mod}$, where $\operatorname{Tor}_0^R(M, -) = M \otimes_R -$.

More in 6320.

4 Fields

4.31 Nov 9, 2018

Let F be a field. There is a unique homomorphism of rings $\varphi\colon \mathbb{Z} \to F$, where $\varphi(1) = 1$ and hence

$$\varphi(n) = \begin{cases} \underbrace{1 + \cdots + 1}_{n \text{ times}} & \text{if } n \geq 0 \\ \underbrace{-1 - \cdots - 1}_{n \text{ times}} & \text{if } n < 0 \end{cases}$$

Then observe that

$$\mathbb{Z}/\ker\varphi \hookrightarrow F,$$

where F is a field, so $\mathbb{Z}/\ker\varphi$ better not have any zero-divisors; we have $\mathbb{Z}/\ker\varphi$ is an integral domain, and $\ker\varphi$ is a prime ideal of $\mathbb{Z}$. So $\ker\varphi = \langle n\rangle$ for $n = 0$ or $n = p$ a prime.

The characteristic of F is $\operatorname{char} F = n$. Now if $\operatorname{char} F = 0$ then

$$\varphi\colon \mathbb{Z} \hookrightarrow F \quad \text{ extends to } \mathbb{Q} \hookrightarrow F$$

which we view as $\mathbb{Q} \subseteq F$. Otherwise if $\operatorname{char} F = p$ then $\mathbb{F}_p = \mathbb{Z}/\langle p\rangle \hookrightarrow F$, which we view as $\mathbb{F}_p \subseteq F$. We say that $\mathbb{Q}/\mathbb{F}_p$ is the prime field of F.

Consider a subfield $F \subseteq K$, where both F and K are fields. We call K a field extension of F, and denote this K/F. The degree of an extension K/F is $[K : F] = \dim_F K$. For extensions $F \subseteq K \subseteq L$, we have $[L : F] = [L : K][K : F]$. The proof idea is as follows: if either $[L : K]$ or $[K : F]$ are infinite, then this is easy; if both are finite then take a basis $a_1, \dots, a_m$ of L over K and a basis $b_1, \dots, b_n$ of K over F. As an exercise, one can show that $a_i b_j$ for $i \in [m], j \in [n]$ is a basis of L over K. Then $[L : F] = mn = [L : K][K : F]$.

Consider an extension K/F and fix $\alpha \in K$. Let $F[\alpha]$ and $F(\alpha)$ be the smallest subring and subfield respectively of K containing F and α. We have a homomorphism of F-algebras

$$\begin{aligned} \varphi\colon F[x] &\to K \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

and again this induces $F[x]/\langle\ker\varphi\rangle \xrightarrow{\sim} F[\alpha] \subseteq K$, and since K is a field we have that $\ker\varphi$ is a prime ideal of $F[x]$; we have $\ker\varphi = \langle 0\rangle$ or $\ker\varphi = \langle p\rangle$ with $p \in F[x]$ monic and irreducible.

As before, if $\ker\varphi = \langle p\rangle$ then we get

$$F[x]/\langle p\rangle \xrightarrow{\sim} F[\alpha]$$

and note that since $F[x]/\langle p\rangle$ is a field then so is $F[\alpha]$, and hence $F[\alpha] = F(\alpha)$. We have

$$[F(\alpha) : F] = \dim_F F[x]/\langle p\rangle = \deg p,$$

and we say $p \in F[x]$ is the minimal polynomial of α over F (where the minimal polynomial is the monic polynomial in $F[x]$ of minimal degree such that $p(\alpha) = 0$).

On the other hand, if $\ker\varphi = 0$, that is, $f(\alpha) \neq 0$ for all nonzero $f \in F[x]$, then $F[\alpha]$ is not a field, and φ extends to a map $F(x) \xrightarrow{\sim} F(\alpha)$. In this case we say α is transcendental over F; if $\ker\varphi = \langle p\rangle$ as discussed above we say α is algebraic over F.

4.32 Nov 12, 2018

Let F be a field, and K/F a field extension (that is, a field K such that $F \subseteq K$).

Take $\alpha \in K$. Then we might have that α is transcendental over F, that is, there is no non-zero $f \in F[x]$ with $f(\alpha) = 0$. Then we have

$$\begin{aligned} F[x] &\xrightarrow{\sim} F[\alpha] \subseteq F(\alpha) \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

that is, transcendental elements are basically like free variables (from the point of view of algebra). Since $F[x]$ is an infinite dimensional vector space over F (it has F-basis $\{1, x, x^2, \dots\}$), we also have $[F(\alpha) : F] = \infty$.

Otherwise, we have that α is algebraic over F. Then there is a unique monic $m_{\alpha,F} \in F[x]$ of minimal degree such that $m_{\alpha,F}(\alpha) = 0$ [there is at least one such monic polynomial, and if there are two, one can apply the division algorithm]. We call $m_{\alpha,F}$ the minimal polynomial of α over F. We have, like last time,

$$\begin{aligned} F[x] &\twoheadrightarrow F[\alpha] \subseteq K \\ f &\mapsto f(\alpha), \\ \text{inducing } F[x]/\langle m_{\alpha,F}\rangle &\xrightarrow{\sim} F[\alpha] \end{aligned}$$

where we also have $F[x]/\langle m_{\alpha,F}\rangle$ is a field because $m_{\alpha,F}$ is irreducible. Also, we have

$$[F(\alpha) : F] = [F[\alpha] : F] = \deg m_{\alpha,F}.$$

Example 4.32.1. Fix $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and we have $m_{\alpha,\mathbb{Q}} = x^3 - 2$. We have the inclusion of fields

$$\begin{tikzcd} \mathbb{Q}(\alpha) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

and the isomorphism

$$\begin{aligned} \mathbb{Q}[x]/\langle x^3 - 2\rangle &\xrightarrow{\sim} \mathbb{Q}[\alpha] \\ \bar{f} &\mapsto f(\alpha). \end{aligned}$$

Then, $\mathbb{Q}[\alpha]$ has $\mathbb{Q}$-basis $1, \alpha, \alpha^2$, and $\mathbb{Q}[x]/\langle x^3 - 2\rangle$ has $\mathbb{Q}$-basis $1, \bar{x}, \bar{x}^2$. Here's a question: what is $(2+\alpha)^{-1}$?

We can work in $\mathbb{Q}[\alpha]$: polynomial division gives

$$x^3 - 2 = (x^2 - 2x + 4)(x + 2) - 10$$

so for $x = \alpha$ we have $(\alpha^2 - 2\alpha + 4)(\alpha + 2) = 10$ and

$$(2+\alpha)^{-1} = \frac{4}{10} - \frac{2}{10}\alpha + \frac{1}{10}\alpha^2.$$

Now let $\beta = \sqrt[3]{2}e^{2\pi i/3} \in \mathbb{C}$. We have

$$\mathbb{Q}[\beta] \xleftarrow{\sim} \mathbb{Q}[x]/\langle x^3 - 2\rangle \xrightarrow{\sim} \mathbb{Q}[\alpha]$$

sending $c_0 + c_1\beta + c_2\beta^2$ to $c_0 + c_1\alpha + c_2\alpha^2$.

Consider an isomorphism of fields $\varphi\colon F \xrightarrow{\sim} F'$, and fix $M \in F[x]$ irreducible. Set $m' = \varphi(m) \in F'[x]$ (that is, apply φ to the coefficients of m). Then m' is irreducible. Take a root α of m (in some extension of F) and a root β of m' (in some extension of F'). Then we have isomorphisms

$$\begin{tikzcd}
F(\alpha) & F[x]/\langle m\rangle \arrow[l, "\sim"'] \arrow[r, "\sim"] & F'[x]/\langle m'\rangle \arrow[r, "\sim"] & F'(\beta) \\
f(\alpha) & \bar{f} \arrow[l, mapsto] & \bar{f} \arrow[r, mapsto] & f(\beta) \\
& f \arrow[r, mapsto] & \overline{\varphi(f)} &
\end{tikzcd}$$

and we get an isomorphism $\varphi_{\text{new}} \colon F(\alpha) \xrightarrow{\sim} F'(\beta)$ such that $\varphi_{\text{new}}|_F = \varphi$ and $\varphi_{\text{new}}(\alpha) = \beta$. Note that φ_{new} is unique!

Definition 4.32.2. An extension K/F is a splitting field for $f \in F[x]$ if f factors into degree 1 terms in $K[x]$ (sometimes called "splits completely") and no field $F \subseteq K' \subsetneq K$ has this property.

Theorem 4.32.3. *Fix $f \in F[x]$ and set $n = \deg f$. Then a splitting field K for f exists, and $[K : F] \leq n!$.*

Proof. Induct on $n \geq 1$. For $n = 1$ this is easy. So suppose this is true for polynomials of degree at most $n-1$, and pick $f \in F[x]$. Take an irreducible factor $M \in F[x]$ of f. Then $L := F[x]/\langle f\rangle$ is a field extension of F of degree $\deg m \leq n$. There is an $\alpha \in L$ such that $f(\alpha) = 0$. Then $f(x) = (x-\alpha)g(x)$ with $g(x) \in L[x]$, and $\deg g = n-1$. By the inductive hypothesis, there is an extension K/L with $[K : L] \leq (n-1)!$ such that g splits completely in $K[x]$. This says that f splits completely in $K[x]$, and

$$[K : F] = \underbrace{[K : L]}_{\leq (n-1)!}\underbrace{[L : F]}_{\leq n} \leq n!$$

Now we can replace K by the smallest dimensional $F \subseteq K' \subseteq K$ for which f splits completely in $K'[x]$. □

Take $f \in F[x]$. A splitting field K/F of f is unique up to isomorphism fixing f:

$$\begin{tikzcd}
K \arrow[rr, "\sim"] & & K' \\
& F \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

The idea is to build up inductively. Take $m \in F[x]$ irreducible dividing f and $\deg m > 1$ if possible (and if not, then we'd be done), and choose roots $\alpha_1 \in K$ and $\beta_1 \in K'$, so that

$$\begin{tikzcd}
F_1 := F_0(\alpha_1) \arrow[r, leftrightarrow, "\exists!\varphi_1"] \arrow[d, dash] & F_0(\beta_1) =: F_1' \arrow[d, dash] \\
F_0 = F \arrow[r, leftrightarrow, "\text{id}"] & F_0' = F
\end{tikzcd}$$

As before, take $m \in F_1[x]$ irreducible dividing f and $\deg m > 1$ (again, if possible; if not, we'd be done), and choose roots $\alpha_2 \in K$ and $\beta_2 \in K'$ of m'; we can repeat

$$\begin{tikzcd}
K = F_m(\alpha_{m+1}) \arrow[r, leftrightarrow] \arrow[d, dash] & F_m'(\beta_{m+1}) = K' \arrow[d, dash] \\
\vdots \arrow[d, dash] & \vdots \arrow[d, dash] \\
F_2 := F_1(\alpha_2) \arrow[r, leftrightarrow, "\exists!\varphi_2"] \arrow[d, dash] & F_1'(\beta_2) =: F_2' \arrow[d, dash] \\
F_1 := F_0(\alpha_1) \arrow[r, leftrightarrow, "\exists!\varphi_1"] \arrow[d, dash] & F_0(\beta_1) =: F_1' \arrow[d, dash] \\
F_0 = F \arrow[r, leftrightarrow, "\text{id}"] & F_0' = F
\end{tikzcd}$$

4.33 Nov 14, 2018

Fix a nonzero $f \in F[x]$ for some field F. We had

Definition 4.33.1. An extension K/F is a splitting field of f over F if f splits completely in $K[x]$ and does not split completely in $K'[x]$ for any field $F \subseteq K' \subsetneq K$. So

$$f(x) = c\prod_{i=1}^{n}(x - \alpha_i)$$

with $c \in F^\times$ and $a_i \in K$, and $F(\alpha_1, \dots, \alpha_n) = K$.

Last time, we showed the existence of a splitting field K/F of f over F, and moreover showed that $[K : F] \leq n!$. We also showed that it is essentially unique: for two splitting fields of f over F, say K and K', there is an isomorphism $\varphi\colon K \to K'$ such that $\varphi|_F = \mathrm{id}_F$. This is not unique, and the failure of uniqueness is measured in Galois theory (which is a 6320 thing). In any case, up to isomorphism, we can talk about "the" splitting field.

Note that if $f(x) = c(x - \alpha_1)\dots(x - \alpha_n)$ is the factorization of f in K, then $f(x)$ factors as

$$f(x) = c\prod_{i=1}^{n}(x - \varphi(\alpha_i))$$

in K'.

Example 4.33.2. Let $f = x^4 - 2 \in \mathbb{Q}[x]$. This is irreducible (by Eisenstein at $p = 2$). We will work over $\mathbb{C}$, that is,

$$f = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)$$

and hence its splitting field is $K = \mathbb{Q}(\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$. We have

$$[K : \mathbb{Q}] = \underbrace{[K : \mathbb{Q}(\sqrt[4]{2})]}_{=2}\underbrace{[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]}_{=4} = 8$$

and by the way $8 \leq 4!$.

Example 4.33.3. Let $F = \mathbb{F}_p(t)$ and consider $f = x^p + t$. We claim that f is irreducible in $(\mathbb{F}_p(t))[x]$: by Gauss' lemma, it suffices to check it is irreducible in $(\underbrace{\mathbb{F}_p[t]}_{\text{UFD}})[x]$. But clearly f is irreducible in

$$(\mathbb{F}_p[x])[t] \cong \mathbb{F}_p[t][x] \cong (\mathbb{F}_p[t])[x]$$

because it is degree 1 in t.

Let α be a root of f (in some extension of F). We have

$$(x - \alpha)^p = \sum_{n=0}^{p}\binom{p}{n}x^n(-\alpha)^{p-n} = x^p + (-\alpha)^p \in \mathbb{F}_p[x].$$

But since α is a root we have $0 = \alpha^p + t$ and hence

$$(x - \alpha)^p = x^p - \alpha^p = x^p + t$$

so that $x^p + t = (x - \alpha)^p$. It follows that $K = F(\alpha)$ and $[K : F] = p$. We'll see later that this sort of phenomenon doesn't happen in characteristic 0, that is, an irreducible polynomial will give distinct roots.

Consider nonzero $f \in F[x]$, and let K/F be a splitting field of f. Then

$$f(x) = c\prod_{i=1}^{r}(x-\alpha_i)^{e_i}$$

with $c \in F^\times, \alpha_i \in K$ are distinct, and $e_i \geq 1$. We say f is separable if it has no multiple roots, that is, $e_1 = \cdots = e_r = 1$.

We'll give a simple criterion to check if f is separable.

Let $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. The derivative of f is $f' = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$. We get some of the usual properties (when we restrict to polynomials): it's linear, and there are the chain/product rules.

Lemma 4.33.4. *Let α be a root of f (in some field). Then α is a multiple root of f if and only if $f'(\alpha) = 0$.*

Proof. If $f(x) = (x-\alpha)^e g(x)$ for $e \geq 1$ and g is such that $g(\alpha) \neq 0$, then $f'(x) = e(x-\alpha)^{e-1}g(x) + (x-\alpha)^e g'(x)$. So

$$f'(\alpha) = e(x-\alpha)^{e-1}g(\alpha) = \begin{cases} eg(\alpha) \neq 0 & \text{if } e = 1 \\ 0 & \text{if } e > 1 \end{cases}$$

□

Theorem 4.33.5. *For $f \in F[x]$ nonzero, we have f is separable if and only if f and f' are relatively prime in $F[x]$.*

The point is that we don't have to understand splitting fields, we can just work over the base field.

Proof. The backwards direction follows from the fact that $\langle f, f'\rangle = \langle 1\rangle = F[x]$, and so $af + bf' = 1$ for $a, b \in F[x]$. Now if α (in some extension of F) satisfies $f(\alpha) = f'(\alpha) = 0$ then $a(\alpha)f(\alpha) + b(\alpha)f'(\alpha) = 0$, a contradiction. So there are no multiple roots, by the previous lemma. Hence f is separable.

Conversely, if f and f' are not relatively prime. So there is an irreducible $m \in F[x]$ dividing f and f'. Take α to be a root of m in some extension of F. Then $f = mg_1$ and $f' = mg_2$ implies $f(\alpha) = m(\alpha)g_1(\alpha) = 0$ and $f'(\alpha) = m(\alpha)g_2(\alpha) = 0$, so that f has a repeated root at α by the previous lemma. □

Example 4.33.6. Consider $f = x^p + t \in \mathbb{F}_p(t)[x]$, and observe that $f' = px^{p-1} = 0$. This means that any root of f is a multiple root of f, as we saw. In particular, f is not separable (which we already knew).

Example 4.33.7. Consider $f = x^n - 1 \in F[x]$, and observe that $f' = nx^{n-1}$. If $\operatorname{char} F | n$, then we have the same situation in Example 4.33.6, and f is not separable. In the other case, if $\operatorname{char} F \nmid n$ then $x^n - 1$ and nx^{n-1} are relatively prime (because the only irreducible dividing nx^{n-1} is x); it follows that f is separable.

Proposition 4.33.8. *We have*

a) If $f \in F[x]$ is irreducible and $f' \neq 0$, then f is separable.

b) When $\operatorname{char} F = 0$, we always have $f' \neq 0$ when $\deg f \geq 1$. In particular, f is separable if and only if f is a product of nonassociate irreducible polynomials.

Proof. Everything is clear except for part (a), so we'll prove that:

If f is irreducible then the only factors of f up to units are 1 and f. This shows that $\gcd f, f' = 1$ or f. Note that $f \nmid f'$ since $\deg f' < \deg f$ and $f' \neq 0$. This implies that f is separable. □

Remark 4.33.9. If $f \in F[x]$ is irreducible and $\operatorname{char} F = p > 0$, then $f(x) = f_{\text{sep}}(x^{p^h})$ for a unique $h \geq 0$ and a unique separable $f_{\text{sep}} \in F[x]$.

4.34 Nov 16, 2018

Today we'll talk about cyclotomic fields.

Example 4.34.1. (Cyclotomic Fields) Fix $n \geq 1$. Consider $f = x^n - 1 \in \mathbb{Q}[x]$. The roots of f, say in $\mathbb{C}$, are the n-th roots of unity. They form a cyclic group (under multiplication); call this group $\mu_n = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}$. Usually we pick $\zeta_n = e^{2\pi i/n}$. The splitting field of f is $\mathbb{Q}(\zeta_n)$.

We say $\zeta \in \mu_n$ is primitive if it has order n in μ_n. Define the n-th cyclotomic polynomial to be

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x - \zeta) \in \mathbb{Q}(\zeta_n)[x].$$

Then we have

$$\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a)$$

which is well defined in the sense that if $a \cong b \pmod{n}$ then $x - \zeta_n^a = x - \zeta_n^b$. If you like, you can define

$$\Phi_n(x) = \prod_{\substack{a \leq n \\ \gcd(a,n)=1}} (x - \zeta_n^a)$$

and it is obvious that $\deg \Phi_n = \#(\mathbb{Z}/n\mathbb{Z})^\times =: \phi(n)$ (where ϕ is the Euler totient function).

We have

$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$

This is a factorization (a priori in $\mathbb{Q}(\zeta_n)$); we claim that $\mathbb{Z}[x]$.

We will induct on $n \geq 1$. The claim is true for $n = 1$, that is, $\Phi_1(x) = x - 1$. Now assume $\Phi_d \in \mathbb{Z}[x]$ for $d < n$. Then

$$\underbrace{\prod_{d|n} \Phi_d}_{\substack{\in \mathbb{Z}[x], \\ \text{primitive}}} \cdot \Phi_n = \underbrace{x^n - 1}_{\substack{\in \mathbb{Z}[x], \\ \text{primitive}}}$$

so by Gauss' Lemma $\Phi_n \in \mathbb{Z}[x]$.

Proposition 4.34.2. *The polynomial $\Phi_n \in \mathbb{Z}[x]$ is irreducible.*

Proof. Suppose $\Phi_n = fg$ with $f, g \in \mathbb{Z}[x]$ and f irreducible. Take any root ζ of f. Take any prime $p \nmid n$. We have $\Phi_n(\zeta^p) = 0$. So ζ^p is a root of f or g.

Suppose first that $g(\zeta^p) = 0$. Then $f(x)$ and $g(x^p)$ have a common root ($x = \zeta$). Since f is irreducible and primitive we have $f | g(x^p)$ in $\mathbb{Z}[x]$. Taking mod p shows that $\bar{f} | \bar{g}(x^p) = \bar{g}(x)^p$ in $\mathbb{F}_p[x]$. So in particular $\bar{f}$ and $\bar{g}$ are not relatively prime (in $\mathbb{F}_p[x]$). So $x^n - 1 = \bar{\Phi}_n = \bar{f}\bar{g} \in \mathbb{F}_p[x]$ is not separable. This is a contradiction, because $h := x^n - 1$ and $h' = nx^{n-1}$ are relatively prime in $\mathbb{F}_p[x]$ (remember we assumed $p \nmid n$), so by Theorem 4.33.5 we see that h is in fact separable.

So $f(\zeta^p) = 0$ for all primes $p \nmid n$. So for any root ζ' of Φ_n, we have $\zeta' = \zeta^a$ for some $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. If $a = p_1 \dots p_r$ with $p_i \nmid n$, then $\zeta' = (\dots((\zeta^{p_1})^{p_2}) \dots)^{p_r}$ and so ζ' is a root of f. Then f has all the roots of Φ_n. Furthermore both Φ_n and f are monic, and Φ_n is separable. Then we are done since f is irreducible. □

Corollary 4.34.3. *We have $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \phi(n)$.*

This corollary is equivalent to the previous proposition.

Remark 4.34.4. The polynomials Φ_n are important for number theory. For $p \nmid n$, we have Φ_n splits completely in $\mathbb{F}_p[x]$ if and only if $p \equiv 1 \pmod{n}$.

Example 4.34.5. (Finite fields) Fix a finite field $\mathbb{F}$ and let $p = \operatorname{char} \mathbb{F} > 0$. We have $\mathbb{F}_p \subseteq \mathbb{F}$. We have $|\mathbb{F}| = p^{[\mathbb{F}:\mathbb{F}_p]}$, where recall that $[\mathbb{F} : \mathbb{F}_p] = \dim_{\mathbb{F}_p} \mathbb{F}$.

Fix a prime p and an integer $n \geq 1$. Let's construct a field with p^n elements. Consider the group $\mathbb{F}^\times$, which has order $p^n - 1$. Then if $a \in \mathbb{F}^\times$, we have $a^{p^n-1} = 1$; this says that for any $a \in \mathbb{F}$, a is a root of $x^{p^n} - x$. It follows that

$$x^{p^n} - x = \prod_{a \in \mathbb{F}} (x - a)$$

and this is supposed to be suggestive (this is not a proof; we assumed $\mathbb{F}$ exists).

Indeed, fix p and $n \geq 1$. Let K be a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Then $x^{p^n} - x \in \mathbb{F}_p[x]$ is separable since $x^{p^n} - x$ and $p^n x^{p^n-1} - 1 = -1$ are relatively prime. So $\mathbb{F} := \{\alpha \in K \colon \alpha^{p^n} - \alpha = 0\}$. Note that separability means that $|\mathbb{F}| = p^n$.

We claim that $\mathbb{F}$ is a subfield of K. Obviously, 0 and 1 are in $\mathbb{F}$; if $\alpha, \beta \in \mathbb{F}$ we have $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ so $\alpha + \beta \in \mathbb{F}$, and $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n}$ so $\alpha\beta \in \mathbb{F}$.

Finally, the field $\mathbb{F}$ with p^n elements is unique up to isomorphism, so it is often denoted $\mathbb{F}_{p^n}$. Uniqueness follows from the fact that K is unique up to isomorphism.

Definition 4.34.6. A field K is algebraically closed if every non-constant $f \in K[x]$ has a root in K (equivalently, if all nonzero $f \in K[x]$ split completely in K).

An example is $\mathbb{C}$.

Next time, we'll prove

Theorem 4.34.7. *Every field F is contained in an algebraically closed field.*

The proof will be a bit painful.

4.35 Nov 19, 2018

We'll finish fields today. [There's a final homework that's on blackboard; it'll be due next Friday, Nov 30. There will be a takehome final that'll go up after the last class; it'll be due on Dec 13 at 4:30 pm.]

Recall that a field K is algebraically closed if every non-constant $f \in K[x]$ has a root in K (equivalently, all nonzero $f \in K[x]$ split completely). Today we will prove

Theorem 4.35.1. *Every field F is contained in an algebraically closed field.*

Proof. Sometimes fields are uncountably large, so we have to do something more drastic (Zorn's lemma). Here's a proof due to Artin:

For each non-constant $f \in F[x]$, denote by x_f an indeterminate variable. Consider the polynomial ring $R = F[\{x_f : f \in F[x]\}]$. Let I be the ideal of R generated by $\underline{\text{all}}$ the $f(x_f)$ with $f \in F[x]$, that is, $I = \langle \{f(x_f) : f \in F[x]\}\rangle$. Observe that for $\bar{x}_f \in R/I$, we have $f(\bar{x}) = \overline{f(x_f)} = 0$.

The idea is to choose a maximal ideal $I \subseteq \mathfrak{m} \subsetneq R$, and so $R/\mathfrak{m}$ is a *field* extension of F such that every $f \in F[x]$ has a root (and it has a root of the same reason as above).

For this idea to work we better show that $I \neq R$. Suppose that $1 \in I$. Then $g_1 f_1(x_{f_1}) + \dots + g_n f_n(x_{f_n}) = 1$ for some $f_i \in F[x]$ and $g_i \in R$. For ease of notation set $x_i = x_{f_i}$ for all i. We have other variables $x_{n+1}, \dots, x_m$ such that $g_1(x_1, \dots, x_m) f_1(x_1) + \dots + g_n(x_1, \dots, x_m) f_n(x_n) = 1$. Let K/F be a splitting field of $f_1(x) \dots f_n(x)$, that is, a field where all of the f_i simultaneously split. Let $\alpha_i \in K$ be a root of $f_i(x)$. Now set $x_i = \alpha_i$ for $i \in [n]$. Then

$$1 = g_1(\alpha_1, \dots, \alpha_n, x_{n+1}, \dots, x_n) \underbrace{f_1(\alpha_1)}_{=0} + \dots + g_n(\alpha_1, \dots, \alpha_n, x_{n+1}, \dots, x_n) \underbrace{f_n(\alpha_n)}_{=0} = 0.$$

Now we can use our idea: by Zorn's Lemma, there is a maximal ideal $I \subseteq \mathfrak{m} \subsetneq R$ [since R/I has a maximal ideal]. We have a $K_1 := R/\mathfrak{m} \supseteq F = K_0$ so that every $f \in K_0[x]$ has a root in K_1. We can repeat this construction to get $K_2 \subseteq K_3 \subseteq \dots$ with the property that every $f \in K_n[x]$ has a root in K_{n+1}. Now define

$$K = \bigcup_{n \geq 1} K_n,$$

an extension of F. One should check that K is a field (it's important that the K_i are nested); for $f \in K_e[x]$ with degree $d \geq 1$. Then f splits completely in $K_{d+e} \subseteq K$: in each extension K_{n+1}/K_n we are guaranteed a new root of f. So K is algebraically closed since

$$K[x] = \bigcup_{e \geq 1} K_e[x].$$

□

Definition 4.35.2. Fix an extension K/F. The $\underline{\text{algebraic closure}}$ of F in K is

$$L = \{\alpha \in K : \alpha \text{ algebraic over } F\}.$$

Observe that $F \subseteq L \subseteq K$ is a subfield: we have $F \subseteq L$ and $0, 1 \in F \subseteq L$; if $\alpha, \beta \in L$ we have

$$[F(\alpha, \beta) : F] = [F(\alpha)(\beta) : F(\alpha)][F(\alpha) : F] \leq [F(\beta) : F][F(\alpha) : F] < \infty$$

because α, β are algebraic over F. So all $\gamma \in F(\alpha, \beta)$ are algebraic over F; in particular, $\alpha \pm \beta, \alpha\beta, \alpha^{-1}$ (if $\alpha \neq 0$) are all algebraic.

Let K be an algebraically closed extension of F. Let $\bar{F}$ be the algebraic closure of F in K. It's a fact that $\bar{F}$ is unique up to an isomorphism that fixes F. So we call $\bar{F}$ *the* algebraic closure of F.

Remark 4.35.3. One can show that $\bar{\mathbb{Q}}$ exists without Zorn's lemma, because every $\alpha \in \bar{\mathbb{Q}}$ is a root of some $f \in \mathbb{Q}[x]$; enumerate the irreducibles of $\mathbb{Q}[x]$ and repeatedly take splitting fields (there are only countably many irreducibles).

5 Algebraic Geometry

5.36 Nov 26, 2018

There won't be so much geometry today.

Theorem 5.36.1 (Hilbert's Nullstellensatz – weak form)**.** *If F is algebraically closed, then the maximal ideals of the ring $F[x_1, \dots, x_n]$ are precisely $\langle x_1 - a_1, \dots, x_n - a_n\rangle$ with $a_i \in F$.*

Note that $\langle x_1 - a_1, \dots, x_n - a_n\rangle$ are clearly maximal ideals; the content of the theorem is that all the maximal ideals are of this form. Observe that this gives a bijection between maximal ideals of $F[x_1, \dots, x_n]$ and tuples in F^n.

Also, this theorem is not necessarily true when F is not algebraically closed (even in one variable, and $F = \mathbb{Q}$).

Corollary 5.36.2. *For F algebraically closed, and fixed $f_1, \dots, f_r \in F[x_1, \dots, x_n]$, then*

$$\langle f_1, \dots, f_r\rangle = \langle 1\rangle \iff \text{there is no } a \in F^n \text{ such that } f_1(a) = \cdots = f_r(a) = 0$$

Proof. The forward direction is easy, because if there are $g_1, \dots, g_r$ so that $g_1 f_1 + \cdots + g_r f_r = 1$, and the $f_i(a) = 0$ for all $i \in [r]$, then $0 = 1$.

For the backward direction, suppose that $\langle f_1, \dots, f_r\rangle \subsetneq \langle 1\rangle$, then $\langle f_1, \dots, f_r\rangle \subseteq \mathfrak{m}$. But the weak Nullstellensatz tells us that $\mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n\rangle$. In particular, we have

$$f_i = \sum_{j=1}^{n} g_{i,j}(x_j - a_j)$$

so $f_i(a) = 0$ for all i. □

We'll prove the theorem after some lemmas:

Lemma 5.36.3 (Artin-Tate)**.** *Let $A \subseteq B \subseteq C$ be commutative rings. Assume*

a) A is Noetherian

b) C is a finitely generated A-algebra

c) C is a finitely generated B-module.

Then B is a finitely generated A-algebra.

Proof. Take $x_1, \dots, x_m$ that generate C as an A-algebra, and $y_1, \dots, y_n$ that generate C as a B-module. We have

$$x_i = \sum_{j=1}^{n} b_{i,j} y_j$$

with $b_{i,j} \in B$, and

$$y_i y_j = \sum_{k=1}^{n} b_{i,j,k} y_k$$

with $b_{i,j,k} \in B$. Let $B_0 \subseteq B$ be the A-algebra generated by the $b_{i,j}$ and $b_{i,j,k}$. Note that B_0 is Noetherian, because $B_0 = A[b_{i,j}, b_{i,j,k}]$, which is a quotient of $A[x_{i,j}, x_{i,j,k}]$, which is Noetherian by the Hilbert basis theorem (Theorem 2.16.8), since A is also Noetherian.

We have that C is generated as an A-algebra by $x_1, \dots, x_m$, and hence it is generated as a B_0 module by $y_i, \dots, y_n$. Because $B \subseteq C$ and B_0 is Noetherian, then B is a finitely generated B_0-module, so B is a finitely generated A-algebra. □

Theorem 5.36.4 (Zariski's Lemma)**.** *Let K/F be a field extension such that K is a finitely generated F-algebra. Then K is a finite extension of F.*

Remark 5.36.5. It is important that K is a field. Observe that $F[x]$ is not a field; it's a finitely generated F-algebra, but it has infinite dimension as an F-vector space.

Being a finitely generated F-algebra is in general very different from being a finitely generated F-vector space. But when K is a field then it's the same.

Proof of Theorem 5.36.4. We have $K = F[x_1, \dots, x_n]$ for some $x_i \in K$. Observe that if the x_i are all algebraic over F, then $K = F[x_1, \dots, x_n]$ is a finite extension of F.

Otherwise, there is an r such that (perhaps after reordering):

- $x_1, \dots, x_r$ are algebraically independent over F (that is, $F(x_1, \dots, x_{i-1})(x_i)$ is transcendental over $F(x_1, \dots, x_{i-1})$ for all $i \in [r]$).
- $x_{r+1}, \dots, x_n$ are algebraic over $F(x_1, \dots, x_r)$.

This number r is well defined (it is called the transcendence degree of F).

Secretly, we should be looking for a contradiction (otherwise K would not be finite dimensional). So define $L = F(x_1, \dots, x_r)$. Observe that K is a finite extension of L, and K is a finitely generated F-algebra (by assumption). Thus Artin-Tate says that $L = F(x_1, \dots, x_r)$ is a finitely generated algebra over F, say with generators $f_1/g_1, \dots, f_m/g_m$ with $f_i, g_i \in F[x_1, \dots, x_r]$ relatively prime.

If $\pi \in F[x_1, \dots, x_r]$ is an irreducible dividing a denominator of some $\alpha \in L$, then $\pi | g_1 \dots g_m$. This contradicts the fact that $F[x_1, \dots, x_r]$ has infinitely many irreducibles up to units. □

We are now able to prove the weak Nullstellensatz.

Proof of Theorem 5.36.1. Fix a maximal ideal $\mathfrak{m} \subseteq F[x_1, \dots, x_n]$, and consider $F' = F[x_1, \dots, x_n]/\mathfrak{m}$ as an extension of F. Here F' is a field and is finitely generated as an F-algebra. By Zariski's lemma F/F' is a finite extension and is hence algebraic. Because F is algebraically closed, we have $F' = F$. So $F[x_1, \dots, x_n]/\mathfrak{m} = F$, and we have the quotient map

$$\varphi \colon F[x_1, \dots, x_n] \to F[x_1, \dots, x_n]/\mathfrak{m} = F$$

which is a homomorphism of F-algebras. If $a_i := \varphi(x_i) \in F$ for all i, we have $\varphi(x_i - a_i) = 0$, and so $\mathfrak{m} = \ker \varphi \supseteq \langle x_1 - a_1, \dots, x_n - a_n \rangle$, which is a maximal ideal. So $\mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. □

5.37 Nov 28, 2018

Last time we talked about Hilbert's Nullstellensatz (at least, its weak form):

Theorem 5.37.1. *If F is algebraically closed, then the maximal ideals of $F[x_1, \ldots, x_n]$ are $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$ with $a_i \in F$.*

What if F is not algeraically closed? Let $\bar{F}$ be an algebraic closure of F. For $a \in \bar{F}^n$, we get a homomorphism $\varphi_a\colon F[x_1, \ldots, x_n] \to \bar{F}$ given by $f \mapsto f(a)$. This homomorphism is an homomorphism of F-algebras. The image of φ_a is $F[a_1, \ldots, a_n] \subseteq \bar{F}$. Because the a_i are all algebraic (they're in $\bar{F}$), the kernel of φ_a is a maximal ideal of $F[x_1, \ldots, x_n]$.

We won't prove it, but it's a fact that all maximal ideals are of this form. The proof uses Zariski's lemma; it's the same idea as last time. But note that different $a \in \bar{F}^n$ may give the same ideal $\ker \varphi_a$ (it's not a bijection anymore). For example, $a = i$ or $a = -i$ give homomorphisms $\mathbb{R}[x] \to \mathbb{C}$ given by $f(x) \mapsto f(a)$; they both have kernel $\langle x^2 + 1\rangle$.

Let F be a field. We'll give two key definitions:

Definition 5.37.2. For a set $S \subseteq F[x_1, \ldots, x_n]$, its vanishing locus is

$$\mathbf{V}(S) := \{a \in F^n \colon f(a) = 0\, \forall f \in S\}.$$

If I is the ideal of $F[x_1, \ldots, x_n]$ generated by S, then $\mathbf{V}(S) = \mathbf{V}(I)$. Also, observe that it usually suffices to consider finite S, because the ideal generated by S is finitely generated (Hilbert basis theorem; see Theorem 2.16.8). Dummit and Foote uses different notation; they call this set $Z(S) := \mathbf{V}(S)$.

A subset of F^n is an algebraic set if it is $\mathbf{V}(S)$ for some S.

Definition 5.37.3. For a set $X \subseteq F^n$, define the ideal

$$\mathbf{I}(X) := \{f \in F[x_1, \ldots, x_n] \colon f(a) = 0 \forall a \in X\}.$$

Let R be a commutative ring, and let $I \subseteq R$ be an ideal. The radical of I is

$$\operatorname{rad}(I) := \{f \in R \colon f^n \in I \text{ for some } n \geq 1\}.$$

You can check it's an ideal. Also $I \subseteq \operatorname{rad}(I)$. We say I is radical if $\operatorname{rad}(I) = I$. For example, prime ideals are radical, and intersections of radical ideals are radical.

Observe that $\mathbf{I}(X)$ is radical, since if $f^n \in \mathbf{I}(X)$, then $(f(a))^n = 0$ for all $a \in X$; because we are in a field $f(a) = 0$ and $f \in \mathbf{I}(X)$.

Let I be an ideal. Then consider $\mathbf{I}(\mathbf{V}(I))$. It's easy to show that $I \subseteq \mathbf{I}(\mathbf{V}(I))$. Also, $\mathbf{I}(\mathbf{V}(I))$ is a radical ideal so we can say more; $\mathbf{I}(\mathbf{V}(I)) \supseteq \operatorname{rad}(I)$.

Theorem 5.37.4 (Hilbert's Nullstellensatz)**.** *If F is algebraically closed and $I \subseteq F[x_1, \ldots, x_n]$ is an ideal, then*

$$\mathbf{I}(\mathbf{V}(I)) = \operatorname{rad}(I).$$

Proof. This is called the Rabinowitsch trick. We only need to prove $\mathbf{I}(\mathbf{V}(I)) \subseteq \operatorname{rad}(I)$. Take any non-zero $f \in \mathbf{I}(\mathbf{V}(I))$.

Define $g := 1 + x_{n+1} f \in F[x_1, \ldots, x_{n+1}]$. Let $J \subseteq F[x_1, \ldots, x_{n+1}]$ be the ideal generated by g and I. Observe that $\mathbf{V}(J)$ is empty, because if $(a_1, \ldots, a_n, a_{n+1}) \in \mathbf{V}(J) \subseteq F^{n+1}$, then $f(a_1, \ldots, a_n) = 0$ because $f \in I \subseteq J$, also $g = 1 + a_{n+1} f(a_1, \ldots, a_n) = 0$, which is a contradiction.

Weak Nullstellensatz says that $J = \langle 1 \rangle = F[x_1, \dots, x_{n+1}]$ (otherwise, $J \subseteq \mathfrak{m} = \langle x_1 - a_1, \dots, x_{n+1} - a_{n+1} \rangle$ and $(a_1, \dots, a_{n+1}) \in \mathbf{V}(J)$). In particular, this says that

$$1 = hg + \sum_{i=1}^{m} h_i b_i$$

with $h, h_i \in F[x_1, \dots, x_{n+1}]$ and $b_i \in I$. In particular, for

$$x_{n+1} = \frac{-1}{f}$$

we have

$$1 = 0 + \sum_{i=1}^{m} h_i \left(x_1, \dots, x_n, \frac{-1}{f} \right) b_i(x_1, \dots, x_n).$$

Clear denominators: multiplying by a large enough power of f gives

$$f^r = \sum_{i=1}^{m} \underbrace{f^r h_i \left(x_1, \dots, x_n, \frac{-1}{f} \right)}_{\in F[x_1, \dots, x_n]} b_i$$

and $b_i \in I$. Thus $f^r \in I$, and $f \in \text{rad} I$. □

Corollary 5.37.5. *Let F be algebraically closed. We have inclusion reversing bijections*

$$\begin{tikzcd} \{\text{algebraic sets in } F^n\} \arrow[r, bend left, "\mathbf{I}"] & \{\text{radical ideals of } F[x_1, \dots, x_n]\} \arrow[l, bend left, "\mathbf{V}"] \end{tikzcd}$$

Proof. We should show that $\mathbf{V}$ is surjective. This follows from the observation that $\mathbf{V}(I) = \mathbf{V}(\text{rad}(I))$ (which isn't hard to check). The Nullstellensatz says that $\mathbf{I} \circ \mathbf{V} = \text{id}$, and these two give the corollary. □

As an example of this Corollary, observe that

$$\{\text{points in } F^n\} \longleftrightarrow \{\text{maximal ideals of } F[x_1, \dots, x_n]\}$$

This is the statement of the weak Nullstellensatz.

Let F be algebraically closed. On F^n, we can define the Zariski topology: closed sets are precisely the algebraic sets in F^n. This defines a topology. If $X \subseteq F^n$ is an algebraic set, it gets a topology from F^n. From here we can define a notion of irreducible spaces (we'll talk about this more next time), and there will be a correspondence

$$\{\text{irreducible algebraic sets in } F^n\} \longleftrightarrow \{\text{prime ideals of } F[x_1, \dots, x_n]\}$$

5.38 Nov 30, 2018

Last time, we fixed an algebraically closed field F and considered an ideal $S \subseteq F[x_1, \dots, x_n]$; we defined the algebraic set

$$\mathbf{V}(S) = \{a \in F^n : f(a) = 0 \text{ for all } f \in S\},$$

and for a subset $X \subseteq F^n$, we defined the ideal

$$\mathbf{I}(X) = \{f \in F[x_1, \dots, x_n] : f(a) = 0 \text{ for all } a \in X\}$$

of $F[x_1, \dots, x_n]$. We proved the Nullstellensatz, which gave a correspondence

$$\begin{aligned} \{\text{algebraic sets in } F^n\} &\leftrightarrow \{\text{radical ideals of } F[x_1, \dots, x_n]\} \\ X &\mapsto \mathbf{I}(X) \\ \mathbf{V}(I) &\leftarrow\!\shortmid I \end{aligned}$$

which we proved using the weak Nullstellensatz, which gave a correspondence

$$\{\text{points in } F^n\} \leftrightarrow \{\text{maximal ideals of } F[x_1, \dots, x_n]\}$$

which then extended to a correspondence between all the algebraic sets and all the radical ideals.

We kept giving F^n more and more properties (topologies, morphisms), so we will ("pretentiously") denote it by $\mathbb{A}^n_F$ so we don't confuse it with the boring vector space F^n.

We want to define morphisms of $\mathbb{A}^n_F$. More specifically, let $X \subseteq \mathbb{A}^n_F$ and $Y \subseteq \mathbb{A}^m_F$ be algebraic sets.

Definition 5.38.1. A morphism from X to Y is a function $\varphi\colon X \to Y$ such that

$$\varphi(a) = (f_1(a), \dots, f_m(a))$$

for all $a \in X$, with $f_1, \dots, f_m \in F[x_1, \dots, x_n]$.

This is the category of algebraic sets over F. The main thing is that composing two morphisms is a morphism (because when you compose two polynomials it's a polynomial).

Example 5.38.2. Let $X \subseteq \mathbb{A}^n_F = F^n$. Take any $f \in F[x_1, \dots, x_n]$; the map $\varphi\colon X \to \mathbb{A}^1_F = F$ given by $a \mapsto f(a)$ is a morphism. Note that different f might give the same morphism: note that $f(a) = g(a)$ for all $a \in X$ precisely when $f - g \in \mathbf{I}(X)$, so two functions will give the same morphism precisely when they differ by a function in $\mathbf{I}(X)$.

Motivated by this we define

Definition 5.38.3. The coordinate ring of $X \subseteq \mathbb{A}^n_F$ is

$$F[X] := F[x_1, \dots, x_n]/\mathbf{I}(X),$$

which we can view as the ring of morphisms $X \to \mathbb{A}^1_F$.

Observe that $F[\mathbb{A}^n_F] = F[x_1, \dots, x_n]$, since $\mathbf{I}(\mathbb{A}^n_F) = \{0\}$. Also, the ring $F[X]$ is reduced, that is, if $a \in F[X]$ with $a^n = 0$ and $n \geq 1$, then $a = 0$; this is because $F[X]$ is a quotient by a radical ideal. Indeed, if $a^n = 0$, then $a = \bar{f}$ for $f \in F[x_1, \dots, x_n]$, so $0 = a^n = \bar{f}^n$; we have $f^n = 0 \in \mathbf{I}(X)$, which is a radical ideal so $f \in \mathbf{I}(X)$, so $a = \bar{f} = 0$.

Example 5.38.4. Let $X = \mathbb{A}^1_F$, and $Y \subseteq \mathbf{V}(y - x^3) \subseteq \mathbb{A}^2_F$. Consider the map

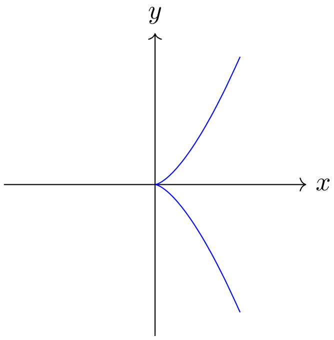
$$\begin{aligned} \varphi\colon X &\to Y \\ t &\mapsto (t, t^3) \end{aligned}$$

which is actually a morphism (in particular because $\varphi(t) \in \mathbf{V}(y - x^3)$); it has an inverse $\psi\colon Y \to X$ given by $(x, y) \mapsto x$ so X and Y are isomorphic algebraic sets. We remark that we might want to stop thinking of Y as living inside its ambient space $\mathbb{A}^2_F$ (like with manifolds, where after we have the charts we might want to forget about the ambient space).

Example 5.38.5. Let $X = \mathbb{A}^1_F$, and $Y = \mathbf{V}(y^2 - x^3) \subseteq \mathbb{A}^2_F$. The morphism

$$\begin{aligned} \varphi \colon X &\to Y \\ t &\mapsto (t^2, t^3) \end{aligned}$$

is bijective, but one can show that φ has no inverse morphism (intuitively, you'd want the map to be $(x, y) \mapsto y/x$, but this is not a polynomial). Geometrically we also see this: for $F = \mathbb{R}$ we can plot the set of points $Y \subseteq \mathbb{R}^2$:



and $(0, 0) \in Y$ is the problem because it's not smooth there.

Suppose you have a morphism $\varphi \colon X \to Y$ of algebraic sets. This induces a homomorphism of F-algebras

$$\begin{aligned} \varphi^* \colon F[Y] &\to F[X] \\ f &\mapsto f \circ \varphi \end{aligned}$$

which we call the pullback.

Here's a fact: there is a bijection

$$\{\text{morphisms } X \to Y\} \longleftrightarrow \{\text{homomorphism of } F\text{-algebras } F[Y] \to F[X]\}$$

where $\varphi \mapsto \varphi^*$ is the pullback described earlier, and the content is that one can go backwards. In particular it becomes clear that morphisms from $X \to Y$ only depend on these rings $F[X]$ and $F[Y]$ rather than the ambient spaces.

We have a contravariant functor

$$\{\text{algebraic sets over } F\} \to \{\text{finitely generated reduced } F\text{-algebras}\}$$

so that on the objects $X \mapsto F[X]$ and on the morphisms $(\varphi \colon X \to Y) \mapsto (\varphi^* \colon F[Y] \to F[X])$.

Here's a FACT: This functor is an equivalence of categories (we'll talk about this more next time). In many ways this says that the category of algebraic sets is the same as the category of finitely generated reduced F-algebras, though algebraic sets are very geometric and the F-algebras are very algebraic.

With this equivalence of categories in mind, we can ask for a way to "go back": given a finitely generated reduced F-algebra R, can you construct an algebraic set (in a reasonable way)? (Yes; come to lecture next time to see $\mathrm{Spec}_{\mathfrak{m}}(R)$)

What if you start with a general commutative ring? Can we make some sort of geometric object (even if it's not quite an algebraic set)? (Yes; come to lecture next time to see affine schemes and $\mathrm{Spec}(R)$)

5.39 Dec 3, 2018

We're trying to get a hint of schemes.

We fix a commutative ring R. We can define

$$\operatorname{Spec}(R) := \{\mathfrak{p} \colon \mathfrak{p} \text{ prime ideal of } R\}$$

and

$$\operatorname{Spec}_{\mathfrak{m}}(R) := \{\mathfrak{m} \colon \mathfrak{m} \text{ maximal ideal of } R\}.$$

Of course, $\operatorname{Spec}_{\mathfrak{m}}(R) \subseteq \operatorname{Spec}(R)$.

Prior to this we were thinking about ideals $I \subseteq F[x_1, \ldots, x_n]$ for algebraically closed F, and algebraic sets

$$X = \mathbf{V}(I) = \{a \in F^n \colon f(a) = 0 \, \forall f \in I\}.$$

We also had the coordinate ring $F[X] := F[x_1, \ldots, x_n]/\mathbf{I}(X)$, where

$$\mathbf{I}(X) = \{f \in F[x_1, \ldots, x_n] \colon f(a) = 0 \, \forall a \in X\}.$$

This coordinate ring is a finitely generated reduced F-algebra.

What is $\operatorname{Spec}_{\mathfrak{m}}(F[X])$? Recall that we had a correspondence: maximal ideals of $F[X]$ correspond to maximal ideals of $F[x_1, \ldots, x_n]$ that contain $\mathbf{I}(X)$ by some isomorphism law (the fourth one, apparently). But now the maximal ideals of $F[x_1, \ldots, x_n]$ are precisely $\mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ with $a \in F^n$, by weak Nullstellensatz. Observe that $\mathfrak{m}_a \supseteq \mathbf{I}(X)$ precisely when $a \in X$. In this sense,

$$\begin{aligned} \operatorname{Spec}_{\mathfrak{m}}(F[X]) &= X \\ \mathfrak{m}_a &\leftarrow\!\shortmid a \end{aligned}$$

For algebraic sets $X \subseteq F^n$ and $Y \subseteq F^m$, recall that a morphism $\varphi \colon X \to Y$ is a function such that $\varphi(a) = (f_1(a), \ldots, f_m(a))$, with $f_i \in F[x_1, \ldots, x_n]$. This induces a pullback homomorphism of F-algebras

$$\begin{aligned} \varphi^* \colon F[Y] &\to F[X] \\ \underbrace{g}_{Y \to \mathbb{A}^1_F} &\mapsto g \circ \varphi \end{aligned}$$

We can recover φ from φ^*.

For $a \in X$, we claim that

$$(\varphi^*)^{-1}(\mathfrak{m}_a) = \mathfrak{m}_{\varphi(a)};$$

to see this fix $a \in X$ and take $g \in F[Y]$. Then

$$\begin{aligned} g \in \mathfrak{m}_{\varphi(a)} &\iff g(\varphi(a)) = 0 \\ &\iff (g \circ \varphi)(a) = 0 \\ &\iff \varphi^*(g)(a) = 0 \\ &\iff \varphi^*(g) \in \mathfrak{m}_a \\ &\iff g \in (\varphi^*)^{-1}(\mathfrak{m}_a). \end{aligned}$$

Remark 5.39.1. In general, for a homomorphism $\psi \colon R \to R'$ of rings and $\mathfrak{m} \subseteq R'$ a maximal ideal, $\psi^{-1}(\mathfrak{m})$ need not be a maximal ideal of R; we have a map

$$R/\psi^{-1}(\mathfrak{m}) \xhookrightarrow{\bar{\psi}} R'/\mathfrak{m}$$

but rings could certainly embed into fields. On the other hand, the inverse image of a prime ideal must be a prime ideal.

If $X \subseteq F^n$ and $f \in F[X]$, one can observe that

$$X - \mathbf{V}(f) = \mathrm{Spec}_{\mathfrak{m}}(F[x]_f)$$

where the right side is the spectrum of the localization of the ring $F[X]$ with respect to f.

For R a commutative ring, we can endow the set $\mathrm{Spec}(R)$ with a topology; define for $S \subseteq R$ the set

$$\mathbf{V}(S) = \{\mathfrak{p} \in \mathrm{Spec}(R) \colon f \in \mathfrak{p} \text{ for all } f \in S\}.$$

The Zariski topology on $\mathrm{Spec}(R)$ is defined by letting the closed sets be the $\mathbf{V}(S) = \mathbf{V}(I)$ (for $I = \langle S \rangle$). Let's quickly check this:

We have $\mathbf{V}(0) = \mathrm{Spec}(R)$ and $\mathbf{V}(1) = \emptyset$;

If I and J are ideals then $\mathbf{V}(I) \cup \mathbf{V}(J) = \mathbf{V}(IJ)$ because $\mathfrak{p} \in \mathbf{V}(IJ) \iff IJ \subseteq \mathfrak{p}$, and since $\mathfrak{p}$ is prime this happens precisely when $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$. This means that $p \in \mathbf{V}(I) \cup \mathbf{V}(J)$;

We also have

$$\bigcap_{a \in A} \mathbf{V}(I_a) = \mathbf{V}\left(\sum_{a \in A} I_a\right)$$

since $\mathfrak{p} \in \cap_{a \in A} \mathbf{V}(I_a)$ if and only if $I_a \subseteq \mathfrak{p}$ for all a precisely when $\sum_{a \in A} I_a \subseteq \mathfrak{p}$, which happens precisely when $\mathfrak{p} \in \mathbf{V}(\sum_{a \in A} I_a)$.

Example 5.39.2. Let R be a local integral domain such that $\mathrm{Spec}(R) = \{0, \mathfrak{m}\}$ and observe that the closure of 0 is $\{0, \mathfrak{m}\}$.

We can endow $X := \mathrm{Spec}(R)$ with more structure that makes it more useful. In particular, we want to give it a structure sheaf $\mathcal{O}_X$: we want

- A ring $\mathcal{O}_X(U)$ for every open $U \subseteq \mathrm{Spec}(R)$, with the additional assumption that $\mathcal{O}_X(\emptyset) = \{0\}$
- For $U \subseteq V$ an inclusion of open sets, we have a restriction homomorphism $\mathrm{res}_{V,U} \colon \mathcal{O}_X(V) \to \mathcal{O}_X(U)$ with the additional property that $\mathrm{res}_{U,U} = \mathrm{id}$, and if $U \subseteq V \subseteq W$ we have $\mathrm{res}_{W,U} = \mathrm{res}_{V,U} \circ \mathrm{res}_{W,V}$
- If we have open sets $U, U_\alpha \subseteq X$ so that
$$U = \bigcup_{\alpha \in A} U_\alpha$$
and we have $f_\alpha \in \mathcal{O}_X(U_\alpha)$ such that
$$f_\alpha|_{U_\alpha \cap U_\beta} = f_\beta|_{U_\alpha \cap U_\beta}$$
for all $\alpha, \beta \in A$, then there exists a unique $f \in \mathcal{O}_X(U)$ such that $f|_{U_\alpha} = f_\alpha$ for all $\alpha \in A$.
- For $f \in R$, we also want
$$\mathcal{O}_X(X - \mathbf{V}(f)) = R_f$$
where R_f is the localization of R with respect to f.

The first two items define a presheaf. Also, one can check that there is a unique such $\mathcal{O}_X$ up to a natural notion of isomorphism. We say that $\mathrm{Spec}(R)$ with its topology and $\mathcal{O}_X$ is an affine scheme. Recall earlier

$$\{\text{algebraic sets over } F\} \longleftrightarrow \{\text{finitely generated reduced } F\text{-algebras}\}$$

sending $X \mapsto F[X]$. The inverse is given by $\mathrm{Spec}_{\mathfrak{m}}(R) \hookleftarrow R$. It turns out there is an equivalence of categories

$$\{\text{affine schemes}\} \longleftrightarrow \{\text{commutative rings}\}$$

with $\mathrm{Spec}(R) \hookleftarrow R$ and $X \mapsto \mathcal{O}_X(X)$.