Groups & Rings: Lecture #18

Irreducible polynomials (§17.2–17.3)

- Units in polynomial rings
- Division algorithm
- Euclid's algorithm, gcd
- Irreducible polynomials
- Irreducibility in $\mathbb{Q}[x]$
  - Gauss' lemma
  - Eisenstein's criterion

Units in pol. rings

Today: Mostly pol. ring $F[x]$ where F field.

Recall: $F[x]$ integral domain, $\deg(0) = -\infty$

Rmk: Units $(F[x])^\times = F^\times$ non-zero constant polynomials
$= \{ p(x) \in F[x] : \deg p = 0 \}$

Rmk: Because F int. domain: $\deg pq = \deg p + \deg q$

Exc 17.4 #7: Find a unit $p(x) \in \underbrace{\mathbb{Z}_4}[x]$, $\deg p > 0$.

NB! not an integral domain

Let's try with $p(x) = ax + b$, $q(x) = a'x + b'$, $a, b \in \mathbb{Z}_4$

Want $p(x)q(x) = 1$. Need $aa' = 0$ and $bb' = 1$.

Pick $a = 2$, $a' = 2$. Pick $b = 1$, $b' = 1$.

Check if it works:

$$(2x+1)(2x+1) = \underbrace{(2x)^2}_{4x^2 = 0} + \underbrace{2 \cdot 2x}_{=0} \cdot 1 + 1^2 = 1$$

Conclusion $2x + 1$ is a unit.

Rmk: We saw that $y = 2x+1$ was a solution to $y^2 = 1$

Equation $y^2 = 1$ may have more than 2 sol's.

Reason: $\mathbb{Z}_4$ not an integral domain. (see factor thm further down)

For a similar problem, see: Exam 2019-08-12 #6a

Division algorithm

$\exists^! =$ exist unique

$$\left(\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)} \right)$$

Thm (Division algo. 17.6) $f(x), g(x) \in F[x]$, $g \neq 0$.
Then $\exists^! q(x), r(x) \in F[x]$, $\deg r(x) < \deg g(x)$ s.th.

$$f(x) = g(x) \cdot \underbrace{q(x)}_{\text{quotient}} + \underbrace{r(x)}_{\text{remainder}} \qquad (r = 0 \text{ possible})$$

sketch of pf: "Long division": start w/ leading coeff of $g(x)$.
Coeff's of $q(x)$ exists (uses F field) and are unique (uses F int. domain).

Cor (Factor theorem, 17.8) $f(x) \in F[x]$, $\alpha \in F$. Then

$$f(\alpha) = 0 \iff f(x) = (x - \alpha) q(x)$$

pf: By div algo: $f(x) = (x - \alpha) q(x) + r(x)$
where $\deg r(x) < 1$, so $r(x) = \beta \in F$.

$$f(\alpha) = 0 \iff r(\alpha) = \beta = 0 \qquad \square$$

Cor: $f(x) \in F[x]$ of degree $n \Rightarrow f$ has at most n roots.
pf: $\alpha_1, \dots, \alpha_m \in F$ roots $\overset{\text{factor thm}}{\Rightarrow} f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) q(x)$

$$\overset{F \text{ ID}}{\Rightarrow} \deg f(x) = m + \deg q(x) \qquad \square$$

y^2-1 has solutions $y=\pm 1$ in R for any ring R. By factor thm, these are the only solutions if R is a field but not in general.

Ex (continued)

not a field

Let $R=\mathbb{Z}_4[x]$, $f(y)\in R[y]$, $f(y)=y^2-1$

Then $f(2x+1)=0$, $f(1)=0$, $f(-1)=0$

So $f(y)$ has more than 2 roots! In fact, if $y=2p(x)+1$ for any $p(x)\in R$, then:

$$f(y) = (2p(x)+1)^2-1 = 0$$

so $f(y)$ has infinitely many roots in R.

not a field

Easier ex: $R=\mathbb{Z}_6$, $R[y]$, $f(y)=2y$

Roots of $f(y)$: $y=0$, $y=3$ 2 roots (too many!)

Euclid's algorithm

Def: Let R be a ring. Let $a, b \in R$

- a is a divisor of b, written $a \mid b$ if $b = ac$ for some $c \in R$.
- d is a greatest common divisor of a, b if
  - (a) $d \mid a$ and $d \mid b$ (d is a common divisor)
  - (b) if $e \mid a$ and $e \mid b$ for some $e \in R$ then $e \mid d$. (d is "greatest")

Ex: $R = \mathbb{Z}$. $a \mid b \Rightarrow |a| \leq |b|$

$\gcd(a,b) \overset{\text{exercise}}{\Longleftrightarrow}$ a common divisor d s.th $|d|$ is maximal

Return to $R = F[x]$.

Rmk: $f(x) \mid g(x) \Rightarrow \deg f(x) \leq \deg g(x)$

greatest c.d. $\Longleftrightarrow$ c.d. of maximal degree

non obvious: exercise

(Book requires gcd in $F[x]$ to be monic.)

Euclidean algorithm: Start with $f(x), g(x) \in F[x]$

Goal: Find $d(x)$ gcd of $f(x)$ and $g(x)$.

Can assume: $\deg f(x) \geq \deg g(x)$.

Use division algorithm repeatedly:

First time: divide f by g:

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

Rmks: • If $d \mid f$ and $d \mid g \Rightarrow d \mid r$.

• If $d \mid r$ and $d \mid g \Rightarrow d \mid f$

• Thus: $d \mid f \;\&\; d \mid g \overset{(*)}{\iff} d \mid g \;\&\; d \mid r$

Claim: d gcd of f & $g \iff d$ gcd of g & r

pf: Use $(*)$ and definition of gcd.

Now, replace f & g w/ g&r and repeat.

	Start with	(f, g)	$\deg f \geq \deg g$	degree drops in every step.
(div f/g)	$\rightsquigarrow$	(g, r)	$\deg g > \deg r$	
(div g/r)	$\rightsquigarrow$	(r, s)	$\deg r > \deg s$	
⋮	⋮			
	$\rightsquigarrow$	$(v, \underline{0})$	$\deg 0 = -\infty$	$\Rightarrow$ $\underline{v \text{ is a gcd}}$

To be more precise:

$$d \text{ gcd of } f \,\&\, g \overset{\text{Claim above}}{\iff} \cdots \overset{\text{Claim above}}{\iff} d \text{ gcd of } v \,\&\, 0$$

$$\underset{\text{exercise}}{\iff} d = v \cdot \underset{\text{elt of } F^{\times}}{(\text{unit})}$$

Pseudo-code

```
FUNCTION gcd(f, g)
   IF deg f ≥ deg g THEN (a,b)=(f,g) ELSE (a,b)=(g,f)
   WHILE b≠0
       r = REMAINDER OF a/b      (that is, a=bq+r, deg r < deg b)
      (a, b) = (b, r)
   REPEAT
   RETURN a
```

Prop 17.10: $f, g \in F[x]$. A gcd d of f, g exists and is unique up to mult. with a unit (element of $F^\times$).
(unique if we require the gcd to be monic)

Moreover: $d(x) \in \{a(x)f(x) + b(x)g(x) : a(x), b(x) \in F[x]\} = \underbrace{(f, g)}_{\text{smallest ideal cont. } f \,\&\, g}$

pf: Existence and uniqueness from Euclid's algorithm.
For final claim: Note that $(f,g) \subseteq F[x]$ ideal so:

$$r(x) = f(x) - g(x)q(x) \in (f,g)$$
$$s(x) = \underbrace{g(x)}_{\in (f,g)} - \underbrace{r(x)}_{\in(f,g)} q_2(x) \in (f,g) \quad \text{etc} \ldots \quad \overset{d}{\overset{\shortparallel}{v}} \in (f,g) \quad \square$$

Ex: $g(x) = x^3 + x^2 + x + 1$ in $\mathbb{Q}[x]$
$f(x) = x^4 + 2x^2 + 1$ $\qquad gq = x^4 - 1$

$$(x^4 + 2x^2 + 1, \quad x^3 + x^2 + x + 1) \qquad q = x - 1, \ r = 2x^2 + 2$$
$$\rightsquigarrow (x^3 + x^2 + x + 1, \quad 2x^2 + 2) \qquad q_2 = \tfrac{1}{2}x + \tfrac{1}{2}, \ s = 0$$
$$\rightsquigarrow (2x^2 + 2, \quad 0)$$

$\gcd(f, g) = 2x^2 + 2$ unique up to mult w/ $\mathbb{Q}^\times$

The unique monic gcd is $x^2 + 1$.

Aside: Example considered in $\mathbb{Z}[x]$:
$f(x) = (x^2+1)^2$
$g(x) = (x^2+1)(x+1)$

(so works over $\mathbb{Z}[x]$ as well)

Irreducible polynomials

Def: R be an integral domain. $r \in R$ is irreducible if

(a) r is non-zero & not a unit, and

(b) $r \neq ab$ where a, b not units.

Back to $R = F[x]$. Equivalent definition:

$$f(x) \in F[x] \text{ irreducible } \iff \begin{cases} \text{(a) } \deg f \geq 1, \text{ and} \\ \text{(b) } f \neq gh, \ \boxed{\begin{matrix}\deg g \geq 1 \\ \deg h \geq 1\end{matrix}} \end{cases}$$

(or equiv: $\deg g < \deg f$)

Ex: • $x^2+1 \in \mathbb{R}[x]$ irreducible but

• $x^2+1 = (x+i)(x-i) \in \mathbb{C}[x]$ reducible (= not irreducible)

• $x^2+1 \in \mathbb{Q}[x]$ irreducible (follows from irr in $\mathbb{R}[x]$)

• $x^2+1 \in \mathbb{Z}[x]$ irreducible. To see this, suppose it is reducible. Then product of two monic polynomials of deg 1 but $x^2+1 = (x+a)(x+b)$ impossible. (no roots in $\mathbb{Z}$)

• $x^2+1 \in \mathbb{Z}_2[x]$ reducible: $x^2+1 = (x+1)^2$

General approach: If $f(x) \in F[x]$ has degree ≤ 3 then irreducible $\iff$ no roots. (particularly useful if F finite b/c only finitely many roots to check)

If $\deg f \geq 4$, this fails:

Ex: $(x^2+1)^2 \in \mathbb{R}[x]$ reducible but has no roots.

Irreducibility in $\mathbb{Q}[x]$

Simple observation: If $f(x) \in \mathbb{Z}[x]$ monic, then
f irr $\iff \nexists f = gh$ with $g(x), h(x)$ monic of smaller degree

Simple corollary: If $f(x) \in \mathbb{Z}[x]$ monic and reducible
then $f(x) \in \mathbb{Q}[x]$ also reducible.

Monic important: Note that $4x \in \mathbb{Z}[x]$ not irr: $4x = 2 \cdot 2x$
but $4x \in \mathbb{Q}[x]$ irr.

Thm 17.14 (Gauss' lemma) If $f(x) \in \mathbb{Z}[x]$ monic
and $f = g \cdot h$ in $\mathbb{Q}[x]$, then $f = G \cdot H$ in $\mathbb{Z}[x]$
where $\deg G = \deg g$, $\deg H = \deg h$.
In particular, if $f(x)$ reducible in $\mathbb{Q}[x]$
$\Rightarrow f(x)$ reducible in $\mathbb{Z}[x]$

Conclusion: If $f(x) \in \mathbb{Z}[x]$ monic then:
$f(x)$ irreducible in $\mathbb{Z}[x] \iff f(x)$ irr in $\mathbb{Q}[x]$.

(General version: replace monic by "primitive")

Ex: Prove that $f(x) = x^4 + x^3 + 1 \in \mathbb{Q}[x]$ is irreducible.

Step 1: By Gauss lemma: enough to prove that irr in $\mathbb{Z}[x]$.

Step 2: Enough to prove that it is irr in $\mathbb{Z}_p[x]$ for some prime p

Contrapositive: f red in $\mathbb{Z}[x] \Rightarrow$ red in $\mathbb{Z}_p[x]$

$f(x) = p(x)q(x)$ in $\mathbb{Z}[x]$

$\Rightarrow f(x) = p(x)q(x)$ in $\mathbb{Z}_p[x]$ so f red.

Try $p=2$.

Step 3: Linear factor? ($\Leftrightarrow$ roots?)

$f(0) \equiv 1 \pmod 2$

$f(1) \equiv 1 \pmod 2$

$\Rightarrow$ no roots $\Rightarrow$ no linear factor

Step 4: Quadratic factor?

Suppose $\exists a, b, c, d \in \mathbb{Z}_2$ s.th:

$$x^4 + x^3 + 1 \overset{(*)}{=} (x^2 + ax + b)(x^2 + cx + d) \quad \text{in } \mathbb{Z}_2[x]$$

Equal constant terms $\Rightarrow bd = 1 \Rightarrow b = d = 1$

Equal x^3-coefficients $\Rightarrow a + c = 1 \Rightarrow a = 1, c = 0$

Gives:

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

So $(*)$ doesn't hold

Eisenstein's criterion

Thm 17.17: $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$

Let p prime number. If $p \mid a_0, \ldots, a_{n-1}$ except $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ irreducible. (Eisenstein pol)

Ex: $f(x) = 3x^3 + 12x + 2$ is irreducible in $\mathbb{Z}[x]$

(Eisenstein polynomial for $p=2$)

Useful fact: The cyclotomic polynomial (p a prime)

$$\Phi_p(x) = \frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \cdots + 1$$

is irreducible in $\mathbb{Q}[x]$. (not an Eisenstein polynomial)

(Roots of Φ_p in $\mathbb{C}$ are the primitive p^{th} roots of unity $e^{\frac{2\pi i}{p}\cdot k}$, $k=1,\ldots,p-1$)

Trick: Coord change $\mathbb{Q}[x] \overset{\phi}{\cong} \mathbb{Q}[y]$ ring isomorphism.

$y = x-1$

$$f(x) \longmapsto f(y+1)$$

$$g(x-1) \longleftarrow g(y)$$

(binom. thm)

$$\phi(\Phi_p(x)) = \Phi_p(y+1) = \frac{(y+1)^p - 1}{(y+1)-1} = y^{p-1} + \binom{p}{1} y^{p-2} + \cdots + \binom{p}{p-1}$$

$$= y^{p-1} + \underbrace{p}\, y^{p-2} + \cdots + \underbrace{\binom{p}{p-2}} y + \underbrace{p}$$

Thus: $\Phi_p(y+1)$ irr

$\overset{(exc)}{\Longrightarrow}$ $\Phi_p(x)$ irr

all coeff div. by p
constant p not div by p^2 $\Big\}$ $\Rightarrow$ Eisenstein