Introduction to Algebra - Lecture Notes

by Toby Chen - Mathematics at Queen Mary's University of London

February 26, 2024

Contents

1 Week Three

1.1 Lecture One

1.2 Lecture Two

1.2.1 Introduction

Example of Modular Arithmetic, choose an integer $n = 11$, such that $12 \equiv 1 \mod n$, and equally the following statement is true, $3 \equiv 25 \mod n$. Lets check the results. $12 \equiv 1 \mod n$ is true because $1 - 12 = (-11)$, which is divisible by 11. We can also check $3 \equiv 25 \mod n$, and this is true because $25-3 = 22$ which is divisible by $n = 11$.

We can use the counter example of $4 \equiv 25 \mod n$, which is **not** true because $25-4 = 21$, which is not divisible by $n = 11$.

We should recall that we have proved that $\equiv$ on $\mathbb{Z}$ is in fact an equivalence relation, i.e., $\equiv = \mathcal{R}$. Recall that an equivalence relation $\mathcal{R}$ on $\mathcal{S}$ can produce equivalence classes $[a]_{\mathcal{R}}$, such that $a \in \{b \in \mathcal{S} : a\mathcal{R}b\}$.

Example of Equiv Classes, let $n = 11$, therefore $[3]_{11} = \{b \in \mathbb{Z} : 3 \equiv b \mod 11\}$ which produces $\{3+11k : k \in \mathbb{Z}\}$. This is an **equivalence class**.

1.2.2 Last Monday

We defined addition, subtraction and multiplication on the set $\mathbb{Z}_n$ of equivalence classes $[a]_n$, i.e., $[a]+[b] \equiv [a+b]$, and similarly $[a][b] = [ab]$. Note that $[a] + [b] \neq [a] \cup [b]$. Also note that we cant define division in the same sense, that being that we cant state that $\frac{[a]}{[b]}$ does not exist.

Recall that $a, b \in \mathbb{Z}$ such that $a \mid b \in \mathbb{Z}$. If $\exists c \in \mathbb{Z} : b = ac$, we can see that $c = \frac{a}{b}$.

1.2.3 Definition

Let $[a] \in \mathbb{Z}_n$. If there exists an integer $b \in \mathbb{Z}$, such that $[a][b] = [ab] = [1]$, then we call this equivalence class $[b]$ the multiplicative inverse of $[a]$. *note,* $[b]$ plays a role of $\frac{[1]}{[b]}$.

Example, take $n = 5$. What is the multiplicative inverse of $[2]_5 \in \mathbb{Z}_5$? *We need to find* $b \in \mathbb{Z} : [2][b] = [1]$. Therefore, since $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$, we will solve this via trial and error. Try $[b] = [1]$, therefore $[2][1] = [2] \neq [1]$, hence its not $[1]$. Try $[b] = [3]$ such that $[2][3] = [6] = [1]$. So $[3]$ is the multiplicative inverse of $[2]$.

1.2.4 Exercise

Let $n = 6$, what is the multiplicative inverse of $[-1]$?

My attempt, we will try trial and error. Try $[b] = 1$, ...

Answer, Try $[-1]$ such that $[-1][-1] = [1]$, and so $[-1]$ is the multiplicative inverse of $[-1]_6$.

1.2.5 Exercise

What is the multiplicative inverse of $[2]_6$ in $\mathbb{Z}_6$?

Answer, No multiplicative inverse. Why? If it did there would be $b \in \mathbb{Z} : [2][b] = [1]$, however we know that, $[2b] \equiv [1] \mod 6$. But, given $r \equiv s \mod n \iff [r] \equiv [s]$, we can say that,

$$\begin{aligned}
&\implies 2b \equiv 1 \mod 6, \\
&\implies 6 \mid 2b - 1, \\
&\implies 6 \text{ not } \mid 2b - 1 \text{ becuase contradiction.}
\end{aligned}$$

1.2.6 Theorem 12

The equivalence class $[a] \in \mathbb{Z}_n$ has a multiplicative inverse iff $\gcd(a, n) = 1$.

Proof of Theorem 12, "Lets prove the if part of the "statement", i.e., if $\gcd(a, n) = 1$, then $[a]$ has a multiplicative inverse in $\mathbb{Z}_n$. And Since $\gcd(a, n) = 1$, it follows from Bezouts identity that $\exists b, c \in \mathbb{Z} : ab+nc = \gcd(a, n) = 1$.

$$\implies 1 \equiv ab \mod n.$$

This is because $ab - 1 = nc$, and therefore is divisible by n.

$$\implies [1] = [ab] = [a][b].$$

Q.E.D.

1.2.7 Example

let $n = 2023$. What is the multiplicative inverse of $[23]_2023 \in \mathbb{Z}_2023$? One should notice that we simply cant just use a trial and error method here as there are too many possibilities to try. How might we go about this (use theorem 12)?

Solution, we need to workout $r, s, \in \mathbb{Z} : 2023r + 23r = \gcd(2023, 23)$. Therefore we use Euclid's algorithm,

$$\begin{aligned}
&2023 = 23 \times 87 = 22, \\
&23 = 22 + 1 \therefore \gcd(2023, 22) = 1.
\end{aligned}$$

We can now work "back up",

$$\begin{aligned}
&1 = 23 - 1 \times 22, \\
&\ = 23 - 1 \times (2023 - 23 \times 88), \\
&88 \times 23 + (-1) \times 2023.
\end{aligned}$$

So [88] is the multiplicative inverse in $\mathbb{Z}_2023$.

2 23/02/2024

2.1 Recall

Last week (not here) we defined a group, **Def**: A group $(G,)$, is a set G with operation , satisfying (G_0) if $a, b \in G, ab \in G$, and if (G_1) if $a, b, c \in G, a(bc) = (ab) * c$, and if (G_3) if for every element $a \in G\ \exists\ b \in G : ab = b \times a = e$...

!!!REVISE GROUPS!!!

2.2 Rings

2.2.1 Definition of a Ring

A ring is a set R, which comes equipped with two operations, $+$ and $\times$ (these may not be addition and multiplication as we known). These satisfy conditions,

1. $(R + 0)$ if $a, b \in R$, then $a + b \in R$.
2. $(R + 1)$ if $a, b, c \in R$, then $a + (b + c) = (a + b) + c$ which is in R.
3. $(R + 2)$ if there is a element a and 0, "zero", in R, satisfying the condition $a + 0 = 0 + a = a\ \forall R$.
4. $(R + 3)$ if for every element $a \in R$, there exists $b \in R : a + b = b + a = 0$.
5. $(R + 4)$ if $\forall\ a, b \in R, a + b = b + a$.
6. $(R \times 0)$ if $\forall\ a, b \in R, a \times b \in R$, i.e., its a closed group(?).
7. $(R \times 1)$ if $a, b, c \in R : a \times (b \times c) = (a \times b) \times c$.
8. $(R \times +)$ if $a, b, c \in R$, then $a \times (b + c) = a \times b + a \times c$.
9. $(R + \times)$ if $a, b, c \in R$, then $(b + c) \times a = b \times a + c \times a$.

Remarks:

1. Note that $a \times (b + c)$ is not necessarily then same as $(b + c) \times a$.

2. By $(R+0) - (R+4), (G,) = (R, +)$, i.e., a ring is a group.
3. We write ab for $a \times b$.
4. A ring $(R, +, \times)$, is said to be a commutitative ring if $\forall\ a, b \in R, ab = ba$.

Lets consider some example, 0 is the identity element with respect to $+$, and so needs to be in a ring R. Therefore the smallest ring we know is,

$$0 = \begin{cases} 0 + 0 = 0, \\ 0 \times 0 = 0. \end{cases}$$

This is the smallest possible ring, simply because there is only one element, and this is a requirement for a ring. Secondly consider $\mathbb{Z}, +, \times$. This is a ring.

Now consider $\mathbb{C}[x]$, to be the set of polynomials in one variable x, with coefficients in $\mathbb{C}$,

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c, c_i \in \mathbb{C}.$$

Note that all of the above are commutitative, the following is not. The set $M_2(\mathbb{C})$ of 2- by- 2 matrices with entries in $\mathbb{C}$ is a ring, i.e.,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}, a, b, c, d \in \mathbb{C}$$

This defines addition for a 2- by- 2 matrix. Multiplication is given by,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}, a, b, c, d \in \mathbb{C}$$

This $M_2(R)$ is not commutitative, $A, B \in M_2(R)$ because ???.

Let $(G,)$ be an abelian group by $(\mathbb{Z}, +)$, $(M_2(R), +)$. Define $+$ to be . Define,

$$\times = \begin{cases} \forall\ a, b \in G, \\ a \times b = e. \end{cases}$$

where e is the identity element in $(G,)$.

For $\sqrt{-1} = i$, we can have $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$.

3 Groups

We will now look at groups and look at their properties. We can now see two motivations for the group

4 26/02/2024

4.1 Last Weeks Recap

A ring is a is a set R with $+, \times$ where R_0 if $a, b \in R$ then $a + b \in R$. R_1 if $a, b, c \in R : a + (b + c) = (a + b) + c$. R_2 if $\exists\ 0 \in R : 0 + a = a + 0 = a$. R_3 if $\forall\ a \in R\ \exists\ b \in R a + b = b + a = 0$. R_4 if $a, b \in R : a + b = b + a$. Note that R_0 to R_4 is an abelian group. A ring be definition is an abelian group. This also refers to $+$. $R_{0\times}$ if $a, b \in R : a \times b = ab \in R$. $R_{1\times}$ if $a, b, c \in R : a \times (b \times c) = (a \times b) \times c$. $R_{\times +}$ if $a, b, c \in R : a \times (b + c) = a \times b + a \times c$. The reverse is also a condition.

Remarks:

1. $(R, \times)$ is not a group. This is because there is no identity element with respect to $\times$. Note that there is also no inverse.

4.1.1 Definition

$\forall\ a, b \in R : ab = ba$, then therefore R is commutitative, this is known as a abelian group.

example, $\{0\}$ with addition is $0 + 0 = 0$ and with multiplication $0 \times 0 = 0$.

example, $(\mathbb{Z}, +, \times)$ is a commutitative ring.

example, $(\mathbb{Z}_n, +, \times) = \{[0], [1], [2], \ldots, [n-1]_n\}$.

example, If $(G,)$ is an abelian group then $(G, , \times)$ is a ring where $\forall a, b \in G : a \times b = e$, e is the identity element of G. We can now look at $R_{\times +}$ to see that $a \times (b + c) = a \times b + a \times c$. The LHS gives $a \times (b + c) = e$, therefore $a \times b = e$ and $a \times c = e$, tje identity element. Therefore we have $a \times b + a \times c = e \times e = e$. This is because G, is a group.

Example, If $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$.
Example, If $M_2[\mathbb{R}] := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$.

Example, the set of all functions from $\mathbb{R} \to \mathbb{R}$ defines a ring. Take for example $f, g : \mathbb{R} \to \mathbb{R} : (f + g) : \mathbb{R} \to \mathbb{R}$, where $x \mapsto f(x) + g(x)$, and also $x \mapsto f(x)g(x)$.

4.2 New Content

Recall that $(R, +)$ is an abelian group.

4.2.1 Proposition 15

Let $(R, +, \times)$ be a ring. The zero element with respect to $+$ is unique. Also, any element in R has a unique inverse with respect to $+$, i.e., $a \in R,\ \exists!\ b \in R : a + b = b + a = 0$. Lastly if $a + b = a + c$ then $b = c$.

4.2.2 Proposition 16

For every element $a \in R$ we have $a \times 0 = 0 \times a = 0$.

Proof, $\exists\ 0 \in R : a + 0 = 0 + a = a$. Therefore let $a = 0$, therefore $0 + 0 = 0$. multiply both sides by $a \in R : 0a + 0a = 0a \implies a(0 + 0 = 0a) \implies a(0 + 0) = a0 + 0$. We cna now deduce that $a0 + a0 = a0 + 0$, and using *Proposition 15* say $a0 = 0$.

4.2.3 Definition

Let $(R, +, \times)$ be a ring. If R has an element 1: $a \times 1 = 1 \times a = a\ \forall\ a \in R$, then we say that R is a ring with an identity element. This is known as the multiplicative identity. Note that the additive identity is 0. Some rings may include $(\mathbb{Z}, +, \times), (\mathbb{R}, +, \times), (\mathbb{Q}, +, \times)$. $\{0\}$ is a ring with the identity 0, because it is defined that $0 \times 0 = 0$.

If R is a ring with identity, then $M_2(\mathbb{R})$ of 2-2 matrices with entires in R is a ring with identity,

$$\begin{pmatrix} 1_R & 0 \\ 0 & 1_R \end{pmatrix}.$$

4.2.4 Theorem 17

$\mathbb{Z}_n :=$ the set of equivalence classes $[a]_n$ with respect to $\equiv \mod (n)$, is a commutitative ring with the identity $[1]$. This is because $[1][a] = [1a] = [a]$ and that $[a][1] = [a1] = [a]$.

Some rings indeed have no identities, i.e., $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ of even integers. This is because 1 is not even. Another *example* is consider $R = \left\{ f : \mathbb{R} \to \mathbb{R} : \int_0^\infty f(x)dx < \infty \right\}$. This is a ring without identity because for $\mathbb{R} \to \mathbb{R} : x \mapsto 1$, this giving $\int_0^\infty 1dx = \infty$.

4.2.5 Definition

Let $(R, +, \times)$ be a ring with identity. An element $a \in R$ is called a unit if $\exists\ b \in R : ab = ba = 1$. In other words $\{\text{units in } R\} = \{\text{elements in } R \text{ with multiplicative inverse}\}$.

4.2.6 Definition

Let R^x denote a set of units in $(R, +, \times)$ with identity.