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.