Lecture 3

Finite fields

Recall: A field F is a set with two binary operations $+, \cdot$ s.t

i) $(F, +)$ is an abelian group.

ii) $(F-\{0\}, \cdot)$ is an abelian group.

iii) Distributive property

$$a \cdot (b+c) = a \cdot b + a \cdot c$$
$$(b+c) \cdot a = b \cdot a + c \cdot a$$

Examples: $F = \mathbb{Q}$ $\quad + =$ usual addition

$\cdot =$ usual multiplication

$(\mathbb{Q}, +, \cdot)$ is a field.

Non-example: $(\mathbb{Z}, +, \cdot)$ is not a field.

$2 \cdot x = 1$, there is none.

Characteristic of a field (ring)

1 multiplicative identity

0 additive identity

$1+1 = 2\cdot 1$

$\underbrace{1+1+1+\cdots+1}_{n} = n\cdot 1$

Is it possible that $n\cdot 1 = 0$ for some n?

Ans: Both Yes & No!

Over $\mathbb{Q}$ $n\cdot 1 = 0$ $n \in \mathbb{N}$

No!

Characteristic 0

Defn: Let F be a field (or a ring). The characteristic of F, denoted by $\mathrm{Char}(F)$

is the smallest natural number $\underline{n}$ such that $n \cdot 1 = 0$.

If no such n exists, we say that char(F) $= 0$.

<u>Aside:</u> Suppose F is a char 0 field.

$1 \in F$

$1+1 \in F$, . . . $n \in F$
$2 \in F$

$\mathbb{N} \subseteq F$

0 & Additive inverses are there

$\mathbb{Z} \subseteq F$

Multiplicative inverses are also there

$\boxed{\mathbb{Q} \subseteq F}$

($\mathbb{Q}$ is a subfield of F)

Non-zero characteristic

F field $\text{char}(F) = n \qquad n \neq 0$

(1) $\quad a, b \in F \qquad a \cdot b = 0$

HW Exc (1) Show that if a or b is 0 then $a \cdot b = 0$.

$a \neq 0 \ , b \neq 0$

$$a \cdot b = 0$$

Multiply it with a^{-1}

$$a^{-1}(ab) = a^{-1}0 = 0$$
$$(a^{-1}a)b = 0$$
$$1 \cdot b = 0$$
$$b = 0 \qquad \rightarrow\leftarrow$$

n Cannot be Composite $\Rightarrow$ n has to be prime

$$n = m_1 m_2$$
$$n \cdot 1 = 0$$
$$(m_1 \cdot 1)(m_2 \cdot 1) = 0$$

field F $\quad$ $\text{char}(F) \neq 0$

$\Rightarrow \text{char}(F) = p$ $\quad$ prime number

finite fields

$\mathbb{F}_p(x)$ has infinitely many elements.

<u>Finite fields:</u> $\mathbb{F}_p$ $\quad$ this is a field that contains exactly p elements

$p = 7$

$$\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$\downarrow$

Remainders when we divide by 7

$$4+5 = 2$$
$$4 \cdot 5 = 6$$

$$\mathbb{F}_p = \{0, 1, 2, 3, 4, \ldots, p-1\}$$

$a+b$ (remainder mod p)

$a \cdot b$ (————)

The reason $\mathbb{F}_p$ is a field is because of Euclid's lemma, the fact that gcd as a linear combination of two integers.

Exc: Show that $\mathbb{F}_p$ is a field.

$\{\mathbb{F}_p\}_{p \text{ prime}}$ are examples of finite fields but these are not all.

$\{\mathbb{F}_{p^r}\}_{\substack{p \text{ prime} \\ r \geq 1 \in \mathbb{N}}}$ are all the finite fields.

$\mathbb{F}_4 = \{0, 1, 2, 3\}$ $\quad 2 \times 2 = 4 = 0$

mod n construction is not Correct

$\mathbb{F}_2 \quad \{0, 1\}$

---

① Degree 2 polynomials over $\mathbb{F}_2$

$ax^2 + bx + c \qquad a, b, c \in \mathbb{F}_2$

(a, b, c)	ax^2+bx+c
0 0 0	0
0 0 1	1
0 1 0	x
0 1 1	$x+1$
1 0 0	$x^2 = x \cdot x$
1 0 1	$x^2+1 = (x+1)^2$
1 1 0	$x^2+x = x(x+1)$
1 1 1	x^2+x+1 doesn't factorize

(2) Look for polynomials of degree 2 that do not factorize

$$(x+1)^2 = x^2+2x+1 = x^2+1$$

x^2+x+1 is our candidate.

$\mathbb{F}_2[x]$ = {Set of all polynomials in one variable x & with coefficients in $\mathbb{F}_2$}

HW Exc: Check that $\mathbb{F}_2[x]$ is a ring under usual addition & multiplication.

Construct a quotient ring $\dfrac{\mathbb{F}_2[x]}{\langle x^2+x+1\rangle}$

Think of $\mathbb{Z}/p\mathbb{Z}$

Challenge HW

Show that $\dfrac{\mathbb{F}_2[x]}{\langle x^2+x+1\rangle}$ is a field. $\mathbb{F}_4$

Aside (Ideals)

$\longrightarrow \langle x^2+x+1\rangle = \{ f(x^2+x+1) \mid f \in \mathbb{F}_2[x] \}$

$$\frac{\mathbb{F}_2[x]}{\langle x^2+x+1\rangle} = \left\{ \begin{matrix} 0, & 1, & x, & x+1 \\ (0,0) & & & \end{matrix} \right\}$$

$$\left\{ \begin{matrix} 1+1=0 \\ 2x=0 \\ 2(x+1)=2x+2=0 \end{matrix} \right\}$$

(a,b) $\quad$ $(ax+b)$

$$\begin{matrix} 0\ 0 & & 0 \\ 0\ 1 & & 1 \\ 1\ 0 & & x \\ 1\ 1 & & x+1 \end{matrix}$$

$x+(x+1) = 2x+1 = 1$

$(1,0)+(1,1) = (2,1) = (0,1) = 1$

$x(x+1) = x^2+x = 1$

$x^2+x = (x^2+x+1) - 1$

$$\begin{array}{c} \mathbb{F}_{p^r} \\ | \\ \mathbb{F}_p \end{array}$$

$$\mathbb{F}_{p^r} = \mathbb{F}_p[x] \big/ \langle f \rangle \qquad \deg(f) = r$$

$$\simeq \mathbb{F}_p[x] \big/ \langle g \rangle$$

{ There is exactly one finite field of a given order up to isomorphism. }

Exc: $\mathbb{F}_8$ Construct $\mathbb{F}_8$ explicitly.

$$\begin{array}{c} \mathbb{F}_8 \\ | \\ \mathbb{F}_2 \end{array}$$

$\mathbb{Z}$	$\mathbb{F}_p[x]$
$\| \ \|$ to compare	degree to compare
$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{F}_p[x]/\langle f \rangle$
$\{0, 1, 2, 3, 4, \ldots, p-1\}$	$\{g \mid \deg g < \deg f\}$