1 January 9

Going to do on chalkboard because he prefers the pacing; so not going to be any notes produced by him. No final exam, quizzes every two weeks, so keep on top of things; the last quiz may be weighted more. Good idea to review linear algebra, like eigenvectors/eigenvalues, etc.

Today's lecture will be off the top of his head, got into police incident last night.

1.1 Rings Intro

Can think of a generalization of $\mathbb{Z}$, where you have an addition $+$ and a multiplication $\cdot$. We assume that $(R, +)$ is an abelian group; $\cdot$ is associative, there exists an identity 1_R, but that's it; and the distributive law $a(x+y) = ax + ay$, $(x+y)a = xa + ya$. (Don't forget about closure of the opertions!!!).

These things are completely ubiquitious: there are a lot more examples of rings than groups.
Examples:

- $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$
- polynoimal with coefficients in $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$
- $n \times n$ matrices with entries in $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$ (product is not commutative)

$$1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} \vec{a} \\ \vec{b} \end{pmatrix} \begin{pmatrix} \vec{p} & \vec{q} \end{pmatrix} = \begin{pmatrix} \vec{a}\cdot\vec{p} & \vec{a}\cdot\vec{q} \\ \vec{b}\cdot\vec{p} & \vec{b}\cdot\vec{q} \end{pmatrix}$$

In a ring, we can have $xy = 0$ even if $x, y \neq 0$, e.g. $x = y = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $R = 2 \times 2$ matrices. x is a left zero divisor, y is a right zero divisor. $x^n = 0$ is possible for $x \neq 0$. So very few things hold in all rings. But rings can do much of what we want to do in a lot of contexts: addition/subtraction, multiplication, but no division.

E.g. suppose $x^n = 0$, $x \in R$. Then there exists a multiplicative inverse for $(1 - x)$.

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots x^{n-1} + \underbrace{x^n}_{0} + \underbrace{x^{n+1}}_{0}$$

$$\begin{aligned}(1-x)(1+x+x^2+\cdots+x^{n-1}) &= (1+x+x^2+\cdots+x^{n-1}) - x(1+x+x^2+\cdots+x^{n-1}) \\ &= (1+x+\cdots+x^{n-1}) - x - x^2 - \cdots - x^{n-1} - x^n \\ &= 1 - x^n = 1\end{aligned}$$

So act similarly to what we expect, but have to be careful about commutative. Note that this is like the approximation that analysts do, where we are assuming x^n is sufficiently small... well, this is like "infinitely small", and some people in algebraic geometry actually do stuff like this.

See

$$\begin{aligned}(x+y)^2 &= (x+y)(x+y) \\ &= x(x+y) + y(x+y) \\ &= x^2 + \underbrace{xy + yx}_{\text{not same unless} xy=yx} + y^2\end{aligned}$$

So when our ring is commutative, we recover the binomial theorem we know and love.

1.2 Types of Rings (lots!)

(a). Commutative (multiplication is commutative). Algebra works as it should, but still have to deal with zero divisors. Huge field, "commutative algebra".

(b). Domains: no zero divisors $xy = 0 \implies x = 0$ or $y = 0$. Usually applies to commutative rings.

(c). Division rings: $(R^*, \cdots)$ is a group (which may or may not be commutative). [Note $R^* := R \setminus \{0\}$]

(d). Fields: $(R^*, \cdot)$ is a commutative group

Remark 1. $0 \cdot a = a \cdot 0 = 0$, $\forall a \in R$

Proof. $a + 0 \cdot a = (1 + 0) \cdot a = 1 \cdot a = a$ and so $0 \cdot a = 0$, $\forall a$, and works the same on the other side. □

Note then that $0 = 1 + (-1)$ and so $0 \cdot a = (1 + (-1))a = a + (-1)a = 0$, hence the additive inverse of the multiplicative identity, multiplied by a gives a's additive inverse as well.

Now let $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Claim: this is a field. $(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (bc + ad)\sqrt{2} \in R$. We now want to show $\frac{1}{a+b\sqrt{2}}$ exists in R. See

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in R$$

provided $a^2 - 2b^2 \neq 0$. Always true since $a^2 - 2b^2 = 0 \iff \frac{a^2}{b^2} = 2$ so $\frac{a}{b} = \pm\sqrt{2}$. We have $a + b\sqrt{d}$ as long as $\sqrt{d}$ is irrational.

What about these funny noncommutative division rings. Define $\mathbb{H}_{\mathbb{R}} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \text{ or } \mathbb{Q}\}$ where $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$ and $ji = -k$, $kj = i$, $ik = -j$. We have division:

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk)}{a^2 + b^2 + c^2 = d^2}$$

These are called the Quaternions.

A note on the axioms: some people actually define rings without the multiplicative identity, but we will always assume it has one.

Definition 1 (Nilpotent elements). $x^n = 0$ for some $n \in \mathbb{Z}^+$ ("infinitely small")

"Something going off in my pocket doesn't sound that good, but it's been that kind of day."

There are a lot of pathologies in rings. Something that holds for one might be really different in another. For example, when we drop that division axiom, things get really wonky.

1.3 Matrix rings

A matrix is an array with m rows, n columns, with entries a_{ij} in the i-th row and j-th column. We now let $a_{ij} \in R$ where R can be any ring (not just $\mathbb{Q}, \mathbb{C}, \mathbb{R}$). We call this $M_{n\times m}(R)$. The rules of algebra are the same as always, e.g.

$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} := \begin{pmatrix} a\alpha + b\beta + c\gamma \\ d\alpha + e\beta + f\gamma \end{pmatrix}$$

where the multiplication and addition is in R. This works because we don't need division in the entries of matrices, unless perhaps we are taking inverse.

Remark 2. $M_{1\times 1}(R) = R$ and not neccesarily commutative

It is surprising that we are able to say things about these matrices. We have that $M_{n\times n}(R)$ is a ring, which we normally write as $M_n(R)$ (the product of $n \times n$ matrices is $n \times n$).

Scalar matrices $\begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 0 & \alpha & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha \end{pmatrix}$ where $\alpha \in R$. This turns out to be a copy of R (isomorphic), where the identity is $I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$.

Assume that R is commutative and $A \in M_n(R)$. When does A^{-1} exist in $M_n(R)$? There is a formula for A^{-1} when $R = \mathbb{R}, \mathbb{C}, \mathbb{Q}$. If $A = (a_{ij})$ and $B = (b_{ij})$ where $b_{ij} = (-1)^{i+j} \det A_{ij}$ (A_{ij} is deleting the ith row and j-th column), then $AB = BA = \det A \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} \det A & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \det A \end{pmatrix}$ so $A^{-1} = ff$. Now, the trouble is that in linear algebra, they don't tell you what a determinant is, only how to compute it. So we will use this definition of the determinant:

Definition 2 (Determinant). if R is commutative and A is the $n \times n$ matrix with entries $a_{ij} \in R$, then

$$\det A := \sum_{\sigma \in S_n} (-1)^{\operatorname{sgn}(\sigma)} \prod_{i=1}^{n} a_{i\sigma(i)}$$

We can see if $n = 2$ and given $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, we ff

Given $A = (a_{ij})$, can define $B = (b_{ij})$ as $b_{ij} = (-1)^{i+j} \det A_{ji}$ also makes sense, so $AB = \det(A)I$ is true!

How can we prove this? Well, we saw $n = 2$, and could see an inductive proof. But we will go about it in a different way using the properties of the determinant. $\det(A)$ can be thought of as a function of the n-rows of $A = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ where v_i are row vectors. Check: swapping 2 rows sends $\det(A) \to -\det(A)$; adding a multiple of one to another doesn't change $\det(A)$; multiplying a row by a constant scales $\det(A)$ by the same constant. Now we can show there's a unique function (up to scalar) that satisfies this set of properties, and our defined det satisfies these properties. Finally, for real matrices, can use the transformations $1, 2, 3$ to put A in reduced echelon from to compute our typical formula for the det that way.

Note for those taking differential geometry, this is an example of an exterior product.

Note we haven't done anything for the inverse, but we have just looked at the determinant.

This stuff is discussed somewhat in the book, 2.3. But Nike will say more about this stuff next time.

2 January 11

2.1 Determinants

Three determinant properties ff (check overleaf and get notes from Sushrut)

Claim: these 3 properties determine det uniquely. Observation: if 2 rows are the same, then det $= 0$. Let $v_i = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}$, and e_i be the i-th coordinate vector $\begin{pmatrix} a_{i1} & \cdots & 1 & \cdots 0 \end{pmatrix}$. We note that $v_i = \sum j = 1^n a_{ij} e_j$. Then $\det(A) = \det(\sum a_{ij} e_j) = \det \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$. Using the linear property (?)

$$\det \begin{pmatrix} a_{11} e_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} + \det \begin{pmatrix} a_{12} e_2 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} + \cdots + \det \begin{pmatrix} a_{1n} e_n \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \tag{1}$$

And then repeat in the second row, and third row, etc. The only terms that will survive have the formula

$\det \begin{pmatrix} e_{\sigma(1)} \\ e_{\sigma(2)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}$ where $\sigma \in S_n$ and the coefficient (??) is the product of the a's. We have

$$\begin{aligned} \det \begin{pmatrix} ae_1 + be_2 \\ ce_1 + de_2 \end{pmatrix} &= \det \begin{pmatrix} ae_1 \\ ce_1 + de_2 \end{pmatrix} + \det \begin{pmatrix} be_2 \\ ce_1 + de_2 \end{pmatrix} \\ &= \det \begin{pmatrix} ae_1 \\ ce_1 \end{pmatrix} + \det \begin{pmatrix} ae_1 \\ de_2 \end{pmatrix} + \det \begin{pmatrix} be_2 \\ ce_1 \end{pmatrix} + \det \begin{pmatrix} be_2 \\ de_2 \end{pmatrix} \\ &= ad \det \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} - bc \det \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \\ &= ad - bc \end{aligned}$$

Expansion of det in rows and columns follows from (1) (check). Formula for inverse, adjugate etc. similar proof (check), so $AA^* = \det(A)I$ is always true, where A^* (cofactor/adjugate) is made from minors. If $\det A$ has an inverse in R^*, then A^{-1} exists in $M_n(R)$. It is also true that $\det(AB) = \det(A)\det(B)$ in general, and also follows from the three properties of the det.

These basic facts are summarized on page 95 and 96 (but probably don't do this expansion).

2.2 Ideals, quotients, and homomorphisms

Definition 3 (Ring homomorphism). If R and S are rings, a map $f\colon R \to S$ is called a proper *homomorphism* if $f\colon (R,+) \to (S,+)$ is a homomorphism of gruops, $f(xy) = f(x)f(y)$, and $f(1_R) = 1_S$.

Note the last condition: it is not free (monoid homomorphism). Basically, as before, this lets us do algebra in S the same as in R. Not $f(ax + ay) = f(ax) = f(ay) = f(a)f(x) + f(a)f(y) = f(a)(f(x) + f(y))$.

Definition 4 (Kernel of ring homomorphism). $\ker(f) := \{x \in R \mid f(x) = 0_S\}$.

So $\ker(f)$ is an additive subgroup. But multiplicatively, this is a little weird, not a monoid. Let $I = \ker(f)$. Note if $y \in R$, $x \in I$, then $yx, xy \in I$ since $f(yx) = f(y)f(x) = f(y) \cdot 0 = 0$. So I is closed under multiplication by R. Note, if $1_R \in I$, then $y \cdot 1_R \in I$ and so $y \in I \forall y$, which means $f(y) = 0 \forall y \implies f(1_R) = 0$ which is not allowed for a proper homomorphism. So $1_R \notin I$ always. Hence, I is *not* a subring of R: there is no multiplicative identity.

Note: we almost never consider the trivial ring in our statements. We want $1 \neq 0$, so 1 is invertible, and a lot of other nice things. Without excluding, a lot of our statements about rings become trivially false.

Definition 5 (Ideal). A (proper) *ideal* in a ring is a subgroup $I \subsetneq (R,+)$ such that $\forall y \in R, \forall x \in I$, $yx, xy \in I$.

Definition 6 (Quotient ring). Let R be a ring and $I \subset R$ be a proper ideal. The *quotient ring* is the set of coset R/I (under $+$) where multiplication is $(x + I)(y + I) = xy + I$ (identity is $1 + I$).

Let us check that this is well-defined: representatives for $x + I$ and $y + I$ are $x + i_1$,$y + i_2$ where $i_1, i_2 \in I$. Then $(x + i_1) \cdot (y + i_2) = xy + xi_2 + i_1 y + i_1 i_2 \in xy + I$. So the multiplication is well-defined (?? check later... do we need set inclusion the other direction? but definition?)

Example: Let S be any ring, and $R = \mathbb{Z}$. Define $f\colon \mathbb{Z} \to S$ by $f(1) = 1_S$, $f(n) = (1_S + \cdots + 1_S) = n1$, and $f(-n) = -(1_S + \cdots + 1_S)$. It is obvious this is a homomorphism (exercise). This is called the *canonical* homomorphism $f\colon \mathbb{Z} \to R$. (Note this is the only way to map $\mathbb{Z}$ to R.) There are 2 kinds of rings:

- f injective, then $f(\mathbb{Z}) \subseteq R$ and is isomorphic to $\mathbb{Z}$. We say that it has $\operatorname{char}(R) = 0$.
- f is not injective, then f contains a quotient of $\mathbb{Z}$ so R contains $\mathbb{Z}/n\mathbb{Z}$ for some $\min n > 1$ characteristic in ker.

So either $R \supseteq \mathbb{Z}$ (via f) or $R \supseteq \mathbb{Z}/n\mathbb{Z}$ for some $\min n > 1$ (via f).

In $\operatorname{char}(n)$, $f(n) = (1_S + \cdots + 1_S) = 0$ be definition. Then $nx = x + \cdots x - x(1 + \cdots 1) = x \cdot 0 = 0$. So "multiplication by n" means 0 in rings of characteristic n.

Note that if we have $\operatorname{char}(2)$, then $1_S + 1_S = 0$, so $x + x = 0 \forall x$, and so $x = -x$ (even when $x \neq 0$). This is not nice, we don't like 1 being its own inverse: this is why a lot of things in number theory say "consider all odd primes".

If $n = p =$ prime and x, y commutative, then

$$(x+y)^p = \sum \binom{p}{i} x^i y^{p-i} = x^p + y^p$$

since $\binom{p}{i}$ is divibisible by p if $0 < i < p$. Frobenius transform (??) $f \colon R \to R$, $x \mapsto x^p$ is a homomorphism for commutative R for char(p); important in number theory.

Definition 7 (Ideal generated by a set). Let R be a ring and $\{x_j\}_{j \in J}$ be a collection of elements in R. The ideal generated by J is the set of combinations of the form

$$\sum R x_j R$$

which are combinations of $\alpha x_j \beta$, $\alpha, \beta \in R$ (might be R and not proper).

Note proper ideals don't contain units (invertible elements).

If I, J are ideals, then $I \cap J$ is an ideal, $I + J = \{i + j \mid i \in I, j \in J\}$ is an ideal (not neccesarily proper). $I \cap J \supseteq IJ = \{ij \mid i \in I, j \in J\}$ is an ideal.

In general, if he gives us some random ring, a hard problem to find the ideals in it. Will usually study more simple properties in this class. There is work in classyfing rings and their ideals.

All in section 2.5 and 2.6. Will continue next time and briefly touch on homomorphism theorems, same as before (read it).

3 January 16

Wrapping up stuff from last time.

(a). The det when the characteristic is 2. We assume last time $1 \neq -1$. But we can actually just reword things. Recall $\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod a_{i\sigma(i)}$. If row i, row j are the same, then σ term is the same as the term for $\sigma\tau$, $\tau = (ij)$. So each term appears twice, which is 0 in char $= 2$ as well.

(b). Define ideals as sets (additive subgroups) that are multiplicatively closed by elements of R on both sides: $rI \subseteq I, Ir \subseteq I, r \in R$. Note, we also hvae left and right ideals, i.e. $rI \subseteq I$ or $Ir \subseteq I$, however, these are not kernals of homomorphisms. But they will make an appearance studying noncommutative rings. If you want to make quotients, need two-sided ideals.

Note, if R is a commutative ring, R is a field $\iff$ there are no nontrivial ideals.

Proof. Suppose R is a field, $I \subset R$ is an ideal, and $I \neq \{0\}$. If $a \in I$, $a \neq 0$. $a^{-1} \in R$ (since it is a field), so $1 = a^{-1} \cdot a \in I$ hence $I = R$.

If R has no zero ideals, then R is a field. Pick $a \neq 0$, $aR =$ ideal, so $x(aR) = xaR = a(xR) \subseteq aR \implies aR = R \implies$ there is a b with $ab = 1$. □

Corollary 1. *If R is a field, $f \colon R \to S$ a homomorphism, then f is injective*

Proof. $\ker f = \{0\}$ □

3.1 Principal Ideals

Let us assume that R is commutative. $\forall a \in R$, aR is an ideal. This is called a principal ideal generated by a. $aR = R \iff a$ is a unit. In general, a not a unit $\implies aR \subsetneq R$ (a proper ideal). Example: $R = \mathbb{Z}$, $R/aR \cong \mathbb{Z}/a\mathbb{Z}$.

Let $R = \mathbb{R}[x] =$ polynomials with real coefficients. Let $a = x^2 + 1$ and $I = aR =$ multiples of $x^2 + 1$. Claim is that $R/I \cong \mathbb{C}$.

Proof. Pick $p(x) \in \mathbb{R}[x] = R$. Using long division of polynomials $p(x) = \underbrace{q(x)(x^2+1)}_{\in I} + \alpha x + \beta$ "Long division of polynomials is something everyone should be able to do. It's like long division of numbers, but worse."

We want to show the cosets of R/I are labelled by $\alpha I+\beta$, $\alpha,\beta\in\mathbb{R}$ (bijective correspondance). See $\alpha x+\beta+I=\alpha' x+\beta'+I \implies \alpha=\alpha',\beta=\beta'$ since $\alpha x-\alpha' x+\beta-\beta'\in I \implies \alpha'' x+\beta''\in I=(x^2+1)R$ and we have a linear equaling a quadratic, so $\alpha''=\beta''=0$.

Multiplication: $(\alpha x+\beta)\cdot(\alpha' x+\beta')=$ coset of gh (definition) $=$ coset of $\alpha\alpha' x^2+\alpha\beta' x+\beta\alpha' x+\beta\beta' \equiv -\alpha\alpha'+\alpha\beta' x+\beta\alpha' x+\beta\beta'$ since $x^2+1\in I \implies x^2=-1+I$. But this looks like multiplication in $\mathbb{C}$. In particular, $(x+I)(x+I)=-1$, so $(x+I)=i$ since $i^2=-1$. And $\mathbb{R}[x]/I$ contains $\mathbb{R}$ via $0x+\beta$. □

$\mathbb{C}=\mathbb{R}+i\mathbb{R}$, $i^2=-1$, where $(\alpha i+\beta)(\alpha' i+\beta')=$ same formula as before. So we have recovered $\mathbb{C}$ ("the correct definition of $\mathbb{C}$"):

$$\mathbb{C}=\frac{\mathbb{R}[x]}{I},\quad I=(x^2+1)\mathbb{R}[x]$$

Notation: $(a)=aR=$ the principal ideal generated by a.

Ex. $\mathbb{Q}[x]$ and $I=(x^3-2)$. Cosets are repsented by polynomials of degree ≤ 2, ax^2+bx+c (long divison). We have $(ax^2+bx+c)(a'x^2+b'x+c)=aa'x^4+(\dots)x^3+\cdots=aa'x^3x+(\dots)x^3+\cdots$, have to do long division on this to get a quadratic representative. We have $x^3-2\in I \implies 2+I=x^3+I$. In R/I we have $\overline{2}=\overline{x}^3$. So our polynomial becomes $aa'(2)x+(\dots)2+\cdots$. We get $\mathbb{Q}$ with a solution of $x^3-2=0$ i.e. $\sqrt[3]{2}$??? Note $\mathbb{Q}\hookrightarrow\mathbb{Q}[x]\to\mathbb{Q}[x]/I$ (the first map is to the constant polynomial). Note that since the whole map is injective, we have that $\mathbb{Q}[x]/I$ contains $\mathbb{Q}$. So we have enlarged $\mathbb{Q}$ by adding solutions to an equation which did not have solutions in $\mathbb{Q}$. We have an algebraic definition $\sqrt[3]{2}$, namely $\overline{x}$ with $(\overline{x})^3=2$. So technically, we think of all cube roots of 2 as the same. It's just some symbol. It isn't until Galois theory that we might consider them different, because then we're thinking of the symmetries of our roots, and we'll see taking the complex conjugate fixes 1 root and swaps 2, so there is a difference; but not right now.

Again, let $R=\mathbb{Q}[x]$. Consider $f\colon R\to\mathbb{C}$ by $p(x)\mapsto p(\alpha)$, $\alpha\in\mathbb{C}$ is fixed. Is this injective? What is $\ker(f)$? Well, $\ker(f)=\{p(x)\mid p(\alpha)=0\}$. Theorem (deep): $\ker(f)=0$ for almost all α. We need α to be a root of this polynomial. There are only countably many α for which $\ker\neq 0$ nonzero ($\mathbb{Q}[x]$ is countable, but $\mathbb{C}$ is not). These α are called *algebraic*. Generic α are called *transcendental*: not the root of any rational equation. Despite the fact that almost all numbers are transcendental, it is quite hard to prove that a specific transcendental. $e,\pi,\dots$ are transcendental, but no straight forward proof, and most numbers you could think of are algebraic. (Note that zeros of $\mathbb{Z}[x]$ are the same: just scale by leading coefficient; if monic polynomials, so leading coefficient is 1, different and called algebraic integers).

Remark 3. $\ker(f)$ does not determine α. E.g. $\alpha_1=\sqrt[3]{2}\in\mathbb{R}$, $\alpha_2=\xi\sqrt[3]{2}$, $\alpha_3=\xi^2\sqrt[3]{2}$ where $\xi=e^{2\pi i/3}$. The kernel in all 3 cases is $I=(x^3-2)$ (not obvious). We will get to this in more detail, something about polynomial irreducible.

Proof. Suppose $p(x)$ is such that $p(\alpha_i)=0$. $p(x)=q(x)(x^3-2)+r(x)$ where $r(x)\in\mathbb{Q}[x]$ has degree ≤ 2. $p(\alpha)=0 \implies q(\alpha)\cdot 0+r(\alpha)=0 \implies r(\alpha)=0$. Have to check that none of these α satisfy rational polynomials of degree ≤ 2 (details are an exercise: can't be linear, and if quadratic, need them to be conjugate, but will see not in $\mathbb{Q}[x]$). □

Generic technique in number theory. Start with a polynomial, and make a quotient ring, etc.

Note the fundamental theorem of algebra says roots of $\mathbb{C}[x]$ are in $\mathbb{C}$ ("algebraically closed"). But recall from our homomorphism, our roots of $\mathbb{Q}[x]$ are in $\mathbb{C}$.

Also note that behind all of this is the assumption we are in a field of characteristic 0. If we don't have this, long division becomes a bit more complicated, but we will talk about this later.

3.2 Fundamental theorem of homomorphisms

Same as for gruops (preimage, etc.). Read it in the book (2.7).

3.3 Fractions

How do we get from $\mathbb{Z}$ to $\mathbb{Q}$. What is the construction $\mathbb{Z}\rightsquigarrow\mathbb{Q}$? Perhaps we define it by $\{\frac{a}{b}\mid a,b\in\mathbb{Z},b\neq 0\}$ Problem is that $\frac{a}{b}$ is not a unique representative! What if we try $\gcd(a,b)=1$. But this assumes existence of gcd $\iff$ unique factorization of $\mathbb{Z}$ (nontrivial). Better: $\frac{a}{b}=\frac{c}{d}\iff ad=bc$.

$$\mathbb{Q}:=\{(a,b)\mid a,b\in\mathbb{Z},b\neq 0\}/\sim$$

where $(a, b) \sim (c, d) \iff ad = bc$. Check: rules of arithmetic apply (postpone for now). "When you're doing fractions in grade 4, assuming unique factorization." "One of the earliest times I realized I liked math was when someone told me that we are using unique factorization in our definition of fractions."

Goal: R is commutative, integral domain (no zero divisors), construct the "smallest" field containing R ($\mathbb{Z}$ gives $\mathbb{Q}$). Let $\mathbb{Q} := \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}/\sim$ where $(a, b) \sim (c, d) \iff ad = bc$, which contain rules of arithmetic.

Theorem 1. *S is a field, $\exists! \iota\colon R \hookrightarrow S$. If T is any other field with $j\colon \mathbb{R} \hookrightarrow T$, then $\exists! f$ which makes*

$$ffcommutativediagram$$

(basically $f\colon \iota = j$ and $f\colon S \to T$; f is injective because any map between two fields has $\ker(f) = 0$).

This is the universal property that defines the ring of fractions.

Thursday quiz will be up until ideals. Review linear algebra: matrices will be on the quiz. Quiz will probably be the second half of the class.

4 January 23

Because of the snow and bus strikes, quiz is just gonna be the same day as quiz 2, unfortunately after add/drop deadline; it will be the full class.

4.1 Fractions over a commutative domain

Recall we were look at fractions last time. Let R be a commutative, integral domain. Want to embed R into the smallest possible field S. Start with $R \times R$, consider pairs (a, b), $b \neq 0$ modulo the relation $(a, b) \sim (c, d) \iff ad = bc$ (motivation: $\frac{a}{b} = \frac{c}{d}$). It is easy to check this is an equivalence relation. Then $S = R' \times R'/\sim$ (second coord nonzero subset), which are the pairs (a, b), $(0, 0)$ is the class of $(0, b)$??? I thought we excluded. Case work is exactly like fractions: $(a, b) + (c, d) = (ad + bc, bd)$ etc. $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, $1 = (1, 1)$, $0 = (0, 0)$.

Ex. $(a, b) \sim (p, q) \iff aq = bp$ and $(c, d) \sim (r, s) \iff cs = dr$. $(a, b) + (c, d) = \frac{ad+bc}{bd} = (ad + bc, bd)$ and $(p, q) + (r, s) = \frac{ps+rq}{qs} = (ps + rq, qs)$... are these equal? ff computing.

Note each nonzero elemenet is invertible, namely $(a, b)^{-1} = (b, a)$. So $R \hookrightarrow S$ via $(a, 1) \leftrightarrow a \in R$ thus we have found a field S plus an injective map $R \hookrightarrow S$. Claim: if $\phi\colon R \hookrightarrow T$ is an injective map, T a field, then there exists a unique $\psi\colon S \to T$ such that the diagram ff (R to S via ι, S to T via ψ, R to T via ϕ) commutes.

Proof. It is clear that if ψ exists then $\psi(a, 1) = \phi(a)$. What about $\psi(a, b)$? Note $(a, b) = (a, 1) \cdot (1, g) \implies \psi(a, b)$ has to satisfy $\psi(a, b) = \psi(a, 1) \cdot \psi(1, b) = \phi(a)\phi(b)^{-1}$ since this is an element that satisfies the multiplicative relation $(b, 1)(1, b) = (b, b) = (1, 1)$, the multiplicative identity. So $\psi(1, 1) = 1 \iff \psi(b, 1)\psi(1, b)1$, hence psi is defined uniquely by $\psi(a, 1) = \phi(a)$, $\psi(1, b) = \phi(b)^{-1}$ (which exists since T is a field). We have to check this is a well-defined homomorphism, but it is an easy calculation. □

Thus, S is the smallest field containing R.

If $R = \mathbb{Z}$, then $S \cong \mathbb{Q}$. If $R = \mathbb{Z} + \mathbb{Z}[i]$, $S \cong \mathbb{Q}[i]$, where $(a + bi)^{-1} = \frac{a-bi}{a^2+b^2} \in \mathbb{Q}[i]$.

Remark 4. S is an abstract field, not necessarily subfield of $\mathbb{C}$ just because we think of R as a subfield of $\mathbb{C}$. But since there is some ϕ from $R \hookrightarrow \mathbb{C}$ (so R lives inside $\mathbb{C}$), then the commutative diagram says that S lives inside $\mathbb{C}$.

ψ need not be injective (?), but ϕ is minimal because it comes from $\psi \circ \iota$... the existence and uniqueness requires ψ or ϕ??? to be injective... worth pondering. But anyway, we get for free that these are injective because mapping into fields, and any homomorphism into fields is injective.

4.2 Polynomial rings

What is a polynomial, e.g. with real coefficients? In calculus, we think of it as a function $f\colon \mathbb{R} \to \mathbb{R}$ where

$$f(X) = \sum_{n=1}^{m} a_n X^n = a_m X^n + \cdots + a_0,\ a_i \in \mathbb{R}$$

We pick some $X \in \mathbb{R}$, we get value $f(X) \in \mathbb{R}$ and can get a graph.

This is *not* what a polynomial is in algebra! Polynomials are not functions. Let $R = \mathbb{Z}/3\mathbb{Z}$. Think of the function $X^2 \colon R \to R$. Then $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 1$. What about X^3? then $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 2$. So as a function, X^3 and X are the same! This does not look like a good thing: we want the notion of the degree of a polynomial to be somewhat sensible, but if we just think of this as a function, we don't really get this. So we *cannot* think of polynomials as functions.

X is not a variable, with some domain. For us X is just a placeholder. So if R is commutative, we define

Definition 8 (Polynomial with coefficients in R). A polynomial with coefficients in R (commutative) of degree m is a sequence $(a_0, a_1, \dots, a_m) \in R \times R \times \cdots \times R$ ($m+1$ times) with $a_m \neq 0$. Morally: $a_m X^m + \cdots + a_0 = f(X)$ (we use the X notation, with the provision that X is a symbol).

The space of polynomials with coefficients in R is the set of bounded sequences $(a_0, a_1, \dots)$ meaning $a_r = 0$ for all r sufficiently large (only finitely many nonzero terms).

We have to make this into a ring. We do addition via coordinates: $\sum a_i X^i = \sum b_i X^I = \sum (a_i + b_i) X^i$. Our multiplication is done how we would expect: $(a_0, \dots)(b_0, \dots) = (c_0, \dots)$ or $(\sum a_i X^i)(\sum b_i X^i) = \sum c_i X^i$ which is obtained by multiplying LHS and collecting powers of X, $c_n = \sum_{p+q=n} a_p b_q$. This defines the multiplicative identity $1 = (1, 0, \dots) = 1X^0$. We can check distributive, but it is routine. This comes with an injective map $\iota \colon R \to \text{Polynomials} = R[X]$ by $r \mapsto (r, 0, \dots)$. So $R =$ constant polynomials (R is a ring of constants).

The fundamental property of $R[X]$: suppose we are given a homomorphism $\phi \colon R \to S$ for some ring S (S is unrestricted). We can think of $\phi(r) \in S$; this means constants are moved inside S (ϕ may not be injective). Now, if $s \in S$ is any element, $f(X) \in R[x]$ is a polynomial, we can define the value of f at $X = s$ via $a_0 + a_1 X + \cdots + a_m X^m \mapsto f(s) = \sum \phi(a_i) s^i \in S$. We get a homomorphism (!) $R[X] \to S$, $X \mapsto s \in S$ (! is both surprising and unique).

We are allowing the domain of our function to really be anything that can be mapped to from R via a homomorphism (otherwise we don't end with a homomorphism); unlike calculus, which normally restricts by what the coefficients were. Now domain is very dependant on $\phi \colon R \to S$. By not specifying what X is, it represents any ring.

The fundamental example is $R = \mathbb{Z}$, $f(X) \in \mathbb{Z}[X]$. Let S be any commutative ring that comes with a homomorphism $\mathbb{Z} \to S$, thus for any $s \in S$, we have an evaluation map $\mathbb{Z}[X] \to S$ by $X \mapsto s \in S$. In particular, this applies when $S = \mathbb{Q}, \mathbb{Z}/p\mathbb{Z}$ for p prime. So a polynomial with integer coefficients can be evaluated at rational numbers, we well as any $x \in \mathbb{Z}/p\mathbb{Z}$ for any p. This is weird: we don't normally think of polynomials like this, normally evalue at $\mathbb{R}$. The study of these polynomials is algebraic geometry. Big themes in modern number theory is if we think of a polynomial with these extended values, we can patch together the values on $\mathbb{Z}/p\mathbb{Z}$, we can say something about the values in $\mathbb{Q}$. This is a subject called arithmetic geometry.

Last time, we saw examples of this when $f(X) \in \mathbb{Q}[X]$, and we can evaluate this at $\alpha \in \mathbb{C}$, and we get a homomorphism $\mathbb{Q}[X] \to \mathbb{C}$ where $X \mapsto \alpha$. If it was injective, then α is transcendental, if it had a nonzero kernel, then it was algebraic, i.e. there exists some $f(X)$ in $\mathbb{Q}[x]$ with $f(\alpha) = 0$ ($f \in \ker$) and α satisfies some algebraic equation $f(X) = 0$.

Ex. $R = \mathbb{Q}[X]/(f(X))$ where $I = f(X) =$ multiples of $f(X)$. If R a field, then $\exists \phi \colon R \to T \iff \exists t \in T$ such that $f(t) = 0$. Reason: $f(X) = \sum a_n X^n \in I$. In R/I have $\sum a_n \overline{X}^n = 0$ ($\overline{X}$ is the image of X in R). So if there's a homomorphism $\psi \colon R \to T$ then $t = \psi(\overline{X})$ has to satisfy $\sum \psi(a_n) t^n = 0$. Think about this a little, says something about roots of polynomials. Near the guts of Galois theory. Read up in the textbook, and we will talk about it next time.

5 January 25

5.1 More polynomials

In all of this, R is a commutative ring, and $R[x]$ are polynomials in X. Polynomials will be identified as a sequence of coefficients. This X is not anything other than a symbol, just keeps track of multiplication and addition.

The fundamental property we discussed last time: given some $\phi \colon R \to S$ which is a homomorphism, and some $s \in S$, then $\exists!$ extension of ϕ to $R[x] \to S$ such that $X \mapsto s$. This is the evaluation homomorphism at $s \in S$. This is given by $\sum_i a_i X^i \mapsto \sum \phi(a_i) s^i$.

This is not as weird as it looks. For example, $\phi \colon \mathbb{Q} \hookrightarrow \mathbb{R}$, think of rational coefficients as complex numbers. Can also take $\phi \colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$: in this case, if $p = 5$ and $f(X) = X^2$ and $s = [2]$, then $1 + X \mapsto 1 + [2] = [3]$ (wait, why did he say $f(X)$?). So we evaluate $f(X)$, then reduce mod p. Another example: $\phi\colon \mathbb{C} \to \mathbb{C}$ where $z \mapsto \bar{z}$. So $\sum a_i X^i \mapsto \sum \bar{a}_i X^2$. so ϕ-evaluation at s gives $\sum \bar{a}_i s^i$.

You have to be careful you know what ϕ is in the background. Consider $R = \mathbb{Q}[X]/I$ where $I = (X^2+1)$. By long division, our ring is just $\mathbb{Q} + \mathbb{Q}x$ where $x = X + I$. Multiplication comes $0 = x^2 + 1 = (X+I)^2 + 1 = X^2 + 1 + I = I$ (what is this showing??) To get ϕ from $R \to \mathbb{C}$ we have to send x to some $s \in S$ such that $s^2 + 1 = 0$. We have $x^2 + 1 = 0 \in R$ so $\phi(x)^2 + \phi(1) = 0$ in $\mathbb{C}$, so we need $s \pm i$ (both are valid)... (something something about the ideal, I'm confused what he is showing again). We can also send $\mathbb{Q}[X] \hookrightarrow \mathbb{C}$ with $X \mapsto \pi$ or $X \mapsto e$; since these are transcendetal, not the root of any polynomial, so not in any ideal. So ker $= 0$ in both cases.

5.1.1 More variables

We can extend this to more than 1 variable. Start with R, form $R[X] = S$. From $S[Y]$" = "$R[X,Y]$, because $S[Y] = \sum a_i Y^i$ where $a_i \in R[X]$. Expand out to get $\sum a_{ij} X^i Y^j, a_{ij} \in R$. We an repeat to get $R[X_1, \ldots, X_n]$. Fact: if $\sigma \in S_n$ is any permutation, then $\exists!\ \phi\colon R[X_1, \ldots, X_n] \to R[X_1, \ldots, X_n]$ where $X_i \mapsto X_{\sigma(i)}$, which is the identity on R (constant terms don't change... or coefficients don't change???). Proof: in the text (symbole pushing + uniqueness of 1 variable polynomial maps).

Same universal property as before: given $\phi\colon R \to S$, $s_1, s_2, \ldots, s_n \in S$, $\exists!$ extension $R[X_1, \ldots, X_n] \to S$ which sends $X_i \mapsto s_i$. Same as before, just evaluating an n-tuple.

Note the variables X_i, X_j commute, in the definition (is it??).

Multivariable polynomials look a little odd. The monomoial of (multi) degree $\vec{a}$ is $\sum c_{\vec{a}} \prod X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$ where $\vec{a} = (a_1, \ldots, a_n)$ is an n-tuple of non-negative integers, and $c_{\vec{a}} \in R$. The (total) degree of $\vec{a}$ is $\sum a_i$.

It is quite helpful to look at the proofs in the book to understand how proofs work with these polynomials. For example, $X^2 + 2XY + Y^2 = X^1(2Y) = X^0 Y + X^2 1 \in R[Y][X]$.

5.1.2 Division of one variable polynomials

Let's stick to the case of one variable for now.

$$f(X) = \sum_{i=0}^{n} a_i X^i, \quad a_n \neq 0$$

a_n is called the leading coefficient. $f(X)$ is called *monic* if $a_n = 1$. n is called the degree of f, deg: $R[X] \to$ non-negative integers.

Fact: if R is a domain, $\deg(f) + \deg(g) = \deg(fg)$, since $(a_n X_n + \cdots)(b_m X^m + \cdots) = a_n b_m X^{n+m} + \cdots$ lower coefficient, and $a_n b_m \neq 0$ since it is a domain.

Corollary 2. *If D is a domain, so is $D[X]$ and $D[X_1, \ldots, X_n]$.*

Now we come to long division in a ring. Assume that R is a domain and commutative as always. Given $f(X), g(X)$ in $R[X]$, want to divide $f(x)$ by $g(x)$ and get a remainder of degree less than g. We want $f(X) = q(X)g(X) + r(X), \deg(r) < \deg(g)$. This is *not* always possible. E.g. $R = \mathbb{Z}, f(X) = X^3 + X + 1, g(X) = 2x + 1$. Then $q(X)g(X) = (2X+1)(a_m X^m + \cdots) = 2a_m X^{m+1} + \cdots$. $\deg(r) = 0$ is $r(X)$ is a constant. So $q(x)g(x) + r(x)$ has a leading cofficient greater than 1, so not equal (Napkin does it again). It will be possible in a field.

What is true in general is the following:

Theorem 2 (Long Division). *Let R be a commutative ring, and $f, g \in R[x]$. Let $g(X) = b_m X^m + \cdots + b_0, b_m \neq 0$. Then $b_m^k f(X) = q(X)g(X) = r(X)$ where $\deg(r) < \deg(g)$ (not necessarily unique), for some k.*

Don't need to be in a domain, but probably need it for uniqueness.

Ex. $X^3 + X + 1 = f(X)$ and $g(X) = 2x + 1$. $2f(X) = 2X^3 + 2X + @$, find $q(X)$ that makes $q(X)g(X)$. We will start with the $2X^3$ term, so $q_1(X) = X^2$ works. Then $2X^3 + 2X + 2 = X^2(2X+1) + r_1(X) = 2X^3 + X^2 + (-X^2 + 2X + 2) = q_1(X)g(X) + (-X^2 + 2X + 2)$. Repeat with $-X^2 + 2X + 2$. Divide by g again, $2(-X^2 + 2X + 2) = q_2(X)(2X+2) + r_2$ works out what r_2 has to be (we had the multiply by 2 again).

That is the division algorithm, and it's kinda a pain, but we are going to need it.

This is easier in the world of fields, we just divide out by the leading coefficient to make $g(X)$ monic. So let R be a field. In this case, get $f(X) = q(X)g(X) + r(X)$ where $\deg(r) < \deg(g)$, and q, r are unique. We can show uniqueness easily: $q(X)g(X)+r(X)=q_1(X)g(X)+r_1(X) \implies g(X)(q(X)-q_1(X))=r_1(X)-r(X)$. The LHS has deg $\geq \deg g$ and the RHS has deg $< \deg g$, so both $r-r_1$ and $g-g_1$ are zero. Can see how this breaks: deg doesn't play nice. Now, there exists a division algorithm in $k[X]$, k a field, reduce the degree by division. There are interesting work in doing multivarible division. The algorithms are very sensitive to what you consider the degree as.

Consequence of long division:

Theorem 3 (Factor theorem)**.** *Suppose k is a field, $f(X)\in k[X]$. Then if $\alpha \in k$ is a solution to $f(X)=0$, then $(X-\alpha)$ divides $f(X)$ (remainder $r=0$), and conversely, if $(X-\alpha)$ divides $f(X)$ then α solves $f(X)=0$.*

Proof. Backwards is obvious: $f(X)=(X-\alpha)g(X) \implies f(\alpha)=(\alpha-\alpha)g(\alpha)=0$. Conversely, suppose $f(\alpha)=0$. (Remark: $f(\alpha)$ by definition is the image of X under $k[X]\to k$, $X\mapsto\alpha$, what we began the class with.) $f(X)=q(X)(X-\alpha)+\alpha_0$ and α_0 is a constant in k. Set $X=\alpha \implies 0=0+\alpha_0 \implies \alpha_0=0$. □

For general $f(X), \alpha\in k$, have $f(X)=q(X)(X-\alpha)+\alpha_0$, $\alpha_0\in k$. Pur $X=\alpha \implies f(\alpha)=0+\alpha_0$ then $\alpha_0=f(\alpha)$ (remainder of division of $f(X)$ by $(X-\alpha)$ is $f(\alpha)$).

Theorem 4. *k a field, $R=k[X]$, $I\subseteq R$ any ideal. Then $\exists$ a unique monic polynommial $f(X)$ such that $I=(f(X))=$ principal ideal generated by f.*

Remark 5. False for multivariable rings

Remark 6. $k[X]$ is similar to $\mathbb{Z}$ in this sense. Principle ideal domains: integral domain in which every ideal is principle.

What is special about $k[X]$ that you can't do in every PID is that you can do long division, so we call it a Euclidean ring.

Cutoff for quiz 2 is all of today.

6 Janaruy 30 (Zinovy)

We will continue looking at polynomial rings. Let F be a field, and $F[x_1,\dots,x_n]$ be the ring of polynomials in n variables with coefficients in F. These are formal polynomials, might get to considering them as functions today.

Why do we care about polynomials, and ideals in polynomial rings?

The universal property: if A is a commutative F-algebra (i.e. A is a ring containing F as a subring; it's an F vector space but can multiply elements) and $a_1,\dots,a_n\in A$, then there exists a homomorphism $f\colon F[x_1,\dots,x_n]\to A$ such that $f(x_i)=a_i$. In particular, if $a_1,\dots,a_n$ generate A as an F-algebra, then f is surjective and $A\cong F[x_1,\dots,x_n]/I$, where $I=\ker f$ is an ideal of $F[x_1,\dots,x_n]$.

(Not every F-algebra is finitely generated, but the most interesting ones are.) For this reason, we want to undersatnd the ideals of the polynomial ring $F[x_1,\dots,x_n]$. Simplest case: $n=1$. Write $F[x]$ instead of $F[x_1]$. We have also restricted ourselves to fields (as opposed to just a commutative ring, for which the universal property still holds) since it is simpler: we already know what all the ideals are, i.e. F and (0).

Last time: division with remainder. Given $f(x),g(x)$ in $F[x]$, $g(x)\neq 0$, $\exists! q(x),r(x)\in F[x]$ such that $f(x)=q(x)g(x)+r(x)$ and $\deg(r)<\deg(g)$. Note that the division algorithm is a theorem, not an algorithm. an algorithm for finding $q(x)$ and $r(x)$ is called "long division".

Corollary 3. *Let $f(x)\in F[x]$, $a\in F$ is a root of $f(x)$ if and only if $f(x)=q(x)(x-a)$ for some $q(x)\in F[x]$.*

Corollary 4. *A polynomial $f(x)\in F[x]$ of degree $d\geq 0$ (not the zero polynomial, which has degree $-\infty$) has at most d roots in F.*

Theorem 5. *$F[x]$ is principle ideal domain (i.e. every ideal is generated by one element).*

Another ring with this property is the integers. Essentially the same proof, uses the division algorithm.

Proof. Let $I \subset F[x]$ be an ideal. We want to show that $I = (g(x)) = \{f(x)g(x) \mid f(x) \in F[x]\}$ for some $g(x) \in F[x]$. If $I = (0)$, we take $g(x) = 0$.

If $I \neq (0)$, take $g(x) =$ non-zero polynomial of minimal degree in I. Now take $f(x) \in I$, want to show that f is a multiple of g, i.e. $f(x) \in (g(x))$. Divide $f(x)$ be $g(x)$ with remainder: $f(x) = q(x)g(x)+r(x)$ where $\deg(r) < \deg(g)$. Note that $f(x), g(x) \in I$, hence $r(x) = f(x) - q(x)g(x) \in I$, but $g(x)$ has smallest degree in I, so $r(x) = 0$. □

Corollary 5. *Let I be a non-zero ideal in $F[x]$. Then $\exists!$ monic polynomial $g(x)$ such that $I = (g(x))$.*

("Monic" means leading coefficient is 1. Ex. $1, x+1, x^2 - x + 17$ are monic. $2x^3 + x^2 + 5x + 3$ is not monic, if $\operatorname{char}(F) \neq 2$.)

Proof. Existence: Find a generator $g(x)$ for I. After rescaling, may assume $g(x)$ is monic (since every leading coefficient is a unit in F).

Uniqueness: Assume $I = (g_1(x)) = (g_2(x))$, $g_1(x), g_2(x)$ are monic. Then $g_1(x) \mid g_2(x)$ and $g_2(x) \mid g_1(x)$, hence $g_1(x) = g_2(x)$ (same degree, so dividing gives a scalar, but both monic, so that scalar is 1. □

Remark 7. If $n \geq 2$, then $F[x_1, \dots, x_n]$ is not a PID. In particular, $I = (x_1, \dots, x_n)$ is not principle (check!). (Argument: Lowest order is either degree 1 or 0, but no degree 0 because constant term is 0, but there is no one degree polynomial that divides both x_1 and x_2, but this is required for I to be principle.)

Now let us go back to the siutation where a commutative ring A is generated by a field $F \subset A$ and one additional element u. Let $h\colon F[x] \to A$ be the homomorphism taking x to u, $\ker(h)$. Choose a monic generator $g(x)$ for $I = \{$polynomials $f(x) \in F[x]$ such that $f(u) = 0$ in $A\}$. So $h\colon F[x] \to A, x \to u$, $I = \ker h = (g(x))$, $g(x)$ monic. Note that if u is transcendental over F, then $I = (0)$, so a monic generator $g(x)$ can only be chosen if u is algebraic over F.

Proposition 1. *Assume u is algebraic over F, i.e. $I \neq (0)$. Let $g(x), A$ be as above, then*

(a). If $g(x)$ is irreducible over F, then A is a field.

(b). If $g(x)$ is reducible over F, then A is not a domain, i.e. A has zero divisors.

($g(x)$ reducible means $g(x) = f(x)h(x)$ where $\deg f > 0, \deg h > 0$.)

Proof. Assume that A is not a field. Then A has an ideal $(0) \subsetneq J \subsetneq A$ (take a noninvertible element in A and generate ideal). Set $I_0 = h^{-1}(J)$, and ideal of $F[x]$. $I_0 = \{f(x) \in F[x] \mid f(u) \in J\}$. Choose a generator for I_0, i.e. $I_0 = (g_0(x))$. Since $(0) \subsetneq J \subsetneq A$, we have $\ker(h) \subsetneq I \subsetneq F[x]$. Recall that $\ker(h) = (g(x))$ and $I = (g_0(x))$. Thus $g_0(x) \mid g(x)$ but $g(x) \nmid g_0(x)$. The first says that $g(x) = g_0(x)q(x)$ and the second says that $\deg(q) \geq 1$. We conclude that $g(x)$ is reducible, proving part (a).

Suppose $g(x)$ is reducible: $g(x) = k(x)l(x)$ where $\deg(k), \deg(l) \geq 1$. Then $g(u) = 0 = h(u)l(u)$ in A. Thus $h(u), l(u) \neq 0$ in A (since $\deg(k) + \deg(l) = \deg(g)$??? this feels like $u = 0$ make this wrong, but we just have $g(x) = x$???) and $h(u)l(u) = 0$, so $k(u), l(u)$ are zero divisors. □

$F[x_1, \dots, x_n]$ is the ring of "formal polynomials" in $x_1, \dots, x_n$. Let R be the ring of polynomial functions $F^n \to F$. We have a natural homomorphism $h\colon F[x_1, \dots, x_n] \to R$. Example: F is a field of 2 elements $= \mathbb{F}_2 = \{0, 1\}$, $n = 1$. Then $h(x^2 - x) =$ zero function $\mathbb{F}_2 \to \mathbb{F}_2$. The moral is that h is always surjective, but may not be an isomorphism. In fact, $\ker(h) \supset (x_1^q - x_1, x_2^q - x_2, \dots, x_n^q - x_n)$ when F is a finite field of order q.

Theorem 6. *If F is an infinite field, then h is an isomorphism. If F is a finite field, $|F| = q$, then $\ker(h) = (x_1^q - x_1, x_2^q - x_2, \dots, x_n^q - x)$.*

Proof. Let F be an infinite field. We need to show that h is injective. In other words, if $f(x_1, \dots, x_n)$ is a non-zero polynomial, then there exist $a_1, \dots, a_n \in F$ such that $f(a_1, \dots, a_n) \neq 0$. We argue by induction on n. Base case: $n = 1$. Here we know that $f(x_1)$ has finitely many roots, at most $\deg(f)$. This, there exists $a_1 \in F$ which is not a root of $f(x_1)$ since F is infinite. Induction step: Write $f(x_1, \dots, x_n) = f_d(x_1, \dots, x_{n-1})x_n^d + f_{d-1}(x_1, \dots, x_n)x_n^{d-1} + \cdots + f_0(x_1, \dots, x_{n-1})$. By inductive assumption, choose $a_1, \dots, a_{n-1} \in F$ such that $f_d(a_1, \dots, a_{n-1}) \neq 0$. Now $f(a_1, \dots, a_{n-1}, x_n)$ is a non-zero polynomial in 1 variable. So by the base case, there exists an $a_n \in F$ such that $f(a_1, \dots, a_{n-1}, a_n) \neq 0$.

Proof of part the second part will be covered next time, or is an exercise. Here's the idea: whenever you see x_i^q replace it wth x_i until you get a polynomial with all variables with degrees less than q. □

7 February 6

Going to skip over the polynomial function stuff Zinovy didn't get to, can just read it and a bit behind schedule because of the snow. So homework pushed back a bit so we can cover symmetric polynomials today, but next week will still be on schedule.

7.1 Symmetric polynomials

Studied for 100s of years, and still don't know where they come from. One source is as follows: $f(X) = 0, f \in \mathbb{Q}[X]$,

$$f = \sum a_n X^n = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = \prod_{i=1}^{n}(X - \alpha_i)$$

(assuming monic). How are a_j and α_i related? $a_0 = (-1)^n \prod \alpha_i$, $a_{n-1} = -\sum \alpha_i$, or generally,

$$a_j = \pm \sum \prod \alpha_i \cdots \alpha_{i_{n-j}}$$

So a_j = are the symmetric functions of roots = elementary symmetric polynomial in roots. Solving the equation $f(X) = 0$ given $a_0, \dots, a_{n-1} = n-1$ symmetric functions of $\alpha_1, \dots, \alpha_n$. We want to find $\alpha_1, \dots, \alpha_n$. But can't, because these a_j can't distinguish between the roots. We talked last term only possible when degree is $2, 3, 4$.

General fact: symmetric functions of roots generate all possible symmetric functions. Start with $X_1, \dots, X_n$ variables, $F(X_1, \dots, X_n)$ polynomial.

Definition 9. F is symmetric if $F(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = F(X_1, \dots, X_n)$, $\forall \sigma \in S_n$. Define P_j = j-th symmetric polynomial $= \sum_{j-\text{tuples}} \prod X_{i_1} \cdots X_{i_j}$ (where $i_1 < i_2 < \cdots < i_j$).

Theorem 7. *If F is symmetric, then*

(a). F is a polynomial function of $P_1, \dots, P_n$

(b). $P_1, \dots, P_n$ are algebraically independent, in the sense that if $F[X_1, \dots, X_n]$ is any polynomial such that $F[P_1, \dots, P_n] = 0$, then $F = 0$.

$k[X_1, \dots, X_n] \cong k[P_1, \dots, P_n]$ (via (b)). So symmetric functions $\subsetneq k[X_1, \dots, X_n]$, but the symmetric functions are isomorphic to $k[X_1, \dots, X_n]$ via $X_i \to P_i$.

Proof. (Part (a)) Some sort of "long division" in n-variables.

Talked about before that long division with multiple variables is a bit undefined in what we mean by one polynomial being "bigger" than another. So we will use the lexicographic ordering of monomials: monomials $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} > X_1^{j_1}\cdots X_n^{j_n}$ by looking for the first index k where $i_k \neq j_k$, bigger one wins. So $X_1^2X_2 > X_1X_2X_3$ and $X_1X_2X_3^2X_4 < X_1X_2X_3^4$. This is an example of a Gröbner basis, relevant in computational algebra.

Remark 8. This depends on the ordering of the X_i, which is arbitrary.

Fact: if P, Q are monomials of degree m, and $P < Q$, then $NP < NQ$ for any other monomial N.

Start with $F[X_1, \dots, X_n]$ symmetric, subtract off polynomials in the $P_1, \dots, P_n$ to reduce the biggest term. this is $\sum$(coeff)monomials $= \sum_d \underbrace{\sum \text{(coeff)monomials of } \deg d}_{F_d = d\text{-th homogenous part}}$, and these F_d are symmetric as well. Fix d, and sconsider $F = F_d$. Sum of terms: (coeff)$X_1^{i_1}\cdots X_n^{i_n}$ where $\sum_{i_k} = d$. This is symmetric, so conains this monomial for all permutations of the X_i. So it contains a biggest term $X_1^{k_1}X_2^{k_2}\cdots X_n^{k_n}$, $k_1 \geq k_2 \geq k_3 \geq \cdots$ (this must be the biggest, otherwise $k_i \leq k_j$ where $i < j$, and could swap them).

Claim: we can find a polynomial expression in $P_1, \dots, P_n$ with the same leading/highest/biggest term. To do this, need to study leading coefficients of the P_i. First, $P_1 = X_1 + \cdots + X_n$ has leading coefficent X_1 (why are we calling these leading coefficient???); $P_2 = \sum_{\text{pairs}} X_iX_j = X_1X_2 + \cdots$ has leading term X_1X_2; generally, $P_j = X_1X_2\cdots X_j + \cdots$, leading term is $X_1X_2\cdots X_j$. Leading term of

$$P_1^{d_1}P_2^{d_2}\cdots P_n^{d_n} = X_1^{\sum_{i=1}^n d_i} X_2^{\sum_{i\geq 1}^n d_i} + \cdots$$

can make this match $k_1, k_2, \dots, k_n$???

Pick $d_n = k_n$, work backwards to solve for $d_1, \dots, d_n$ therefore we get smoe expression in $P_1 \cdots P_n$ with same leading term, scale to match coefficients, subtract to reduce size, repeat. This is symmetric, so contains this monomial for all polynomials of the X_i. Thus, this contains a biggest term with $X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$ where $k_1 \geq k_2 \geq k_3 \geq \cdots$. □

This is annoying to do by hand, not bad with a computer.

Standard problem in computer algebra and algebraic geometry is you have some ring with variables being permuted by some group, might ask which polynomials are invariant. This is just the most basic setup, with we have an arbitrary ring and our group is the symmetric group. Called geometric invariance theory.

Proof. (Part (b)) We are showing algebraic independence of $P_1, \dots, P_n$. Suppose wee have $\sum_{(d)} a_{d_1 \cdots d_r} P_1^{d_1} \cdots P_r^{d_r} = 0$, the sum over r-tuples (d). If nontrivial, there is some coefficient $a_{d_1 \cdots d_r} \neq 0$.

Define $k_i = d_i + d_{i+1} + \cdots + d_r$. Then the degree of $P_1^{d_1} \cdots P_r^{d_r}$ is $m = \sum k_i = \sum i d_i$ (check this yourself, but notation can be a nuisance). We then write this in terms of the $X_1, \dots, X_n$, and look at the terms of highest degree, this appears only once. We will get a contradiction out of that... read the book, it's a pain, notation bogs things down. "Kinda fun, and worth understanding." □

Here's a thing to point out about these multi-variable polynomials: there is a lot of bookkeeping, and this makes it hard, but you just have to get used to it and think it through. In practice, most multi-variable stuff is done on a computer.

7.2 Factorization

Let R be a commutative integral domain (e.g. $\mathbb{Z}$). Given $x \in R$, $x \neq 0$, want to factor it uniquely in some sense. Clearly, if u is a unit, $x = u \cdot u^{-1} x$, so factorizations only unique up to units.

First question: what is the analogue of a prime? In $\mathbb{Z}$, x is called prime if $x = yz \implies y$ or z is ± 1. In a general ring, can adapt this definition.

Definition 10 (Irreducible). x is irreducible in R if x is not a unit, and $x = yz \implies$ either y or z is a unit.

Note that we are not using the word prime here.

Another defining feature of primes in $\mathbb{Z}$ (Euclid's lemma): in $\mathbb{Z}$, p is a prime $\iff p \mid ab \implies p \mid a$ or $p \mid b$. These are different: one is about how p can be divided, this one is how p divides other elements.

Definition 11 (Prime). x is a prime in R if x is not a unit, and if $x \mid ab \implies x \mid a$ or $x \mid b$.

In general, irreducible and prime are not equivalent, even though they are in $\mathbb{Z}$.

Theorem 8. *"Unique factorization" works in $R \iff$ (irreducible $\iff$ prime).*

Let's do some examples of how this thing can break. Let $R = \mathbb{Z}[\sqrt{-5}]$. We can factor 6 in multiple ways: $6 = 3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Can we "match" these factors? (i.e. they are equal up to units). Generally, no.

Is 3 irreducible in $\mathbb{Z}[\sqrt{-5}]$? Assume $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Hard to multiply out, because there are units floating around, but what if we took the abolsute value (and also squaring?): $9 = (a^2 + 5b^2)(c^2 + 5d^2)$, which are all in $\mathbb{Z}$. Will find you can't do it???

What are the units in this ring? $u \cdot r = 1$, so $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$. Then $(a^2 + 5b^2)(c^2 + 5d^2) = 1 \implies a, c = \pm 1$, $b, d = 0$.

Through very non-elementary means, one can show that there are only 10 possible values such that $\mathbb{Z}[d]$ has unique factorization (modular forms or something). Posed by Gauss and not solved until the 50s. Solved by German schoolteacher who went to his grave without recognition.

8 February 27

Let k a field, we might wonder what $k[X]/(f(X))$ is. If $f(X)$ is irreducible (and so $(f(x))$ is maximal), we get another field, $k(u)$ (where u is a root of $f(X)$, $u = \bar{X} = X + (f(X))$). Now, when J is principal and $(g(X)) = J \supset (f(X))$, then $g(X) \mid f(X) \implies g(X) \sim f(X)$. If we instead have $f(X) = g(X)^e$, $g(X)$ irreducible, then $k[X]/(f(X)) = R$, not even an integral domain, since $g(X) \neq 0$ in R, $g(X)^e = 0$ in R. More generally:

Theorem 9. *When $f(X) = \prod g_i(X)^{e_i}$, where the $g_i(X)$ are irreducible, monic, and distinct,*

$$k[X]/(f(X)) \cong \oplus k[X]/(g_i(X)^{e_i})$$

This generalizes the Chinese remainder theorem:

Theorem 10 (CRT)**.** *$R = \mathbb{Z}$, $n = \prod p_i^{e_i}$, $\mathbb{Z}/n\mathbb{Z} \cong \oplus \mathbb{Z}/p_i^{e_i}\mathbb{Z}$.*

When $n = p$ prime, get a field $\mathbb{F}_p$, or if equal to p^e, get $\mathbb{Z}/p^e\mathbb{Z}$.

As long as you don't have repeated roots in the factorization, things don't look too weird. When it is just one, looks like $\mathbb{Z}/p\mathbb{Z}$, but when we add more, it starts looking funkier.

How do we prove the theorem? The proof actually looks a lot like the proof for the Chinese remainder. For CRT, we want $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$, and generally, we want $k[X]/(f(X)) = k[X]/(f_1 f_2) \cong k[X]/(f_1(X)) \oplus k[X]/(f_2(X))$. What is the map in the CRT case? We have $r \bmod pq \mapsto r \bmod p \oplus r \bmod q$. We have $(pq) \subseteq (p)$ and $(pq) \subseteq (q)$. What is the equivalent in the general setting? ff something about homomorphism theorem.

For CRT, how do we prove injectivity? Well, $r \bmod p = 0 \implies p \mid r$ and $r \bmod q = 0 \implies q \mid r$, and since p, q are coprime, this gives $pq \mid r$, and so the kernel is just 0. Similarly, $g(X) = 0 \bmod f_1 \implies f_1 \mid g$ and $g(X) = 0 \bmod f_2 \implies f_2 \mid g$ which imply $f_1 f_2 \mid g$, hence, injective.

Now we prove surjectivity. To get $\mathbb{Z}/pq\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$, consider the element $(r_1, r_2) \in \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$. We want $r \in \mathbb{Z}$ such that $r \equiv r_1 \bmod p$ and $r \equiv r_2 \bmod q$. Bezout's says $\exists m, n$ such that $mp + nq = 1 = \gcd(p, q)$. So $r_2 mp + r_1 nq \equiv r_1 nq \bmod p \equiv r_1(1 - mp) \equiv r_1 \bmod p$. Similarly, $r_2 mp + r_1 nq \equiv r_2 \bmod q$. So $r = r_2 mp + r_1 nq \equiv r_1 nq$. Now in the general setting, we are given $r_1(X) \bmod f_1(X)$ and $r_2(X) \bmod f_2(X)$, want $r(X) \equiv r_1(X) \bmod f_1$ and $r(X) \equiv r_2(X) \bmod f_2$. The same process works, since the g.c.d. exists and is 1. To get $m(X)f_1(X) + n(X)f_2(X) = 1$ for coprime $f_1(X), f_2(X)$, we could use the Euclidean algorithm as in $\mathbb{Z}$, or for a method that works for any PID, we can use the fact that $(f_1(X))$ is maximal. Then $(f_1(X), f_2(X)) \supsetneq (f_1(X)) \implies (f_1(X), f_2(X)) - k[X] \implies 1 \in (f_1(X), f_2(X))$.

(Oops, I've been saying general setting through, but this is really just the polynomial setting).

8.1 Hilbert's basis theorem from quiz

"It is actually quite easy once you see that induction is involved. We've used this technique a bunch of times." Bruh, no shit it's induction.

We have $k[X_1, \ldots, X_n]$, and we want to prove any ideal is finitely generated. We go with induction on n: $n = 1$, $k[X]$, PID¡ so clear (first part). Assume the result for $n-1$ variables, let I be an ideal in $k[X_1, \ldots, X_n]$ in this ring. Take $f \in I$, it is of the form

$$f = a_m(X_1, \ldots, X_{n-1})X_n^m + a_{m-1}(X_1, \ldots, X_{n-1})X^{m-1} + \cdots$$

(the $a_i(X_1, \ldots, X_{n-1})$ are polynomials). Consider the coefficients $a_m(X_1, \ldots, X_{n-1}) \in k[X_1, \ldots, X_{n-1}]$ as f runs over $f \in I$. Claim: this is an ideal J in $k[X_1, \ldots, X_{n-1}]$. To see this, let $g \in I$, so $g = b_r(X_1, \ldots, X_{n-1})X_n^r + \cdots$. Assuming $m \geq r$ (otherwise, leading coefficient won't be mth power???), the leading coefficient of $X^{m-r}g + f$ is $b_r + a_m$, so it is closed under addition. Closure under multiplication is obvious.

By induction, J is finitely generated. So there exists finitely many polynomials $f_1, \ldots, f_s$ in $I \subseteq k[X_1, \ldots, X_n]$ whose leading coefficients generate J. Which means given any $f \in I$, there exists polynomials $g_1, \ldots, g_s$ in $k[X_1, \ldots, X_{n-1}]$ such that the leading coefficient of $\sum_{i=1} g_i f_i$ matches that of $f \implies I = (f_1, \ldots, f_s)$. (Like how proved that $k[X]$ is a P.I.D.)

A simpler way to put this is to state it as R noetherian implies $R[x]$ noetherian: Let $I \subset R[X]$, want finiteily many generators. Write $f \in I = a_m X^m + a_{m-1}X^{m-1} + \cdots + a_0$ (these a_i are functions of f). Let J be genereated by $a_m(f)$ for all $f \in I$, which is an ideal in R, and so it is finitely generated. Then, we show that it these generate I: take top coefficient, match it, and left with a lower degree, then give another combination of the generators, and so on.

Hmm, Arvin might have pointed out a problem... will post an update later (an adjust marks if there is a problem).

Quiz on Thursday: said Euclidean rings are mainly just a curiosity and not a lot of interesting results. So for quiz, really just need to know $\mathbb{Z}$ and polynomial rings are Euclidean rings.

8.2 Intro to modules

Modules are for rings what vector spaces are for fields.

Definition 12 (Module). Let R be a ring (usually commutative). A *module* is an abelian group M plus a map "multiplication by R": $R \times M \to M$ that satisfies the obvious conditions: $(r_1 r_2)m = r_1(r_2 m)$, $(r_1+r_2)m + r_1 m + r_2 m$, $r(m_1 + m_2) + rm_1 + rm_2$, and $1m = m$.

Example: a vector space over a field.

In general, the action of $r \in R$ can be complicated. It is not invertible in general, $rm = 0$ can happen even when $r \neq 0$. For us R will be a P.I.D. (usually $\mathbb{Z}$ and a polynomial X over a field) and M will be a finitely generated module (will say what this means in a second) so that it is much nicer. And in this case, wwe can describe them explicitly, a complete structure theory. But often in research, will get some random module over a complicated ring, and it is quite hard to figure out what is going on. This is commutative algebra, and "it is kind of a black art."

M finite generated module when it is a finite abelian group (and as we discussed, can represent as direct sum of $\mathbb{Z}$ mod prime powers; will get an even stronger result).

Example: $R = \mathbb{Z}$, M is an abelian group, $rm = (m + m + \cdots + m)$ r times. Then M is a $\mathbb{Z}$-module. Quotients of $\mathbb{Z}/n\mathbb{Z}$ will give the theory here?

Example: k a field, $V = k^n$, $A = n \times n$ matrix with entries in k. V is a $k[X]$-module by sending $p(X) = p(A) =$ $n \times n$ matrix acts on k^n. The quotient stuff we talked about the beginning of the lecture will be important here.

These two modules look quite different, but will see can be described by the same structure theory. Particularly, we will be able to describe the matrix A, and will get a lot of things falling out from linear algebra (don't need to go to $\mathbb{C}$ just to get eigenvalues).

9 February 29!

9.1 Modules

Recall the definition: R is a commutative ring, M an abelian group, then M is an R-module if $\exists$ a scalar multiplication $R \times M \to M$ where we write $(r, m) = rm \in M$ that satisfies

(a). $(r + s)m = rm + sm$

(b). $r(m_1 + m_2) = rm_1 + rm_2$

(c). $(rs)m = r(sm)$

(d). $1m = m, \forall m$

(these are only for left modules??? Or does commutativity fix). In particular, ideals $\subseteq R$ are modules.

If R is not commutative, we have left/right modules, just like ideals, $r \cdot m$ (left multiplication) and $m \cdot r$ (right multiplication). We won't see much of these after today, but important to know what they are.

Example: $R = \mathbb{Z}$, $M =$ any abelian group. Then can define the obvious multiplication: $n \cdot m = (m + m + \cdots + m)$ n times. So any abelian gruop is naturall a $\mathbb{Z}$-module.

Let us define $\phi(r)\colon M \to M$ by $m \mapsto rm$ (any R), and so $\phi(r)(m_1 + m_2) = \phi(r)(m_1) + \phi(r)(m_2)$, thus $\phi(r)$ is an abelian gruop hoomormophism $M \to M$. We can see that property (a) says $\phi(r) + \phi(s) = \phi(r + s)$, property (b) says $\phi(r)(m_1) + \phi(r)(m_2) = \phi(r)(m_1 + m_2)$, and property (c) says $\phi(r) \circ \phi(s) = \phi(rs)$. So to say M is a (left) R-module is equivalent to $r \mapsto \phi(r)$ be a homomorphism of rings $R \to \operatorname{Hom}(M, M)$ (abelian group homomorphisms under function composition). (R is not necessarily a commutative ring.)

Example: $M = \mathbb{R}^n$, R are the $n \times n$ matrices, and $v \in \mathbb{R}^n$ (column vector). Multiplication is $(r)v$. Note that the group abelian group homomorphisms from $\mathbb{R}^n$ to itself huge. We could also see a similar right module $v(r)$ (v is a row vector now).

Example: F a field, $M = F^n$, and $A =$ fixed $n \times n$ matrix. M is a module over $F[X]$ by $p(X) \cdot r = p(A) \cdot r$ (the polynomial is like $1 + X + X^2 \mapsto 1 + A + A^2$). The module structure depends on the choice of A; as sets, R and M don't change though. The module structure of F^n gives a way of analysing A. This and $\mathbb{Z}$ are going to be the main modules we look at. In some sense, modules over p.i.d.s are much easier to work with.

M is called finitely generated over R if there exists $m_1, \ldots, m_s \in M$ such that any $m \in M$ is of the form $m = \sum_i r_i m_i$ for some $r_i \in R$ (this should remind you of finite dimensional vector spaces: "finite spanning set" $m_1, \ldots, m_s$).

For us, M is a finite generated module over a PID (a very special case).

Fact (Cayley's theorem for rings) R acts on itself by multiplication $M = (R, +)$, so $r \cdot s = rs$ where $s \in (R, +)$, $r \in R$. This gives a map $R \to \mathrm{Hom}(R, R)$ (under $+$). This is injective, since $r \cdot 1 = r$ so $\phi(r) \neq 0$ if $R \neq 0$. Cayley's says any group is a subgroup of the permutations to itself. This is saying that any ring is a subgring of the homomorphisms to itself under addition. (Of theoretical interest.)

We now look at a so-called *free module*. Let R be a ring, R^n be n tuples of elements of R. We define $(r_1, \ldots, r_n) + (s_1, \ldots, s_n) = (r_1 + s_1, \ldots, r_n + s_n)$ and $r(r_1, \ldots, r_n) = (rr_1, \ldots, rr_n)$. This is the free module of rank n. Note that any $(r_1, \ldots, r_n) = r_1 e_1 + r_2 e_2 + \cdots r_n e_n$ where $e_i = (0, \ldots, 1, \ldots, 0)$ at the ith spot. This expression is unique by definition (not a basis ???).

If $n = 1$, then R is a module over itself. Any element $r = r \cdot 1$, 1 is a generator. Same holds for a unit ε, $r = (r\varepsilon^{-1})\varepsilon$. If ε is not a unit, then $R\varepsilon \subsetneq R$. If $\exists s$ such that $s\varepsilon = 0$. $R \to R$, $x \mapsto x\varepsilon$ is not injective, so $R\varepsilon$ may not be free. I.e. it may not be isomorphic to R (see below).

N, M, are R modules. $\psi \colon N \to M$ is an R-module homomoprhism means that $\psi$is a homomorphism of abelian gruops, and $\psi(rn) = r\psi(n)$ (R-linear). It is isomorphic if injective and surjective. M is called free with rank n if $M \cong R^n$.

Pathology: if R is not commutative, it is possible that $R^n \cong R^m$, $n \neq m$.

10 March 5

10.1 Free modules (cont.)

Recall, if R is a ring, the free module of rank n is the set of n-tuples $R \times \cdots \times R$ with component wise operations. We have $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ in the ith slot. Any $m = (m_1, \ldots, m_n) = \sum_i m_i e_i$ uniquely. The e_i form a basis.

We also talked about homomorphism of modules: $\phi \colon M \to N$, M, N are R-modules, is a homomorphism if $\phi(rm) = r\phi(m)$ for all $r \in R, m \in M$, and ϕ is an abelian group homomorphism, so $\phi(r_1 m_1 + r_2 m_2) = r_1 \phi(m_1) + r_2 \phi(m_2)$. ϕ is an isomorphism if bijective. Notice how similar it looks to linear maps.

M is called *free* if $M \cong R^n$ for some n (in the category of R-modules: all the modules are in some fixed ring R). $\phi \colon M \to R^n$ is an isomorphism if $\phi(f_i) = e_i$, f_i basis for m. Any $m \in M$ is uniquely written as coordinates with respect to the basis $f_1, \ldots, f_n$, i.e. $m = \sum_i r_i f_i$, the $r_i \in R$ are unique. So $m \mapsto (r_1, r_2, \ldots, r_n)$ from ϕ.

Theorem 11. *If R is commutative, then $R^m \cong R^n \iff m = n$.*

(The backwards direction is trivial though.) Proof will be postponed for now. What this theorem means is that if M is free, it has a well-defined rank ($M \cong R^n$ for a unique n). This also tells us the dimension of a finite-dimensional vector space is well-defined (not something usually proven in linear algebra class).

10.2 Building up to structure theorem

We provide a bunch of definitions. Here, we are largely working in commutative rings, but if you weren't, this is just for left modules.

Definition 13 (Submodule). N is a *submodule* of M if N is an abelian subgruop of M and $rN \subseteq N$ $\forall r \in R$.

Definition 14 (Quotient module). Let M a module, $N \subseteq M$ a submodule. M/N exists as an abliean group quotient. It is also a module, via $r(x + N) = (rx + N)$, $r(x + n) = rx + rn \in rx + N$.

Kinda on the opposite end of free modules, we have torsion modules.

Definition 15 (Torsion module). M is called a *torsion module* if for any $m \in M$, $\exists r \in R$, $r \neq 0$, such that $rm = 0$.

Example: if $R = \mathbb{Z}$, M is a finite abliean group, and $nx = 0, \forall x \in M$, $n = \#M$.

Definition 16 (Annihalotor). If we fix $m \in M$, then $\mathrm{ann}_R(m) = \{r \in R \mid rm = 0\}$.

For torsion modules, $\mathrm{ann}_R(m) \neq 0$ for all m. We call $m \in M$ a torsion element if $\mathrm{ann}_R(m) \neq 0$ and $\mathrm{ann}_R(m)$ is an ideal in R (an order ideal???).

In a free module, the basis elements have no annihaltor. (Why???) This is a sense that these are quite different. Torsion modules are usually smaller.

Example: $M = \mathbb{R}^2$, $R = \mathbb{R}[X]$, and $P(X) = \sum a_i X^i$. We can evaluate the polynomial with the matrix $X \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, $P(X) \mapsto P(A)$. If $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in M$, then $X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = A \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 2\alpha \\ 3\beta \end{pmatrix}$, and

$$P(X) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = P(A) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \sum \begin{pmatrix} a_i 2^i 2^i & 0 \\ 0 a^i 3^i & \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha P(2) & 0 \\ 0 & \beta P(3) \end{pmatrix}$$

We then have $\left\{ \begin{pmatrix} \alpha \\ 0 \end{pmatrix} \right\}$ is a submodule, annihalated by $(X-2)$, and $\left\{ \begin{pmatrix} 0 \\ \beta \end{pmatrix} \right\}$ is a submodule, annihalated by $(X-3)$. Any time you have an eigenvector, you have a submodule. M is a torsion module annihilated by $(X-2)(X-3)$. A case of the Cayley-Hamilton theorem, since this is the characteristic polynomial $P_A(X)$ of the matrix, i.e. $P_A(A) = 0$ (the zero transform).

Suppose we try this with the matrix $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ instead. What are the possible submodules? $M = \mathbb{R}^2$ again. So if $N \subsetneq M$ has to be a vector subspace of $\mathbb{R}^2$ (since we require that it is closed under multiplication by all of $R = \mathbb{R}[x]$, and so obviously closed under multiplication by $\mathbb{R}$). The only interesting case is when the dimension is 1 (dim $= 0$ is trivial, dim $= 2$ is just M). So we have $N = \text{span}\{v\} = rv, r \in R$. Since it is a submodule, $rv \in \{v\}$, $r \in R[x]$, hence $Xv = \lambda v$ for some λ, which is true if and only if v is an eigenvector, so $N = \begin{pmatrix} \alpha \\ 0 \end{pmatrix}$, $\alpha \in \mathbb{R}$. So M has a unique submodule $N = \left\{ \begin{pmatrix} \alpha \\ 0 \end{pmatrix} \mid \alpha \in \mathbb{R} \right\}$. Only one eigenvector is a result of the matrix being non-diagonalizable. So $\text{ann}_R(N) = (X-2)$. Note that $(X-2)$ does *not* annihilate M, e.g.

$$(X-2) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = (A-2) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \neq 0$$

But $(X-2)^2$ does kill it, since we just saw that one $(X-2)^2$ puts it into N, and the another $(X-2)$ kills it. So $\text{ann}_R(N) = (X-2)$ and $\text{ann}_R(M) = \big((X-2)^2\big)$. Again, this is the characteristic polynomial.

If $R = \mathbb{Z}$, $M = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Then $\text{ann}_R(M) = (p)$. Here, M is splitting up into two submodules. The analog of our diagonalizable case. If we had had $M = \mathbb{Z}/p^2\mathbb{Z} \supseteq p\mathbb{Z} \supseteq p^2\mathbb{Z}$, let $N = p\mathbb{Z}$, so $\text{ann}_R(N) = (p)$, and $\text{ann}_R(M) = (p^2)$. This is the analog of our non-diagonalizable case. All this is very similar to what we just did with matrices.

Also, just a note, Cayley-Hamilton: given a matrix, take its characteristic polynomial, then $P_A(A) = 0$ for all A.

This is the point of the whole section: modules over a p.i.d. all have very similar structure. We can describe the structure purely in terms of the annihilator ideals.

Some more words on the structure theorem. Let R be a commutative ring; I and ideal, a submodule of R. Consider the quotient module R/I. The direct sums of modules: given M, N are R-modules, $M \oplus N =$ tuples $(m, n) \in M \times N$ with component wise operations (similarly for $M_1, \times, M_r$).

Theorem 12 (Structure Theorem)**.** *Let R be a PID, and M are finite generated R-module. Then*

$$M \cong R^n \bigoplus_{i=1}^{t} R/p_i^{e_i} R$$

for primes p_i, and $e_i \geq 1$ (maybe repeated), and this is unique up to the order of the direct sum.

Similar to what we stated last term, but that was only for finite abelian groups. Since R is a PID, all ideals are free modules with rank 1. Not true, even if Noetherian: $R = \mathbb{Z}[X]$, then $I = (2, X)$ is not free, not torsion. Something like this does not fit into this structure.

For any R, M is called cyclic if $\exists m \in M$ such that $M = \{rm \mid r \in R\}$, $R \to M$, $r \mapsto rm$ is onto.

10.3 Back to proving the theorem

Now lets go back to proving that R commutative means $R^m \cong R^n \implies m = n$. Consider $\phi\colon R^m \to R^n$. Step 1: represent this as a matrix, $e_1, \dots, e_m =$ the standard basis for R^m, and $f_1, \dots, f_n$ the standard basis for R^n. Then $\phi(e_i) = (r_{1,i}, \dots, r_{n,i}) \in R^n$. If $m \in R^n$, so $m = \sum_i \alpha_i e_i$, then linearity gives us $\phi(m) = \sum \alpha_i \phi(e_i)$, so $m = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$, and so we can represent ϕ as a matrix, since $\phi(m) = (r_{i,j})$, that is $n \times m$. We have

$$\phi \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

If $\phi = A$ and $\phi^{-1} = B$, we have $BA = I_{m\times m}$ and $AB = I_{n\times n}$. We'll try to show that if $n \neq m$, one is bigger, and so there is a nontrivial kernel in one direction, can't be injective. This a little sus: n, m different, not square and not necessarily inverse, but we can add stuff in the matrices to force them to be inverses. We'll continue this next time, but maybe read proof in the book, but be warned that since it is a book and they're trying to save space, they write vectors as rows since columns take more space.

11 March 7

Last time, we were talking about isomorphisms between free modules $R^m \cong R^n$ when R is commutative, and that whether it implies $m = n$. We have $\phi\colon R^m \to R^n$ and $\psi\colon R^n \to R^m$. Last time, we expressed ϕ, ψ as matrices A, B, where A is a $n \times m$ matrix and B is a $m \times n$ matrix:

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, \quad B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix},$$

We want to have that $\psi \circ \phi = 1$, i.e. $BA = I_m$ (WLOG, assume $m \geq n$). But BA is not a square matrix, so we will adjust these. Since A has more columns than rows, we add rows with all zeros at the bottom, call this A'. Likewise, we put columns full of zeros at the right of B, call it B'. Then, A', B' are both $m \times m$. We want, $BA = I_m$ so $\psi \circ \phi$ is the identity on R^m, and $AB = I_n$ so $\phi \circ \psi$ is the identity on R^n. Let's compute: $A'B'$ is I_n with zeros in the last $m - n$ columns and rows. $B'A'$ is I_m.

When we are dealing with commutative R (and only place we've used commutativty so far), we have that $B'A' = I_m \implies A'B' = I_m$ (homework problem, p. 97). But this is obviously a contradiction, so we are done. (How did we prove this fact: uses some facts about determinants that you only get with commutative R... I just symbol pushed on the HW).

Nike was thinking of another way to prove this on his bike ride. We have $B'A' = I$. Then $B'A' \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$. Consider $(x_1 \cdots x_m)B'A'$. Note that in a commutative ring, tranposes work the way they think they should (reverses the multiplication): if $v = (\alpha_1 \cdots \alpha_m)$ and $w^T = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix}$. Then $wv^T = \sum \alpha_i \beta_i$ and $vw^T = \sum \beta_i \alpha_i$, which are equal in a commutative ring. Then $(A')^T(B')^T x^T = x^T$, but $(A')^T(B')^T = B'A' = I$. He couldn't figure it out...

Point: if $M \cong R^n$ then n is uniquely determined, called rank(M).

Theorem 13 (Goal). *If M is finintely generated module over a PID R, then*

$$M \cong R^n \bigoplus_{i=1}^{t} R/p_i^{e_i} R$$

where p_i is prime, $e_i \geq 1$, n, p_i, e_i are unique up to reordering.

11.1 Direct sums

Let M be an R module, R commutative. $N_1, \ldots, N_s \subseteq M$ be submodules. Say that $M \cong \bigoplus N_i$ if each m in M is *uniquely* a sum $m = \sum n_i$, $n_i \in N_i$. Means that M is identified with tuples $(n_1, \ldots, n_s) \in N_1 \times \cdots \times N_s$. This is like the basis of a vector space. These N_i have to span and be linearly independent from each other.

Note that there is no requirement that the N_i be nice. Also not gauranteed we can always decompose M into finitely many N_i. Also, the fact that submodules exist does not mean that we can split it up.

Equivalently, we can make our conditions explicit:

$$M = \left\{ \sum_{i=1}^{s} n_i \colon n_i \in N_i \right\}$$

$$N_i \cap \left\{ \sum_{\substack{j=1 \\ j \neq i}}^{s} n_j \right\} = \{0\}$$

i.e. $\operatorname{span}\{N_j\}_{j \neq i} \cap N_i = \{0\}$.

Example: $R = \mathbb{Z}$, $M = \mathbb{Z}/p^2\mathbb{Z}$, p prime. Note that $M \supseteq N = p\mathbb{Z}/p^2\mathbb{Z}$. $\#M = p^2$ and $\#N = p$. We cannot write $M \cong N \oplus$ something ff. Just because N is a submodule, doesn't mean there is a complement. This is getting to the fact that modules are not "semisimple": when there is a subobject, there is a complement to that subobject. Most algebraic objects are not semisimple.

11.2 Starting the Structure Theorem

Proposition 2. *Let R be a PID and $M = R^n$. Suppose $N \subseteq M$, then N is free of rank $\leq n$.*

This is what we would expect from vector spaces. But this is false for general R. Take $R = \mathbb{Z}[X]$ and $I \subseteq R$, $I = (2, X)$ is not free of any rank (saw last time).

Proof. When $n = 1$, this proposition holds by the definition of a PID: since we are saying that the ideals of R ($N \subseteq R$) are free (a domain) of rank 1 (principal ideals).

General case by induction: Assume the statement holds for $n \leq m$, prove for $m + 1$. Consider $N \subseteq M = R^{m+1} = \{(x, \ldots, x_{m+1}) \in R \times \cdots \times R\}$. Consider the projection $N \to R$ induced by $(x_1, \ldots, x_{m+1}) \mapsto x_{m+1}$. This is a R-module homomorphism. If $\phi(N) = 0$, which implies $N \subseteq (x_1, \ldots, x_m, 0) \cong R^m$, so we are done by induction.

If $\phi(N) \neq 0$, then $\phi(N) \subseteq R$ has to be an ideal (a submodule). Hence $\phi(N) = \{rt \colon r \in R, t \text{ fixed}\}$. Pick $s \in N$ such that $\phi(s) = t$. Define $N_1 \subseteq N = Rs$. Define $N_2 \subseteq N = \{n \in N \colon \phi(n) = 0\} = \ker(\phi)$. Claim: $N \cong N_1 \oplus N)2$, where N_1, N_2 free and N_2 has rank $k \leq m$. ff

Remains to check that $N \cong N_1 \oplus N_2$. (i) span given $n \in N$, want $n_1 \in N_1$, $n_2 \in N_2$ such that $n = n_1 + n_2$. $\phi(n) \in \phi(N) = Rt \implies \phi(n) = rt$ for some $\phi(s) = t \implies \phi(rs) = r\phi(t) = rs = \phi(n)$. Then $n = (n - rs) + rs$. But $rs \in N_1$, and $\phi(n - rs) = \phi(n) - \phi(rs) = 0 \implies n_2 \in N_2$. (ii) Need to now show that $N_1 \cap N_2 = \{0\}$. If $x \in N_1 \cap N_2$, then $\phi(x) = 0$ (since $x \in N_2$) so the last component of x is zero. But $x \in N_1$, so $\phi(x) = rt$ for some $r \in R$, and so $r = 0$ since we are in a PID ($x = rs$), so $x = 0$. □

So how are we going to approach the main theorem? Here's the starting point: If $m_1, \ldots, m_r$ are generators of M, then there's $\phi \colon R^r \twoheadrightarrow M$ where $e_i \mapsto m_i$. We have $K = \ker(\phi) \subseteq R^r$, so $M =\cong R^r/K$. Idea: there is a basis of R^r that is adapated to M and K in the sense that K is identified with vectors $(\alpha_1, \ldots, \alpha_r)$ such that $\alpha \in K \iff r_i \mid \alpha_i$ for $r_i \in R$. Then $R^r/K = \bigoplus R/r_iR$. If $r_i = 0$, get a copy of R. If $r_i \neq 0$, get R/r_iR.

The best way to understand it is through an example, which we'll do next time. Getting these nice bases: this should remind you of echelon forms of matrices. The reason this works in a field is that everything is a unit, so we can always get to 1. We can't divide, but we'll get some sort of row reduction.

For the quiz next week, we'll go until the end of 3.6.

12 March 12

Missed class, apparently talked about Smith Normal form.

13 March 14

I think he's addressing the last problem from the previous homework, I came in a little late.

Let R commutative, $M = R^n$. Consider $A =$ an $n \times n$ matrxi $(a_{ij}) = A$. Let $f_i = Ae_i$ be the ith column of A. Claim: $f_1, \dots, f_n \in R^n$ span a free module of rank n if and only if $\det(A)$ is not a zero divisor.

If $\det(A)$ is a zero divisor, then $\text{span}\{f_1, \dots, f_n\}$ iis not free on f_is. Assume that $\det(A)$ is a zero divisor. Produce a non-trivial linear relation between the f_i (the f_i are not independent). Want some $r = (r_1, \dots, r_n) \neq 0$ such that $Ar = 0$. Key fact: $AA^* = A^*A = \det(A)I$, where $A^* = \text{adj}(A) = (b_{ij})$ such that $b_{ij} = (-1)^{i+j}\det(A_{ij})$ where A_{ij} is the $n-1 \times n-1$ matrix obtained by deleting the jth row and ith column (??? should be other way around). So we are saying

$$A \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{pmatrix} = \det(A)e_j$$

If there is some s such that $s\det(A) = 0$, then $A\left(s\begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix}\right) = 0$. This vector of b's is a cnadiate for r, but is it nonzero? We are done if $\exists ij$ such that $s\det(A_{ij}) \neq 0$. If not, then $s\det(A_{ij}) = 0$ for all ij. Suppose that $s\det(A_{ij}) = 0$. $\det(A_{11})$ has an expansion in rows/columns as well, and is equal to a linear combination of elements of A and $n-2 \times n-2$ minors. The point: this can also be written as $A\vec{r}$ for some r if one of these terms is nonzero done. If not s has to annihilate $n-2$ minors as well. Eventually s has to annihilate elements of A, $A\begin{pmatrix} s \\ \vdots \\ s \end{pmatrix} = 0, s \neq 0$.

Some general principal (localization): if R is a domain, we can do something like go to the field of fraction, do regular linear algebra, and then try to get answer back in terms of our original ring.

14 March 21

14.1 Structure theorem

Let R be a PID (like $\mathbb{Z}$), M a finitely generated module. Then we saw

$$M \cong R^n \bigoplus_{i=1}^{t} R/d_iR, \quad d_1 \mid d_1 \mid \cdots \mid d_r$$

We have that R is broken up into cyclic modules. We can also break up each of these R/d_iR to get prime power order:

$$M \cong R^n \bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{k_i} R/p_j^{f_j}R \right) \cong R^n \bigoplus_{p_i \text{ prime (maybe repeats)}} \bigoplus_{j=1}^{n_i} R/p_i^{e_j}R \tag{2}$$

where we have used Chinese Remainder theorem. So when $R = \mathbb{Z}$, we get

$$M = \mathbb{Z}^n \bigoplus_{p \text{ primes}} \bigoplus_{i} (\mathbb{Z}/p^{e_i}\mathbb{Z}) \tag{3}$$

So what we're doing is break down the torsion part into p-Sylow subgroups, and these are isomorphic to a sum of cyclic groups with p-power order.

Uniqueness in form (2): integer n is unique and so is the list of d_i. Uniqueness in form (3): the list of primes p that show up is unique; for each primes, the exponents list is unique.

Since forms (2) and (3) determine each other, we need only check uniqueness of one of the forms. It is easier to show uniqueness for form (2).

Let M be a finite abelian group of order m. Then the structure theorem tells us

$$M \cong \bigoplus_{p_i} \bigoplus_{j=1}^{n_i} \mathbb{Z}/p_i^{e_j}\mathbb{Z}$$

For each p_i, $\bigoplus_{j=1}^{n_i} \mathbb{Z}/p_i^{e_j}\mathbb{Z}$ is a p_i Sylow subgroup. It is clear that the list of primes is unique: the p_i are the primes in the unique factorization of $m = \#G$. In a general PID, M torsion, what is the analogue of order? Since M is torsion and finitely generated (???), there is an element $r \in R$ such that $rm = 0$ for all $m \in M$. The annihalotor is an ideal in a PID, so generated by a single element, say (s). So $sm = 0$ for all $m \in M$. $M \cong \bigoplus R/p_i^{e_i}R$, p_i shows up $\iff$ $p_i \mid s$ ($\mathbb{Z}$ is a UFD). Thus, the list of primes is determinedy by M.

Back when M is a finite abelian gruop, order m, so $\mathbb{Z}$-module:

$$M \cong \bigoplus_{p_i} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

And in a general PID with M torsion:

$$M \cong \bigoplus_{p_i} R/p_i^{e_i}R$$

where the p_i are prime elements of R. In the $\mathbb{Z}$ case, what happens if $M \cong \bigoplus$ to a different decomposition in terms of prime power cyclics? The p-Sylow subgroup in the first decomposition must match with the p-Sylow subgroup in the second, since they are unique. Hence, for each prime p fixed, there is an isomorphism $\bigoplus \mathbb{Z}/p_i^{e_i}\mathbb{Z} \cong \mathbb{Z}/p_i^{f_i}\mathbb{Z}$. And then we get uniqueness, since $e_i = f_i$ for all i.

Students need to be able to see the more general structure in these algebraic objects. Not enough to just know the definitions, can't peel back every time to the definitions. Need to be able to see the bigger picture of the structure.

What is the equivalent of a p-Sylow subgroup in the general case? It is $R[p^s] = \{m \in M \colon p^s m = 0\}$: the elements with order s??? then $\bigcup R[p^s]$ are the elements annihalated by some power of p, this is the "p-Sylow submodule". Some other decomposition has to match p-Sylow pieces. For a general ring, we don't call these p-Sylow, we call them p-primary. So decompositions match p-primary pieces.

How do we prove uniqueness? Similar set up to $\mathbb{Z}$. For uniqueness for $\mathbb{Z}$, we reduce to the case where $\#M = p^n$ for some t. Then $M \cong \bigoplus_{i=1}^t \mathbb{Z}/p^{e_i}\mathbb{Z} \cong \bigoplus_{i=1}^s \mathbb{Z}/p^{f_i}\mathbb{Z}$, and we want this to imply that $s = t$, $e_i = f_i$ for all i. In our general case, we have M p-power order and $M \cong \bigoplus_{i=1}^t R/p^{e_i}R \cong \bigoplus_{i=1}^s R/p^{f_i}R$, and want to say $s = t$, $e_i = f_i$.

Looking at $\mathbb{Z}$ first. Count elements of order $p, p^2, \ldots$, and these have to match. In our first decomposition, p^t elements of order $\leq p$ (since p divides the order of the cyclic group, and we know there exists a unique subgroup of order p for each cyclic group); this is to the power, since we get to choose one of these elements in each cyclic group. In our second decomposition, p^s elements of order $\leq p$. Hence, $t = s$. The equivalent for R a PID is $M[p] = \{m \in M \colon pm = 0\}$. Same argument works for the PID case. We "count" elements in $M[p]$. The problem: there is no particular reason for $M[p]$ to be finite. But $M[p]$ is a module over R/pR, which is a field since we're in a PID and pR is maximal, hence it is finitely generated since M is finitely generated (check). But a finitely generated module over a field is a vector space, so $M[p]$ is a finite dimensional vector space. s, t is the dimension, so they have to be the same.

Recall that for abelian groups, we had that there was a unique subgroup of each order. What is the analogue in the ring case? In R/p^eR, the elements annihalated by p are $p^{e-1}R/p^eR$, which are the elements divisible by p but not by p^e. This has dimension 1 over R/pR: it is generated by p^{e-1}. These cyclic submodules have something inside them For each thing dividing the order, p^e, there is ff. That's how you get $s = t$ in general.

It remains to deal with the exponents. Idea: look at $M[p^2], M[p^3]$. In our $\mathbb{Z}$ case, the trick is to consider $M/M[p]$. $M[p]$ matches up in 1 and 2, as we saw before, so we are able to mod it out (other things, like p, we are not sure is shared by both). In form (2), $M/M[p] \cong \bigoplus_{e_i \geq 2} \mathbb{Z}/p^{e_i - 1}\mathbb{Z}$ and form (3) gives $M/M[p] \cong \bigoplus_{f_i \geq 2} \mathbb{Z}/p^{f_i - 1}\mathbb{Z}$. The number of e_i where $i \mid e_i = 1$ is equal to the number of f_i where $i \mid f_i = 1$. Then the number of $e_i = 1$ is equal to the number of $f_i = 1$. We repeat this until we're done. Therefore, we get uniqueness for torsion modules.

Example: say we have $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}$. If we factor out by the elements of order p, our first summand gets modded out, and the second one becomes $\mathbb{Z}/p\mathbb{Z}$. Something something quotients commute with direct sums??? Would have to check that $M[p]$ is the direct sum of its pieces of $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z}$.

How do we get this for general modules (not torsion)? We have $M \cong R^n \oplus R/p_i^{e_i}R$. Say this is decomposition 1.

$$M^{\text{tor}} = \{m \in M \colon \exists r \neq 0, mr = 0\} = (\underbrace{0, \dots, 0}_{n \text{ slots}}, \dots)$$

Say we have another decomposition 2. $M \cong R^s \oplus$torsion. Torsion matches in both decompositions (where we proved uniqueness, but not needed here), since isomorphisms must map torsion to torsion. Now $M/M^{\text{tor}} \cong R^n \cong R^s$, and so $n = s$. Thus, we have proven uniquness of decompositions. Note: there is not a unique choice, no canonical choice of our free part. This could be infinite order, or just choose a different basis, etc. But the point is that $n = s$.

The set of things with infinite order is not a group. With $\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, we have $m_1 = (1, 1)$ and $m_2 = (1, 2)$ both have infinite order, but $m_1 - m_2$ has order 3.

Will see some applications of the theorem starting next week. The midterm will be up to 3.9. Won't have to compute Smith normal form by hand.

15 March 26

15.1 Applications of the structure theorem

There's only one thing left to do, and that is the applications of the structure theorem, specifically to linear algebra.

Let $R = \mathbb{Z}, k[X]$ where k a field. Suppose M is a finitely generated abelian group, or $M = k^n$ with mutliplication $X \mapsto A = n \times n$ matrix.

In the case of $\mathbb{Z}$, we have $M \cong \mathbb{Z}^n \oplus M_{\text{tor}}$, where M_{tor} are the elements of finite order $\cong$ direct sum of cyclics of prime power order (unique). This allows us to classify all finite abelian groups of given order.

In the case of $k[X]$, our answer depends on A. Structure theorem says $k^n \cong k[X]^m \oplus M_{\text{tor}}$. But recall that the left has dimension n, and $k[X]$ is infinite dimensional, hence $m = 0$. So what is M_{tor}? It is the direct sum of $k[X]$ mod prime powers. What are primes in $k[X]$? They are irreducible polynomials. So we get that k^n with action of A corresponding to multiplication by X is

$$k^n \cong \bigoplus k[X]/p_i(X)^{e_i}$$

where p_i are irreducible (the isomorphism is as a $k[X]$ module). Note that the polynomials p_i and exponents e_i depend on what A.

Let's forget about A for now, and look at the right hand side. Let $V_i = k[X]/p_i(X)^{e_i}$. Let $f(X) = p_i(X)^{e_i} = a_0 + a_1X + \cdots + a_rX^r$. Then V_i is the span of $\{1, X, X^2, \dots, X^{r-1}\}$ (long division). Call v_i the coset of X^i. The v_i are a basis for V_i. Multiplication by X has a simple expression in this basis. $1 \mapsto X$, $X \mapsto X^2$, $X^{r-1} \mapsto X^r = -a_{r-1}X^{r-1} + \cdots + a_0 + (f(X))$ (have to do the long division)... wait apparently this is $X^r = -a_{r-1}X^{r-1} - \cdots - a_0$, so $v_{r-1} \mapsto -a_{r-1}v_{r-1} - \cdots - v_0$. So multiplication by X on v_i is represented by the matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{r-1} \end{pmatrix}$$

For something more concrete, consider $\mathbb{Q}[X]/(X^3 + 2X + 3)$. This is spanned by cosets of $1, X, X^2$. Then $v_0 = 1 \mapsto X = v_1$, $v_1 = X \mapsto X^2 = v_2$, and $v_2 = X^2 \mapsto X^3 = -2X - 3 = -2v_1 - 3v_0$. This looks like the matrix (with respect to the basis $1, X, X^2$):

$$\begin{pmatrix} 0 & 0 & -3 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{pmatrix}$$

We call these matrices companion matrices of f_i: 1s on the off diagonal below and the negative coefficients of f_i in the last row.

Now returning back to the structure theorem. Each term on the right hand side (in the direct sum) is understood via matrix action whose entries come from coefficiens of $f_i(X)$. So we have some unknown matrix A on the left for k^n, and we are modelling it as matrices of the form that we just described above. **There exists a basis for k^n such that A decomposes as blocks, each block is a companion matrix with entries coming from $f_i(X)$.** The structure theorem doesn't tell you what these "companion matrices" are, which polynomials they are, but we will figure out how to get that from A now. The key thing is to analyze these blocks.

Spoiler: the p_i come from Smith form of $A - XI$. We'll prove this later.

15.1.1 Decomposing A

Consider $f(X) \in k[X]$, arbitrary, degree r. $k[X]/f(X)$ is a vector space of dimension r. The standard basis is $1, X, X^2, \ldots, X^{r-1}$, for which multiplication by X is the companion matrix of f.

Let $f(X) = X - \alpha$. $k[X]/(X - \alpha)$ has dimension 1. Let e_0 be the coset of 1, forms a basis. Multiplication by X gives $1 \mapsto X = \alpha$. So we get the 1 block $\begin{pmatrix}\alpha\end{pmatrix}$. Then $Xe_0 = \alpha e_0$ (X to be interpreted as a matrix here???). e_0 is an eigenvector and α an eigenvalue... $X - \alpha$ correspond to eigenvectors (I think he means for any polynomial, we can decompose into a factor here, we get an eigenvector).

In general fields, $p_i(X)$ has degree > 1, don't get eigenvector in the usual sense.

Next case: $(X - \alpha)^e = f(X)$. $V = k[X]/f(X)$ has dimension e. We got the power of an irreducible. We have $f(X)$ is a prime power. Last class, we saw that we had a cyclic group of prime power order. In this, we had p elements of order p (generally, p elements of order $p, p^2, \ldots, p^{n-1}$???). What is the equivalent here? $(X - \alpha)v = 0 \iff v$ is annihilated by $X - \alpha$. But this is just the eigenvector condition: $Xv - \alpha v = 0$. The elements annihilated by $X - \alpha$ are precisely the multiples of $(X - \alpha)^{e-1}$ modulo $(X - \alpha)^e$. But this space is 1 dimensional. So we have a unique eigenvector (up to scalar multiples). So even though we have dimension e, we have a unique eigenvector. This is similar to the case when we have repeated eigenvectors in a vector space.

The standard basis for such V (the companion basis) is messy, it depends on the coefficients of $(X - \alpha)^e$, which is a mess. But there is a simpler basis, $1, (X - \alpha), (X - \alpha)^2, \ldots, (X - \alpha)^{e-1}$. Call these $w_0, w_1, \ldots, w_{e-1}$. Multiplication by $(X - \alpha)$ gives $w_0 \mapsto w_1$, $w_1 \mapsto w_2$, etc. $w_e \mapsto 0$. This corresponds to the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \leftrightarrow X - \alpha I$$

And so if this matrix is M,

$$X = \alpha I + M$$

Which is a matrix in Jordan block form. We only get that this is diagonalizable when p_i is linear (e.g. over $\mathbb{C}$). So diagonlizable over $\mathbb{C} \iff$ no factors $(X - \alpha)^e$, $e > 1$. This explains the thing in linear algebra where some matrices are not diagonalizable. α comes from the characteristic polynomial???

Recap: start wth A, an $n \times n$ matrix over k. k^n as $k[X]$-module $\cong \bigoplus k[X]/p_i(X)^{e_i}$ where p_i is irreducible $e_i \geq 1$ (some unkown p_i, e_i). For any K, A breaks up (after some change of basis) to blocks of companion form for these $f_i = p_i^{e_i}$. This is called rational canonical form. Linear irreudicibles correspond to eigenvectors. Each factor $f(X) = (X - \alpha)^e$ gives a 1-dimensional eigenspace, which are multiples of $(X - \alpha)^{e-1}$. This is true over any field (don't always have linear things though), but over $\mathbb{C}$, all p_i are linear, so A diagionalizable $\iff \forall e_i = 1$. And if $e_i > 1$, we get a Jordan block form. (We can't get Jordan block if we can't decompose into linear factors, which could happen if k is not $\mathbb{C}$.)

This should convince you that the structure theorem completely controls the structure of these matrices, provided you know what the p_i, e_i are.

15.1.2 Finding the polynomials

Unknown: how to find p_i, e_i from A. This is a Smith normal form problem. The analogy to keep in mind is abelian groups: if I give you a number, like 50, and ask for all abelian groups of that order, there are going to be a lot that correspond to that same order.

We have $\mathrm{Ann}(k^n) = \prod p_i^{\max(e_i)}$ = "order" of A, where max is taken for fixed irreducible polynomial p_i.

Fact: $\prod p_i^{e_i}$ = the characteristic polynomial of A. We will do this next time. It will be cool how characteristic polynomial shows up, because it's not obvious.