MA542 Lecture

Timothy Kohl

Boston University

January 31, 2025

Finite Fields

Beyond $\mathbb{Z}_p$ there are many other finite fields.

Consider this example: $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3 \ i^2 = -1 = 2\}$.

The construction mirrors that of $\mathbb{C}$ from $\mathbb{R}$ but this example is a finite ring.

Indeed we can list out the elements explicitly:

$$\{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$$

so that $|\mathbb{Z}_3[i]| = 9$ which is not unexpected if we view it as the set of $\mathbb{Z}_3$-linear combinations of the 'basis' $\{1, i\}$.

This is analogous to how $\mathbb{C}$ is the $\mathbb{R}$-vector space with basis $\{1, i\}$.

The thing to check though is that this is a ring (easy) and that it is commutative (also easy) and that it is a domain. (not quite so easy)

If

$$(a+bi)(x+yi) = (ax-by)+(ay+bx)i = (ax+2by)+(ay+bx)i = 0+0i$$

then we can write this as a matrix equation $A\vec{x} = \vec{0}$ namely

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

and since $a, b \in \mathbb{Z}_3$ is a field, this has a unique solution (i.e. $x = 0, y = 0$) if $det(A) = a^2 - 2b^2 \neq 0$ but this is easy to check since if $a^2 - 2b^2 = 0$ then $a^2 = 2b^2$.

So $a = 0$ if and only if $b = 0$, and if $a \neq 0$ then $b \neq 0$ then $\left(\frac{a}{b}\right)^2 = 2$.

However, this means there is some number $r \in \mathbb{Z}_3$ such that $r^2 = 2$, i.e. $r^2 = -1$ but $0^2 = 0$, $1^2 = 1$ and $2^2 = 4 = 1$.

So $\mathbb{Z}_3[i]$ is a domain and thus a field.

An interesting (and natural) question is whether we can repeat this construction with $\mathbb{Z}_5$ replacing $\mathbb{Z}_3$, i.e.

$$\mathbb{Z}_5[i] = \{a + bi \mid a, b \in \mathbb{Z}_5 \; ; i^2 = -1 = 4\}$$

with the addition and multiplication defined in the way we did for $\mathbb{Z}_3[i]$.

Well, this ring is well defined, and is commutative, but... it is not a domain and therefore not a field.

As it turns out, $\mathbb{Z}_p[i]$ is a field (with p^2 elements!) only when $p \equiv 3 \; (mod \; 4)$, which is equivalent to the equation $x^2 + 1 = 0$ **not** having a solution in $\mathbb{Z}_p$.

Note: In $\mathbb{Z}_3[i]$ one has

$$3(a+bi) = (a+bi)+(a+bi)+(a+bi) = (3a)+(3b) = 0+0i$$

for any $a, b \in \mathbb{Z}_3$ which is an example of the following idea, whose defintion may seem a bit confusing at first.

Recall that in *any* ring R (with unity), $0x = 0$ and $1x = x$ for every $x \in R$ and for any positive integer n we can define $nx = x + x + \cdots + x$ (i.e. x added to itself n times).

Indeed, when we write nx the 'n' is a natural number, but can we regard 'n' as an element of the ring R?

Yes, in that if $1 \in R$ is our unity element then we can define $n \in R$ as

$$1 + 1 + \cdots + 1$$

namely 1 added to itself n times, which is guaranteed to be an element of R,

e.g. in $M_2(\mathbb{Z})$:

$$\begin{aligned} nI &= n \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \cdots + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} \end{aligned}$$

So in $M_2(\mathbb{Z})$, 'n' means $\begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$.

But for the definition we are about to give, we actually are more interested in $nx = x + x + \cdots + x$.

Definition

Let R be a ring, then if for some fixed $n > 0$ one has that $nx = 0$ for any $x \in R$ (but for no smaller non-zero n) we say that R has characteristic n, and we write $char(R) = n$.

If there is no such $n > 0$, i.e. $nx = 0$ for all $x \in R$ means $n = 0$ then we say that R has characteristic 0 and we write $char(R) = 0$.

Examples:

$char(\mathbb{Z}) = 0$

$char(\mathbb{R}) = 0$

$char(\mathbb{Z}_n) = n$

$char(\mathbb{Z}_3[i]) = 3$

$char(\mathbb{Z}_3 \times \mathbb{Z}_2) =? \ 6$

How about $char(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_3)$ for example?

A simple way to determine the characteristic is to look at the unity element 1.

Proposition

Let R be a ring with unity 1. If $\langle 1 \rangle$ (cyclic group under addition) has infinite order then $\text{char}(R) = 0$. If $|\langle 1 \rangle| = n$ then $\text{char}(R) = n$.

And based on our discussion earlier, it's not hard to demonstrate the following.

Proposition

The characteristic of an integral domain is either 0 or a prime.