MA294 Lecture

Timothy Kohl

Boston University

March 19, 2024

Rings, Fields and Polynomials

Beyond groups, there are other algebraic systems which are fundamental to many areas of pure and applied mathematics.

Definition

A ring is a set R together with two binary operations $+$ (addition) and $\cdot$ (multiplication) which satisfy the following properties.

- $(R, +)$ is an abelian group, i.e. $0 \in R$, addition is associative and commutative and for every $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$
- R is closed under $\cdot$, and $\cdot$ is associative, namely $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- For $a, b, c \in R$, one has $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ (i.e. the distributive law holds)

The most fundamental examples we can give involve the integers, or variations thereof.
For example $(\mathbb{Z}, +, \cdot)$ the integers with the usual addition and multiplication are a ring.

And, as we saw early on, $(\mathbb{Z}_m, +, \cdot)$ namely the integers mod m (for $m > 1$) with addition and multiplication mod m are all rings.

Note, another example, although of a slightly different characters is $(2\mathbb{Z}, +, \cdot)$ which is the set of even integers under ordinary addition and multiplication.

This last example is a bit different than $\mathbb{Z}$ in one important way, which we shall discuss in the next slide.

Note:

- If R has an element 1 such that $a \cdot 1 = a$ and $1 \cdot a = a$ we say that R is a ring with unity and most of the rings we will consider *will* be rings with unity. So for example $\mathbb{Z}$ is a ring with unity, but $2\mathbb{Z}$ is a ring *without* unity.
- Even if R is a ring with unity, $(R, \cdot)$ can never be a group as not all elements will have mulitplicative inverses, i.e. there may be $a \in R$ such that for **no** b do we have $a \cdot b = 1$, principally $a = 0$!
- Notationally, we will eventually suppress the '$\cdot$' and write a product like $a \cdot b$ as simply ab.
- The multiplication in R need not be commutative, and indeed there are important examples of rings with a non-commutative multiplication, namely there are elements a, b such that $ab \neq ba$.
- If $ab = ba$ for all $a, b \in R$ we call R a commutative ring.

Speaking of non-commutative rings, here is a prime example.

Definition

For $M_2(\mathbb{R}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}\}$ let addition be defined by:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}$$

and multiplication be defined by

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}$$

In linear algebra one learns that for $A, B, C \in M_2(\mathbb{R})$

$$A + B = B + A$$
$$A + (B + C) = (A + B) + C$$
$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ is the additive identity}$$
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
$$\downarrow$$
$$-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} \text{ is the additive inverse}$$

So we have the following.

Proposition

$M_2(\mathbb{R})$ is a ring with unity where the matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the additive identity, and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the mulitplicative identity (unity).

Note: For rings, we don't use the term 'abelian' or 'non-abelian' but rather commutative, or non-commutative.

Before going further, we mention a few basic facts about rings, which arise from their definition.

Properties of Rings

Let R be a ring, and let $a, b, c \in R$.

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = ab$
4. If we define $b - c$ to mean $b + (-c)$ then $a \cdot (b - c) = a \cdot b - a \cdot c$ and $(b - c) \cdot a = (b \cdot a - c \cdot a)$. If R has unity 1 then
5. $(-1) \cdot a = -a$
6. $(-1) \cdot (-1) = 1$

Let's examine some of these.

FACT 1: $a \cdot 0 = 0$ and $0 \cdot a = 0$
PROOF: Consider $a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ by the distributive law, but since 0 is the additive identity, $0 + 0 = 0$ so we have

$$a \cdot 0 = a \cdot 0 + a \cdot 0$$

and if $-a \cdot 0$ is the additive inverse of $a \cdot 0$ (which exists) then

$$a \cdot 0 = a \cdot 0 + a \cdot 0$$
$$\downarrow$$
$$a \cdot 0 + (-a \cdot 0) = a \cdot 0 + a \cdot 0 + (-a \cdot 0)$$
$$\downarrow$$
$$0 = a \cdot 0 + 0$$
$$\downarrow$$
$$0 = a \cdot 0 \qquad \square$$

FACT 3 $(-a) \cdot (-b) = ab$
Going forward, let's drop the '$\cdot$' for multiplication unless we need it!

PROOF: Consider $(-a + a)(-b)$ which equals $0(-b)$ which is 0 by FACT 1.
However it also equals $(-a)(-b) + a(-b)$ but by FACT 2, $a(-b) = -(ab)$ so we have

$$\begin{array}{r} (-a)(-b) + (-(ab)) = 0 \\ \downarrow \\ (-a)(-b) = ab \end{array}$$

The other facts are left for exercises.

Now, we discussed 2×2 matrices in the discussion of the group $GL_2(\mathbb{R})$ and this has some bearing on the structure of $M_2(\mathbb{R})$ as a ring.

We saw that $\delta = det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ characterizes whether the matrix is invertible, namely when $\delta \neq 0$.

For example $A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ does not have matrix inverse since $det(A) = 0$, or more directly

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

implies

$$\begin{aligned} a + 2c &= 1 \\ b + 2d &= 0 \\ 2a + 4c &= 0 \\ 2b + 4d &= 1 \end{aligned}$$

which is impossible.

Definition

For ring R, an element $x \in R$ is invertible (or a unit) if there exists $y \in R$ such that $xy = 1$ and $yx = 1$.

We have seen that the invertible elements of $\mathbb{Z}_m$, namely $U(m)$ are a group, as is $GL_2(\mathbb{R})$ mentioned above. In general we have:

Definition

For a ring R with unity, the units $U(R)$ are a group with respect to the multiplication in R.

We note that this touches back on the comment earlier that $(R, \cdot)$ is not a group, and it isn't a group, because not every element has a multiplicative inverse, which is quantified by the group $U(R)$.

Examples:

- $R = \mathbb{Z}_m \to U(R) = U(m)$

- $R = \mathbb{Z} \to U(R) = \{\pm 1\}$ (Why?)

- $R = \mathbb{Q}$ (the rationals) implies that $U(R) = \mathbb{Q}^*$, namely the non-zero elements of $\mathbb{Q}$.

- $R = M_2(\mathbb{R}) \to U(R) = GL_2(\mathbb{R})$.

Note: The case of $U(\mathbb{Q}) = \mathbb{Q}^*$, namely that all non-zero elements are units, leads to an important class of rings.

Definition

A commutative ring F is a field if $U(F) = F^* = F - \{0\}$, namely that all non-zero elements of F are invertible.

As we mentioned earlier, in a ring, 0 is never invertible, the reason is that, one can show that in any ring ring $0r = 0$ for any $r \in R$.

So for a field, F we have that $U(F)$ is as big as it can possibly be.

Here are some fundamental examples of rings.

- $\mathbb{Q}$, the rational numbers, e.g. 1, -2, $\frac{1}{3}$, etc.

- $\mathbb{R}$, the real numbers, namely the rationals plus irrationals like π, e, $\sqrt{2}$ etc.

- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R};\ i^2 = -1\}$, the complex numbers where
  $(a + bi) + (c + di) = (a + c) + (b + d)i$
  and (because $i^2 = -1$) $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$

If $z = a + bi \in \mathbb{C}$ where $(a, b) \neq (0, 0)$ (i.e. not the zero element of $\mathbb{C}$) then we have

$$\begin{aligned} \frac{1}{a+bi} &= \frac{1}{a+bi}\frac{a-bi}{a-bi} \\ &= \frac{a-bi}{a^2+b^2} \\ &= \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i \end{aligned}$$

where (since $a, b \in \mathbb{R}$ are not both zero) we have that $a^2 + b^2 > 0$ and so

$$\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i \in \mathbb{C}$$

which means every non-zero element of $\mathbb{C}$ has a multiplicative inverse, which confirms that $\mathbb{C}$ is a *field*.

In all of these examples, the field is infinite in size.

However, there is another important class of examples, namely $\mathbb{Z}_p$ for p prime since

$$U(\mathbb{Z}_p) = U(p) = \{1, 2, \ldots, p-1\} = \mathbb{Z}_p - \{0\}$$

so that $\mathbb{Z}_p$ are all 'finite fields'.

This includes also, the tiny, yet important example, $\mathbb{Z}_2$ which is essential to many applications, as we shall see.

Note: For *any* field F one may construct the ring of (2×2) matrices over

$$M_2(F) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in F\}$$

and similarly consider $GL_2(F) = U(M_2(F))$.

And for finite fields like $\mathbb{Z}_2$ these can be computed without too much effort since, if you recall from linear algebra, a matrix M is invertible if the columns of M form a basis, so for 2 matrices, this would be a basis of F^2.

Recall that the zero vector $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ is never part of a basis, and for a two dimensional vector space, a basis consists of two vectors $\{\vec{v}_1, \vec{v}_2\}$ where $\vec{v}_2$ is not a scalar multiple of $\vec{v}_1$.

So we have 3 choices for $\vec{v}_1 = \begin{pmatrix} a \\ c \end{pmatrix}$ and therefore 2 choices for $\vec{v}_2 = \begin{pmatrix} b \\ d \end{pmatrix}$.

$$GL_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

So $GL_2(\mathbb{Z}_2)$ has six elements and is a non-abelian group, and, in fact, one can show that $GL_2(\mathbb{Z}_2) \cong S_3$.

Another way to prove this, would be do write down all $2^4 = 16$ matrices of size 2×2 with entries from $\mathbb{Z}_2$ and remove those whose determinant is zero and the remaining matrices would be exactly the six shown on the previous slide.