Chapter 11

11.1 Making Fields

- Construction of finite fields & computations in finite fields are based upon polynomial computations

$\mathbb{F}_q$: finite field with q elements

For a prime p, there is one such finite field, $\mathbb{Z}/p = \mathbb{F}_p$

$$GF(q) = \mathbb{F}_q$$

'GF' ~ Galois Field

Remark: issue of uniqueness of a finite field w/ a given # of elements
Hard to prove.

Remark: For a polynomial P (not necessarily irreducible), & for two other polynomials f, g, ~~with~~ all with coeff. in $\mathbb{F}_p$, write

$$f = g \bmod P$$

if P divides $f-g$ ← analogous to congruences for ~~orid~~ ordinary integers. And let's define

$$\mathbb{F}_p[x]/P = \{\text{congruence class mod } P\}$$

where the congruence class $\bar{f}$ mod P of a polynomial f is

$$\bar{f} = \{g \in \mathbb{F}_p[x] : g = f \bmod P\}$$

A polynomial f is reduced mod P if

$$\deg f < \deg P$$

Proposition: Two polynomials f, g which are reduced mod P are equal modulo P iff they are equal (in $F_p[x]$)

Proof. Certainly if f and g are equal then they are equal modulo P, whether or not they are reduced.

On the other hand, suppose f and g are reduced modulo P

and equal modulo P. Then

$$f - g = Q \cdot P$$

for some (quotient) polynomial Q. Looking at degrees,

$$\deg P > \max(\deg f, \deg g) \geq \deg(f-g) = \deg Q + \deg P$$

If all the degrees are integers, this is impossible. The only manner in which this can work out is that $Q = 0$, so by convention, $\deg Q = -\infty$. Thus $f - g = 0$

Theorem: For irreducible polynomial P of degree n, the ring

$$\mathbb{F}_p[x]\text{-mod-}P = \mathbb{F}_p[x]/P$$

of polynomials mod P is a field, with p^n elements. The element x-mod-P is a root in $\mathbb{F}_p[x]/P$ of the equation

$$P(x) = 0 \bmod P$$

Proof: From previous proof, the set of polynomials $f(x)$ of degree strictly less than the degree of P is an irredundant set of representatives for $\mathbb{F}_p[x]/P$, whether or not $P(x)$ is irreducible.

There are p choices (from $\mathbb{F}_p$) for each of the n coefficients of a polynomial of degree strictly less than n, so there are p^n choices altogether, and thus p^n elements in the quotient $\mathbb{F}_p[x]/P$.

Proving existence of multiplicative inverses for non-zero elements f in $\mathbb{F}_p[x]/P$. Given $f \neq 0 \in \mathbb{F}_p[x]/P$, we may suppose that $0 \leq \deg f \leq \deg P$

Since P does not divide f, we have

$$\deg \gcd(f, P) < \deg P$$

Since P irreducible, the $\gcd(f,P)$ cannot have a positive degree, or else it would be a proper factor of P. Thus

$$\deg \gcd(f,P) = 0$$

gcd is non-zero constant. we can adjust gcd's to be monic polynomials by mult. through by non-zero constants,

$$\gcd(f, P) = 1$$

so thus we have

$$af + bP = 1 \quad \text{EEA}$$

$$\Rightarrow \quad a \cdot f = 1 \bmod P \quad \leftarrow \text{multiplicative inverse}$$

Now, verify $\alpha = x\text{-mod-}P$ satisfies

$$P(\alpha) = 0 \bmod P$$

for any polynomial M there is polynomial N s.t.

$$P(x + M \cdot P) = N \cdot P$$

actually we want to prove that for any polynomial h,

$$h(x + M \cdot P) = h(x) \bmod P$$

By Binomial Theorem for any exp k,

$$(x + MP)^k = x^k + \sum_{1 \le i \le k} \binom{k}{i} x^i (MP)^{k-i}$$

i.e. $\quad (x + MP)^k = x^k \bmod P$

$\Rightarrow \quad h(x + MP) = h(x) \bmod P$ (adding together suitable constant multiples of powers)

In particular,

$$P(x + MP) = P(x) = 0 \bmod P$$

so x-mod-P is a root of the equation $P(y) = 0$ in $\mathbb{F}_p[x]/P$

$\square$

11.2 Ex.'s of field Extensions

- Making the complex numbers $\mathbb{C}$ a field extension of the real numbers $\mathbb{R}$
  - not presuming that there is a $\sqrt{-1}$ already existing somewhere

1st, we prove $x^2+1 \in \mathbb{R}[x]$ is irreducible

- x^2+1 has no roots in $\mathbb{R}$
- it is quadratic, so if it were to factor in $\mathbb{R}$ it would have to have two linear factors

- We know that $\mathbb{R}[x]$ mod x^2+1 is a field

Also, $x^2 = -1 \bmod x^2+1$

so x-mod-(x^2+1) is a $\sqrt{-1}$

we also showed (b/c every element has a unique reduced representative) that any element β of the extension is expressible uniquely in the form

$$\beta = a + b\alpha \quad \text{for } a, b \in \mathbb{R}$$

Ex. adjoining a square root of 2 to $\mathbb{Z}/5$

- There is no a in $\mathbb{Z}/5$ s.t $a^2 = 5$
- Thus x^2-2 does not factor in $\mathbb{Z}/5[x]$
- So $\mathbb{Z}/5[x]$ mod x^2-2 is a field, and

$$x^2 = 2 \bmod x^2 - 2$$

So x-mod-(x^2-2) is a square root of 2

11.3 Addition mod P

- Just add the corresponding coefficients of polynomials.
- the degree of a sum of polynomials is less or equal the max of their degrees, so the sum of two reduced polynomials is still reduced.

Ex. $\mathbb{F}_2[x]/(x^4+x+1)$

adding x^3+x+1 and x^2+x+1 gives

$$(x^3+x+1)+(x^2+x+1) = x^3+x^2+2x+2 = x^3+x^2 \mod x^4+x+1$$

since $2=0$

11.4 Multiplication mod P

- Oridinary multiplication of polynomials, then reduction modulo P

Ex. in $\mathbb{F}_2[x]/(x^4+x+1)$, mult x^3+x+1 and x^2+x+1 gives

$$(x^3+x+1)\cdot(x^2+x+1) = x^5+x^4+2x^3+2x^2+2x+1$$
$$= x^5+x^4+1 = x^2+1 \mod x^4+x+1$$

since $2=0$ and

$$(x^5+x+1)-(x)(x^4+x+1) = x^2+1$$

11.5 Multiplicative inverses mod P

- Use of Euclidean Algorithm
- Important that the modulus P is irreducible
- To find ~~an~~ the multiplicative inverse of f mod P such that $f \neq 0 \mod P$, use the EEA to find

polynomials S, T so that

$$S\cdot f + T\cdot P = 1$$

Then $S \cdot f - 1 = T \cdot P$,

so by definition of equality mod P

$$S \cdot f = 1 \bmod P$$

That is,

$$f^{-1} = S \bmod P$$

B/c f is not $0 \bmod P$ and P is irreducible, gcd of the two is 1

so S, T do exist

Ex. mult inverse of x in $\mathbb{F}_2[x]/(x^2+x+1)$

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

Thus,

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

from which

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

i.e.

$$x^{-1} = x+1 \bmod x^2+x+1$$

Exercises

11.01 In the field $K = (\mathbb{Z}/2)[x]/(x^2+x+1)$ let α be the image of x, and compute in reduced form α^5