Outline

Ring

Field

Polynomial Ring

Recap on group

Group is a set G with a operation $+$, $(G,+)$

satisfies

(1) closure : $\forall g,h \in G$, $g+h \in G$.

(2) identity : $\exists\ 0 \in G$, s.t $g+0=0+g=g\ \forall g \in G$

(3) inverse : $\exists\ g \in G$, $\exists\ (-g) \in G$. s.t $g+(-g)=(-g)+g=0$

(4) associativity : $\forall g,h,k \in G$, $(g+h)+k = g+(h+k)$

E.g: $(\mathbb{Z},+)$ is a group.

Ring is a set R with two operations $+, *$ $(R,+,*)$

satisfies

(1) $(R,+)$ is a commutative group.

(2) With respect to $*$:

(a) $\exists$ unique multiplicative identity, $1 \in R$ s.t $1*r=r*1=r$ $\forall r \in R$.

(b) $*$ is associative

(3) $+, *$ are distributive : $\forall a,b,c \in R$

$$(a+b)*c = (a*c)+(b*c)$$

E.g: $(\mathbb{Z},+,*)$ is a ring, $(\mathbb{Z}_n,+,*)$ is a ring

(can do addition, substraction, multiplication, but not division)

Field

A set F with two operations $+, *$ satisfy

(1) $(F, +)$ is a commutative group

(2) $(F \setminus \{0\}, *)$ is a commutative group.

(3) Distributive

E.g: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are infinite field

$\mathbb{F}_p = \mathbb{Z}_p$ where p is prime is a finite field

(can do addition, subtraction, multiplication, division)

Recap: $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ has multiplicative inverse.

$(\mathbb{Z}_p^*, *)$ is a group

Questions:

Q 1: Are there finite fields of arbitrary number of elements?

Q2: How to construct finite fields?

Theorems

① Any finite field has p^d elements (prime power).

② There exists a finite field of p^d elements for all prime power p^d.

③ All finite field of size p^d are isomorphic.

Polynomial Ring

$$f(x) = 3x^2 + 2x + 1$$

coefficients

degree

Polynomial over field F

Let F be a field.

$F[x] = \{ c_d x^d + c_{d-1} x^{d-1} + \dots + c_0 , \quad c_i \in F \}$

E.g.: In $F_2[x]$, $(x+1) \in F_2[x]$

$(x^2 + x) \in F_2[x]$

$$(x+1) + (x^2 + x) = x^2 + 2x + 1$$
$$= x^2 + 1 \quad \in \mathbb{F}_2[x]$$

$$(x+1)(x^2+x) = x^3 + x^2 + x^2 + x$$
$$= x^3 + x$$

$F[x]$ is not a field but a ring.
Just like ring of integers, we can add, subtract, multiply but not division.

$\mathbb{Z}$	$F[x]$, F is a field

Concept of division with remainder

$\mathbb{Z}$:

$a = bq + r$, $r < b$

$11 = 4 \cdot 2 + 3$

$F[x]$:

$f(x), g(x)$ in $F[x]$

$f(x) = g(x)q(x) + r(x)$

$\deg(r(x)) < \deg(g(x))$

$$
\begin{array}{r|l}
 & 3x^2 + 5 \\
\hline
2x^2 + 4 & 6x^4 + 8x + 1 \\
 & 6x^4 + x^2 \\
\hline
 & 10x^2 + 8x + 1 \\
 & 10x^2 + 9 \\
\hline
 & 8x + 3
\end{array}
\quad \text{in } \mathbb{F}_{11}[x]
$$

$6x^4 + 8x + 1 = (2x^2 + 4)(3x^2 + 5) + 8x + 3$

Concept of modulo

$\mathbb{Z}$:

$11 \bmod 4 = 3$

$F[x]$:

$6x^4 + 8x + 1 \bmod 2x^2 + 4 = 8x + 3$

Concept of quotient ring

$\mathbb{Z}$:

Take $n \in \mathbb{Z}$

$\mathbb{Z}_n = \mathbb{Z}/(n)$ is a ring

$F[x]$:

Take $f(x) \in F[x]$

$F[x]/(f(x))$ is a ring

Concept of prime	Concept of irreducible
integer p such that p has non trivial divisors $(1, p)$	$f(x) \in F[x]$ f is irreducible if it has no proper factors other than itself and a constant.
E.g. $2, 3, 5, 7,$	E.g: over $\mathbb{F}_3[x]$ $x+1$ is irreducible $x^2-1 = (x-1)(x+1)$ is not irreducible
$\mathbb{Z}_n$ is a field iff n is a prime.	$F[x]/(f(x))$ is a field iff $f(x)$ is irreducible.
All nonzero elements in $\mathbb{Z}_p$ where p is prime has multiplicative inverse	All nonzero polynomial in $F[x]/(f(x))$ where $f(x)$ is irreducible has multiplicative inverse
$\mathbb{Z}_p$ has p elements $\parallel$ $\mathbb{F}_p = \mathbb{Z}/(p)$	$F[x]/(f(x))$ has p^d elements where $f(x)$ is irreducible over $F[x]$ of degree d. and F is a finite field of order p.

$(\mathbb{Z}_p\setminus\{0\}, *)$ is cyclic $= \langle g \rangle$ (primitive element)

$(\mathbb{Z}_p, +)$ is cyclic $= \langle 1 \rangle$

$(\mathbb{F}_p[x]/(f(x)) \setminus \{0\}, *)$ is cyclic.

$(\mathbb{F}_p[x]/(f(x)), +)$ is cyclic ?

No, unless it has only p elements.

Construction of a finite field of order p^d

---

① Find an irreducible Polynomial over $\mathbb{F}_p$, with degree d, $f(x)$.

② The set $\mathbb{F}_p[x]/(f(x))$ is a finite field of order p^d.

Example: Construct a finite field of order $2^3 = 8$

① $f(x) = x^3 + x + 1$ over $\mathbb{F}_2$

Prove that $f(x)$ is irreducible over $\mathbb{F}_2$.

If $f(x)$ is not irreducible then

$f(x) = x^3+x+1 = (ax+b)(cx^2+dx+e)$

coefficients of				
	$x^3 =$	ca	$= 1$	$\rightarrow c=a=1$
	$x^2 =$	$cb + ad$	$= 0$	$\rightarrow d=1$
	$x =$	$ae + db$	$= 1$	
	$x^0 =$	be	$= 1$	$\rightarrow b=e=1$

There exists no $a, b, c, d, e \in \mathbb{F}_2$ that satisfy all the equations.

② $\mathbb{F}_2[x]/(f(x)) = \{0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1\}$

③ Find the primitive element / generator of $(\mathbb{F}_2[x]/(f(x)), *)$.

$x,\ x^2,\ x^3 = x+1,\ x^2+x,\ x^3+x^2 = x^2+x+1,\ x^3+x^2+x = x^2+1$

$x^3+x = 1$. x generates all nonzero elements in $\mathbb{F}_2[x]/(f(x))$