MA542 Lecture

Timothy Kohl

Boston University

January 27, 2025

Definition

In a ring R with unity 1, it is possible for a given element $a \in R$ to have a multiplicative inverse namely an element $b \in R$ such that $ab = 1$ and $ba = 1$.

Example:

$R = \mathbb{Z}_5$, $a = 2$ has inverse $b = 3$ since $ab = 6 \equiv 1 (mod\ 5)$.

$R = M_2(\mathbb{Z})$, $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has inverse $B = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ since $AB = I$ the identity matrix.

Of course, not every element in a ring with unity will have a multiplicative inverse.

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.

Note, in a ring R with unity, the zero element **never** has a multiplicative inverse.

Why? Well by FACT 1 demonstrated above $a0 = 0$ for any $a \in R$ so $a0 = 1$ is impossible.

And like what one finds in a group the following is true in a ring with unity.

FACT: In a ring R with unity, for each $a \in R$ which has a multiplicative inverse, that inverse is unique (and denoted a^{-1}) and the unity element is unique.

PROOF: (Basically it's the same as the proof that one uses to prove inverses and the identity in a group are unique.)

The question of why R under multiplication is not a group is tied to the existence of those elements in the ring with multiplicative inverses.

Definition

An element of a ring R with unity that has a multiplicative inverse is called a unit.

Theorem

If R is a ring with unity then the set $U(R)$ of the units of R is a group with respect to the multiplication operation in the ring.

Proof.

It's clear that 1 is in $U(R)$ since $1 \cdot 1 = 1$ and for any $a \in U(R)$ one has $a^{-1} \in U(R)$ since by definition $a \cdot a^{-1} = 1$.The remaining detail to check is closure.If $a, b \in U(R)$ then $ab \in U(R)$ since for $c = b^{-1}a^{-1}$ we have $abc = abb^{-1}a^{-1} = aa^{-1} = 1$, the point being that ab is a unit with inverse c. □

Examples of Unit Groups

$U(\mathbb{Z}) = \{\pm 1\}$ Why? Well if $n > 1$ then $mn = 1$ is impossible.

$U(\mathbb{Z}_4) = \{1, 3\}$

In $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ $3 \cdot 3 = 1$ and $1 \cdot 1 = 1$ but $2 \cdot 1 = 2$, $2 \cdot 2 = 0$ and $2 \cdot 3 = 2$.

$U(\mathbb{Z}_7) = \{1, 2, 3, 4, 5, 6\}$

Why? By direct calculation $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$, and $6^{-1} = 6$.

If you look at the difference between

$$U(\mathbb{Z}_7) = \{1, 2, 3, 4, 5, 6\}$$

vs.

$$U(\mathbb{Z}_4) = \{1, 3\}$$

we see that, in particular, $U(\mathbb{Z}_7)$ is as 'large as possible'.

What's the difference?

In general we have

Theorem

$U(\mathbb{Z}_n) = \{r \in \mathbb{Z}_n \mid gcd(r, n) = 1\}$

which you may have already encountered in the previous semester.

The basic argument is that if $gcd(r, n) \neq 1$ then some multiple 'm' of r is 0 where $m < n$. So if r *were* a unit then $mrr^{-1} = (mr)r^{-1} = 0r^{-1} = 0$ but $m(rr^{-1}) = m$ which would mean $m = 0$, which means $gcd(r, n) = 1$ after all.

Note, if $n = p$ a prime then $U(\mathbb{Z}_p) = \{1, 2, 3, \ldots, p-1\}$.

i.e. $U(\mathbb{Z}_p) = \mathbb{Z}_p - \{0\}$.

This is not dissimilar to the fact that if R is say the rationals, reals, or complex numbers, that $U(R) = R - \{0\}$.

More on this later.

Units are important in dealing with the following question.

If $ab = ac$ for $a, b, c, \in R$ does it follow that $b = c$?

i.e. Can we just 'cancel' the common factor of 'a' from both sides?

Not always...

For example, let $R = \mathbb{Z}_8$ and observe that $2 \cdot 2 = 2 \cdot 6$ (since both sides are $4 \in R$) but clearly we can't cancel the factor of '2' on each side as this would imply that $2 = 6$.

Proposition

If R is a ring with unity and $a \in R$ is a unit then $ab = ac$ implies $b = c$.

Proof.

If $ab = ac$ then $a^{-1}(ab) = a^{-1}(ac)$ so that $(a^{-1}a)b = (a^{-1}a)c$ which means $b = c$ since $a^{-1}a = 1$. □

The point is, if $ab = ac$ then it need not be the case that $b = c$.

More on this later.

Division Rings and Fields

Definition

A ring with unity R is a division ring if every non-zero element of R is a unit.
A commutative division ring is called a field.

Examples:

$\mathbb{H}$ is a division ring

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields

Also $\mathbb{Z}_p$ for p a prime is a field (a finite field!)

More on fields later...

Subrings

For groups G, one has the notion of a subgroup $H \leq G$ which is a subset which is a group with respect to the same group operation as in G.

For rings there is a similar concept.

Definition

If R is a ring then a subset $S \subseteq R$ is a subring if S is also a ring with respect to the addition and multiplication in R.

i.e. S is closed with respect to $+$ and $\cdot$, and contains 0

(One does not need to check associativity or the distributive law since they hold in R by assumption.)

The question is, how does one determine if a given subset is a subring?

Proposition (Subring Test)

If $S \subseteq R$ and $a - b \in S$ and $ab \in S$ for all $a, b \in S$ then S is a subring.

Examples: $R = \mathbb{Z}$, $S = 2\mathbb{Z}$ (note $1 \in R$ but $1 \notin S$)

$R = M_2(\mathbb{R})$, $S = M_2(\mathbb{Z})$

$R = C^0(\mathbb{R})$ (continuous functions), $S = C^1(\mathbb{R})$ (differentiable functions)

$R = C^1(\mathbb{R})$, $S = \mathbb{R}[x]$ (the ring of polynomials with coefficients)

We'll talk more about polynomials later.

More examples:

$R = \mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$ (complex numbers)

$S = \mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$ (the Gaussian Integers - an important object of study in number theory)