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 $(x+i_1)\cdot(y+i_2) = xy + xi_2 + i_1y + i_1i_2 \in xy + I$. 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).