lect 11, following Rotman, Irr. poly. p 38+

$\mathbb{Q} \to \mathbb{Z} \to \mathbb{Z}/p$ field

$f \in \mathbb{Q}[x]$, $f \neq 0$ $\quad f = a_n x^n + \dots + a_0 \quad a_i \in \mathbb{Q}$

Clear denom (raf #) (pol. over $\mathbb{Z}$)

$f = \frac{2}{5}x^2 - \frac{4}{3}x + \frac{6}{15} \qquad \operatorname{lcm}(5,3,15) = 15$

$f = \frac{1}{15}(\underline{6}x^2 \underline{-20}x + \underline{12}) \quad \gcd(6,-20,12) = 2$

$f = \frac{2}{15}(\underline{3}x^2 - 10x + \underline{6}) = c(f)\, f^*(x)$

$c(f)$: content of $f$, $\in \mathbb{Q}$ positive

$f^*(x) \in \mathbb{Z}[x]$, gcd(coefficients) = 1

<u>Def</u> $f \in \mathbb{Z}[x]$ is called <u>primitive</u> if gcd of coefficients is 1.

<u>Prop</u> $\forall f \in \mathbb{Q}[x]$, $f \neq 0$ has a unique factorization

$$f = c(f)\, f^*(x)$$

$c(f) \in \mathbb{Q}_{>0}$, $f^*(x) \in \mathbb{Z}[x]$ primitive

$f = c f^*(x)$, $f = e\, h(x) \qquad c f^* = e h$

$\frac{e}{c} = \frac{u}{v}$ $\quad u, v$ - rel. prim. $u, v > 0$

$cf^* = eh \Rightarrow vf^*(x) = uh(x)$  if $v$ not $1 \Rightarrow$

$u \Rightarrow u = 1.$  $v \mid$ each coeff of $h(x)$

$v = 1$  $\square$

**Cor** if $f(x) \in \mathbb{Z}[x]$ then $c(f) \in \mathbb{Z}$

$$f(x) = \underset{\substack{\shortparallel \\ \gcd(\text{coeff } f)}}{c(f)} \cdot f^*(x) \qquad f^*(x) \in \mathbb{Z}[x].$$

**Lemma** the product of prim. polyn. is primitive

$f, g$ - prim $\Rightarrow$ $fg$ prim.  $\mathbb{Z} \to \mathbb{Z}/p.$

$\mathbb{Z}[x] \xrightarrow{\gamma} \mathbb{Z}/p[x]$  $\gamma$ reduces coeff mod $p$.

hom of rings.

$\gamma(a_2 x^2 + a_1 x + a_0) = \underline{a}_2 x^2 + \underline{a}_1 x + \underline{a}_0$

$R \xrightarrow{\gamma} S$

$f, g \xmapsto{\gamma} \gamma(f), \gamma(g)$  $R[x] \to S[x]$

$\cap$

$\mathbb{Z}/p[x].$

$\cap$ integral domain.

If $fg$ not prim.

then some $p$ divides all coeff of $fg$.

$$\mathbb{Z}[x] \xrightarrow{\gamma} \mathbb{Z}/p[x]$$
$$fg \longmapsto 0 \quad \text{(all coeff are } 0 \text{ mod } p\text{)}.$$

$\gamma(f), \gamma(g) \neq 0$ since $f, g$ are <u>prim</u>

$\gamma(f), \gamma(g) \neq 0$ in $\mathbb{Z}/p[x]$.

$$\underbrace{0}_{\gamma(fg)} \quad \gamma(f)\gamma(g)$$

$\gamma(fg) = \gamma(f)\gamma(g)$ since $\gamma$ is a homomorphism contradiction.

**Cor** if $f(x) \in \mathbb{Q}[x]$, $f = g(x)h(x)$ in $\mathbb{Q}[x]$

then $\quad c(f) = c(g)\,c(h)$

$$f^*(x) = g^*(x)\,h^*(x)$$

**Pf** $\quad f(x) = g(x)\,h(x) = c(g)\,g^*(x)\,c(h)\,h^*(x) =$

$$= \underbrace{\big(c(g)\,c(h)\big)}_{\mathbb{Q}_{>0}}\,\underbrace{g^*(x)\,h^*(x)}_{\text{primitive}}$$

Thm (Gauss). if $p(x) \in \underline{\mathbb{Z}[x]}$ is not a product of 2 polynomials in $\mathbb{Z}[x]$ each <u>of degree $< \deg p$</u>, then $p(x)$ is irred. in $\mathbb{Q}[x]$.

**Pf** $\quad$ if $p(x) = g(x)\,h(x)$ in $\underline{\mathbb{Q}[x]}$.

$$p(x) = \Big(\underbrace{c(g)\,c(h)}_{\text{gcd of coeff of } p}\;\underbrace{g^*(x)}_{\text{primitive}}\Big)\,\underline{h^*(x)}.$$

1) $f(x) = x^3 + 5x^2 + 3x + 1$ $\qquad \mathbb{Z} \longrightarrow \underline{\mathbb{Z}/p}$

irr$/\mathbb{Q}$ iff irr$/\mathbb{Z}$ $\qquad$ if $\exists\, p$. s.t. $\bar{f}(x)$ is irr $/\mathbb{Z}/p$

$p=2$ $\quad \bar{f}(x) = x^3 + x^2 + x + 1 =$

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

not irreducible. ?

$p=3$ $\quad \bar{f}(x) = x^3 + 2x^2 + 1$ $\qquad x=0 \quad f(0)=1$

$f(1) = 1 \quad f(2) = 17 = 2 \pmod 3$

no roots in $\mathbb{Z}/3$

$\deg \bar{f}(x) = 3 \Rightarrow$ does not factor $/\mathbb{Z}/3$.

$\Rightarrow$ $f(x)$ irr $/\mathbb{Z}$, $/\mathbb{Q}$.

2) $f(x) = 6x^3 + x + 1$ $\qquad f(x) \in \mathbb{Z}[x]$, not monic

$2, 3 \mid 6$ $\qquad$ reduce mod 3 $\quad \deg \bar{f}(x) < \deg f(x)$.

$p=5$ $\quad \bar{f}(x) = x^3 + x + 1$

$x \in \{0, 1, 2, 3, 4\}$ $\quad \bar{f}(x) \neq 0$ for $x \in \mathbb{Z}/5$ no roots

$\Rightarrow \bar{f}(x)$ irr $/\mathbb{F}_5$ $\quad f(x)$ irr $/\mathbb{Z}$, $\mathbb{Q}$.

**Thm** (Eisenstein criterion)

Let $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$.

If $\exists$ prime $p$, $p \mid a_i \ \forall i < n$, $p \nmid a_n$, $p^2 \nmid a_0$

$\Rightarrow f(x)$ is irreducible $/\mathbb{Q}$.

$p \nmid a_n$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $p^2 \nmid a_0$

$$f = \underline{a_n} x^n + \underbrace{a_{n-1} x^{n-1} + \dots + a_1 x + a_0}_{p \mid a_i \quad \forall i < n}$$

$p = 5 \qquad 3x^4 + 5x^3 - 10x^2 - 15$

$5 \nmid 3 \qquad 5 \mid (5, -10, 0, -15) \qquad 5^2 \nmid -15$

Pf For such $f, p$ $\quad \mathbb{Z}[x] \xrightarrow{\gamma} \mathbb{Z}/p[x]$

if $f$ reducible $/\mathbb{Q}$ $\Rightarrow$ factors over $\mathbb{Z}$.

$f(x) = \underline{g(x)\, h(x)} \qquad \deg g, h < n$

$f(x) = a_n x^n + \dots + a_0 \qquad p \nmid a_n \quad p \mid a_{n-1} \dots a_0$

$p^2 \nmid a_0$

$$\gamma(f) = \underline{a_n}\, x^n + \underset{\overset{\shortparallel}{0}}{\underline{a_{n-1}}}\, x^{n-1} + \dots + \underset{\overset{\shortparallel}{0}}{\underline{a_1}}\, x + \underset{\overset{\shortparallel}{0}}{\underline{a_0}} =$$

$$= \underline{a_n}\, x^n$$

$f = gh \qquad \gamma(f) = \gamma(gh) = \gamma(g)\gamma(h)$

$\underline{a_n}\, x^n = \gamma(g)\gamma(h)$ in $\mathbb{Z}/p[x]$.

$\underline{a_n} \in \mathbb{Z}/p^{\times} \qquad \underset{x^k}{\uparrow} \quad \underset{x^{n-k}}{\uparrow} \quad \underset{\underline{a_n}}{\nwarrow}$

$\gamma(g) = \underline{b}_k x^k \qquad \gamma(h) = \underline{c}_{n-k} x^{n-k}$

$g = b_k x^k + \underbrace{b_{k-1} x^{k-1} + b_0}_{\equiv 0 \bmod p}$ $\quad h = c_{n-k} x^{n-k} + \dots + c_0$

$\gamma(g) = \underline{b}_k x^k$

$g = b_k x^k + b_{k-1} x^{k-1} + \dots + b_0$

$p \nmid b_k \quad p \mid b_{k-1}, \dots \quad p \mid b_0$

$h = c_{n-k} x^{n-k} + c_{n-k-1} x^{n-k-1} + \dots + c_0$

$\underbrace{\phantom{c_{n-k}}}_{\bmod p} \quad \underbrace{\phantom{c}}_{0} \quad \underbrace{\phantom{c}}_{0}$

$\underline{c}_{n-k} x^{n-k} \quad p \mid c_i \quad i < n-k \quad p \mid c_0$

$f = gh \qquad f(0) = a_0 \qquad a_0 = b_0 c_0$

$g(0) = b_0, \; h(0) = c_0 \qquad p \mid b_0, \; p \mid c_0 \Rightarrow$

contradiction $\quad p^2 \mid a_0$

$x^n - 2 \quad n \geq 2 \qquad 4 \nmid 2.$

$p = 2 \qquad x^n + \underbrace{0 x^{n-1} + \dots + 0x - \overline{2}}_{2 \mid a_i \;\; i < n}$

$2 \nmid 1$

irr. $/\mathbb{Q}$.

$x^n - p$ irr. $\qquad x^n - a \qquad$ some $p \quad p \mid a$

$p^2 \nmid a.$

$x^n - 10$.

get irr. $/\mathbb{Q}$ of any degree

Cyclotomic polyn of prime degree

$$\Phi_p(x) = \underbrace{\frac{x^p-1}{x-1}} = x^{p-1} + x^{p-2} + \dots + 1. \quad p \text{ terms.}$$

$p=5 \quad \Phi_5(x) = x^4+x^3+x^2+x+1 \quad 5$ terms

<u>Prop</u> $\Phi_p(x)$ irr in $\mathbb{Q}[x]$ $\forall$ prime $p$.

<u>Pf</u> $f(x)$ irr $\Leftrightarrow$ $f(x+c)$ irr some $c \in \mathbb{Q}$.

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

$$= x^{p-1} + \underset{\overset{\shortparallel}{p}}{\binom{p}{1}} x^{p-2} + \binom{p}{2} x^{p-3} + \dots + \underset{\overset{\shortparallel}{p}}{\binom{p}{p-1}}$$

$p \mid \binom{p}{i} \quad i = 1, 2, \dots, p-1 \qquad 0 \bmod p \qquad p^2 \nmid p$

$\Rightarrow$ irr. by E. criterion.

$\cancel{\Phi_n}(x)$ $n$ composite reducible $\cancel{\Phi_4}(x) = x^3+x^2+x+1$.

Isomorphisms Automorphisms.

$V \overset{f}{\rightleftarrows} W \qquad V \xrightarrow{f} V$

$\exists g$ isom = structure-preserving bijection aut = isom with itself

The inverse map $g$

such that $gf$ = identity map of $V$

$fg$ = identity map of $W$.

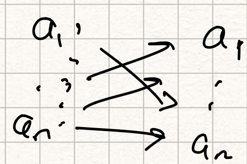
sets – bijections.

<u>Observation</u>

automorphisms of an object constitute a group.

Aut (set $S$ with $n$ elements) = $S_n$

need to order elements.



aut. of fields

$G$ $\quad$ Aut$(G)$ <u>group</u>

inner automorphisms?

$h$ $\quad$ $g \mapsto hgh^{-1}$ $\quad$ conjugation by $h$ automorphism