lecture 6

Sept. 28

We closely follow the material in R. Friedman "Factorization in Polynomial rings" (online) and Rotman (Sections: Poly rings over fields p. 24–31, Prime ideals & maximal ideals 31–37).

Prop (Long division with remainder) $f \in F[x]$, $f \neq 0$. $\forall g \in F[x]$

$\exists!$ $q(x), r(x) \in F[x]$, $\deg r < \deg f$, such that

$$g = qf + r$$

$r=0$ included

$\deg(0) = -\infty$

common convention.

Corollary 1) For $f \in F[x]$, $f \neq 0$ cosets $g + (f)$ have unique representatives r, $\deg r < \deg f$.

2) Polynomials $r(x) \in F[x]$, $\deg r < \deg f$, are in a bijection with elements of $F[x]/(f(x))$

↑ principal ideal generated by f

Any ideal $I \subset F[x]$ has the form $I = (f(x))$ for some f, since $F[x]$ is a PID.

Get a model to work with $F[x]/(f(x))$

Elements: polynomials $a(x)$, $\deg a < \deg f$

Addition: $a(x) + b(x)$

Multiplication: $a(x)b(x) = q(x)f(x) + r(x)$

↑ product of a and b in $F[x]/I$.

$0, 1$ as usual.

Example $f = x^2+1$ $\quad F = \mathbb{R}$ $\quad \mathbb{R}[x]/(x^2+1)$.

Elements $a+bx$ $\quad a,b \in \mathbb{R}$ $\quad x^2=-1$ $\quad$ reduce

Multiplication $(a_1+b_1x)(a_2+b_2x) = a_1a_2 + (a_1b_2+a_2b_1)x + \underbrace{b_1b_2x^2}_{-b_1b_2}$

$= (a_1a_2 - b_1b_2) + (a_1b_2+a_2b_1)x$

Remark $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$ complex numbers

isomorphism is identity on $\mathbb{R}$, takes x to i

$$x \longmapsto i \qquad i^2 = -1$$

$$a+bx \longmapsto a+bi$$

Example $f = x^2-1$. $\quad R = \mathbb{R}[x]/(x^2-1)$.

$a = x+1$, $b = x-1$ $\quad ab = x^2-1 = 0$ in $R \Rightarrow R$ is not an integral domain

Example $F = \mathbb{F}_2 = \{0,1\}$ $\quad 1+1=0$ $\quad$ 2-element field

$f = x^3+x+1$ $\quad R = F[x]/(f) = F[x]/(x^3+x+1)$

$\mathbb{F}_8$ "unique" 8-element field

Elements $a_0 + a_1x + a_2x^2$ $\quad a_0,a_1,a_2 \in \mathbb{F}_2$ $\quad$ 8 elements

$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ $\quad x^3 = x+1 \pmod 2$ in quotient ring

Multiply: $\underset{a}{(x+1)} \cdot \underset{b}{x^2} = x^3 + x^2 = x^2+x+1$ $\quad$ reduce

$x \cdot x^3 = x(x+1)$ in R

$x^4 = x^2+x$

$\underset{a}{(x^2+1)}\underset{b}{(x^2+x)} = x^4 + x^3 + x^2 + x = (x^2+x) + (x+1) + x^2 + x = x+1$

reduce

$1, x, x^2, \underset{x+1}{x^3}, \underset{\substack{x^3 \cdot x \\ x^2+x}}{x^4}, \underset{\substack{x^4 \cdot x \\ x^3+x^2 = x^2+x+1}}{x^5}, \underset{x^2+1}{x^6}, \underset{x(x^2+1) = x^3+x = 1}{x^7}$

$R^* = C_7$ cyclic group of order 7, R is a field

Prop F - field, $a \in F$. A polynomial $f(x) \in F[x]$ can be written $f(x) = (x-a)g(x) + f(a)$. Then $f(a) = 0 \iff (x-a) \mid f$.

$\deg(x-a) = 1 \Rightarrow$ deg of remainder is 0 or remainder $= 0$ ($\deg -\infty$).

$f = (x-a)g + c$

Proof: via long division by $x-a$.

$ev_a : F[x] \longrightarrow F$

substitution $x \to a$

homomorphism

$f(a) = ev_a(f) = ev_a((x-a)g(x) + c)$

$= (a-a)g(a) + c = 0 + c \Rightarrow c = f(a)$

For $f(x)$, a root $a \in F$ of f is a field element such that $f(a) = 0$.

a is a root of $f \underset{\text{def}}{\iff} f(a) = 0 \iff f(x) = (x-a)g(x)$

$x - a \mid f(x)$

Remark: We'll often encounter a case when $F \subset E$ is a subfield of a larger field E. Examples $\mathbb{Q} \subset \mathbb{Q}[\sqrt{n}] \subset \mathbb{R} \subset \mathbb{C}$.

A polynomial $f(x) \in F[x]$ is also a polynomial in $E[x]$

$F[x] \subset E[x]$

subring.

$f(x)$ may have roots a in F

$f(x)$ may have additional roots in E.

Examples 1) $f(x) = x^2 + 1$ no roots in $\mathbb{R}$, roots $\pm i$ in $\mathbb{C}$

2) $f(x) = (x+1)(x^2-2)$ root -1 in $\mathbb{Q}$, additional roots $\pm\sqrt{2}$ in $\mathbb{Q}[\sqrt{2}]$

$\uparrow$

field.

<u>Prop</u> Let $f \in F[x]$, $f \neq 0$, $\deg f = d$. Then there are at most d roots of f in any field E containing F.
In other words, suppose that F is a subfield of a field E.
Then $\#\{a \in E : f(a) = 0\} \leq d$

$\boxed{\text{A polynomial of degree } d \text{ with coefficients in a field } F \text{ can have at most } d \text{ roots in } F}$

(even in any larger field that contains F).

<u>Proof</u> Can assume $E = F$ (since $f \in F[x] \Rightarrow f \in E[x]$).
Proof is by induction on degree. $\deg f = 0$ obvious. Assume proved for degree $d-1$. If $\deg f = d$, no root in $F \Rightarrow$ done, $d \geq 0$.
Otherwise take a root a_1. $\Rightarrow f = (x - a_1)g$, $\deg g = d-1$.
Let a_2 be a root of f, $a_2 \neq a_1$. $\Rightarrow$

$$0 = f(a_2) = (a_2 - a_1)g(a_2) \qquad\qquad (a_2 - a_1)g(a_2) = 0$$

$$\Downarrow$$

$F \ni a_2 - a_1 \neq 0$ invertible $\Rightarrow g(a_2) = 0 \Rightarrow$ $\qquad g(a_2) = 0$

a_2 is a root of g. By induction, g has at most $d-1$ roots $\Rightarrow f$ has at most d roots (roots of g and a_1).

Theorem Let F be a field and G a finite subgroup of the multiplicative group $(F^*, \cdot)$. Then G is cyclic. In particular, if F is a finite field, then the group $(F^*, \cdot)$ is cyclic.

Remark: F^* is an abelian group

Examples: $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $(\mathbb{Z}/p)^*$ - find finite subgroups.

Lemma (MA I) A finite abelian group G is cyclic iff G does not contain any subgroups isomorphic to $C_p \times C_p$, for any prime p.

Proof 1: Via classification theorem for finite abelian groups.

$G = C_{n_1} \times \ldots \times C_{n_k}$ product of cyclic groups. Furthermore

$C_n = C_{p_1^{m_1}} \times \ldots \times C_{p_e^{m_e}}$ for $n = p_1^{m_1} p_2^{m_2} \ldots p_e^{m_e}$.

$200 = 2^3 5^2$

$C_{200} = C_8 \times C_{25}$

example

Decompose each C_{n_i} this way

$G = C_{q_1^{a_1}} C_{q_2^{a_2}} \ldots C_{q_r^{a_r}}$ $\quad q_1 \ldots q_r$ primes.

primes repeat $\Leftrightarrow$ G is not cyclic

Proof 2: See Friedman, Prop. 1.9 (page 4, Factorization notes).

$C_{3^2} \times C_{5^3} \times C_{7^{10}} \times C_{2^4}$ cyclic

$C_{5^2} \times C_3 \times C_{7^2} \times C_{3^2} \times C_5$ not cyclic

$$\begin{array}{c} C_3 \times C_{3^2} \\ \cup \\ C_3 \times C_3 \end{array}$$

of form $C_p \times C_p$, p-prime.

$$\begin{array}{c} C_{p^a} \times C_{p^b} \\ \cup \\ C_p \times C_p \end{array}$$

Assume $C_p \times C_p$ is a subgroup of $(F^*, \cdot)$

$H \subset F^*$, $H \simeq C_p \times C_p$.

then $h^p = 1$ for any element h of H.

(since elements of $C_p \times C_p$ have order p or 1)

$|C_p \times C_p| = p^2$.

Consider polynomial $x^p - 1 \in F[x]$ of degree p.

It has at least p^2 roots in F. $p^2 > p$ contradiction.

$x - h \mid x^p - 1$ $\forall h \in H$. too many divisors

For any field F, any finite subgroup $G \subset (F^*, \cdot)$ is cyclic.

Examples 1) $\mathbb{Q}^* \supset G$, G finite $\Rightarrow G \subset \{\pm 1\}$

2) Take all elements of finite order in F^*. That's a subgroup $(F^*)^{fin}$ of F^*. It cannot contain any subgroups isomorphic to $C_p \times C_p$.

3) $\mathbb{R}^* \supset G$, G finite $\Rightarrow G \subset \{\pm 1\}$

4) $\mathbb{C}^* \ni z$, $z^\ell = 1$ some ℓ $\Rightarrow z = e^{\frac{2\pi i m}{n}}$ root of unity

$\{1, e^{2\pi i/n}, e^{4\pi i/n}, \dots\}$ subgroup $\simeq C_n$

Any finite subgroup of $\mathbb{C}^*$ is of this form.

Exercise $(\mathbb{C}^*)^{fin} \simeq \mathbb{Q}/\mathbb{Z}$. rat. #'s modulo integers.

<u>Corollary</u> a) If F is a finite field, $(F^*, \cdot)$ is cyclic

b) $(\mathbb{Z}/p)^*$ is cyclic of order $p-1$.

$(\mathbb{Z}/n, +)$ is cyclic of order n

$(\mathbb{Z}/n)^*$ is not cyclic, in general, if n is not prime

(take $n = 8$).

When n is composite, $\mathbb{Z}/n$ is <u>not</u> a field (not even an integral domain).

$I, J \subset R$ ideals $\Rightarrow$ $I+J$, $I \cap J$ are ideals

zero ideal (smallest)

$$\{0\} \subset I \cap J \subset I, J \subset I+J \subset R$$

smaller than I, J — bigger than I, J

Ideals are easy to manipulate in $\mathbb{Z}$, $F[x]$, since these are PIDs (any ideal is principal).

In an integral domain, principal ideals $(a) = (b)$, $a, b \in R$ iff a, b differ by a multiplication by an invertible element of R (exercise)

$a = rb$, $b = r^{-1}a$.

Example In $\mathbb{Z}$, ideals $(n) = (m)$ iff $m = \pm n$

$\{\pm 1\}$ are the only invertible elements. Ideals

(0), (1), (2), (3), (4), ...

$(1) = \mathbb{Z}$ entire ring, not proper

$(3) = (-3)$, $(4) = (-4)$ ..

bigger ideal, "smaller" number.

$(2) \supset (4)$

$(2) \supset (6)$...

$(n) \supset (nm)$.

Exercise

$(n) + (m) = (\gcd(n, m))$ — $(4) + (6) = (2)$

$(n) \cap (m) = \operatorname{lcm}(n, m)$. — $(4) \cap (6) = (12)$

Ideals in $F[x]$

$(f)=(g)$ iff $f=rg$, $r\in(F[x])^{\times}=F^{\times}$

f,g polynomials. $\Rightarrow$ scale f to be a monic polynomial

$$\{0\},\quad (1),\quad (x-a),\quad (x^2-ax-b),\ \ldots \qquad a\in F \qquad a,b\in F$$

$\{0\}$: zero ideal

$(1) = F[x]$: not proper, entire ring

deg 0 monic poly, deg 1, deg 2 ...

$I=(f(x))$

Each such ideal gives rise to quotient ring $F[x]/I$

$F=\mathbb{Q}$ $\qquad (5x+2)=(x+\frac{2}{5})\subset\mathbb{Q}[x]$

$(6)=(1)=\mathbb{Q}[x]$

$(x)+(x^3)$ sum of ideals $\qquad (x^3)\subset(x)\Rightarrow(x)+(x^3)=(x)$

$(x)+(0)=(x)$ $\qquad (0)\subset(x)$

$(f(x))+(g(x))=(\gcd(f,g))$ $\qquad (x)+(x^2+1)=(\gcd(x,x^2+1))=(1)$

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

$\underbrace{(2x)}_{\text{monic}}\cap(x^3)=(x)\cap(x^3)=(x^3)$, since $(x)\supset(x^3)$

$(f)\cap(g)=(\mathrm{lcm}(f,g))$