

Def'n

Let  $S = \text{set}$ , a **binary operation** on  $S$  is  
a function  $f: S \times S \rightarrow S$   
 $\text{domain} \quad \text{co-domain}$

$$S \times S = \{(a, b) \mid a \in S, b \in S\}$$

Convention

we will often write  $f(a, b)$  as " $a \cdot b$ " or " $ab$ "

allows us to be less  
careful when writing down

long "products"

Def'n

A binary operation  $f: S \times S \rightarrow S$  is **associative**  
if  $\forall a, b, c \in S, f(f(a, b), c) = f(a, f(b, c))$   
in new notation:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

exists  $S = M_n(\mathbb{R}) = n \times n$  matrices w/ real coefficients

$f(A, B) = A \cdot B \leftarrow \text{matrix multiplication, which is associative}$

Key fact composition of functions transformations is associative

Def'n A binary operation is **commutative**

if  $\forall a, b \in S, a \cdot b = b \cdot a$

exists  $(\mathbb{R}, +)$  - real number addition

Def'n Given  $S$  equipped w/ a binary operation,  $\cdot$ , we say

$(S, \cdot)$  has an **identity element**

if  $\exists e \in S$  s.t.  $\forall a \in S, a \cdot e = e \cdot a \rightsquigarrow$  doesn't change identity

Def'n An element  $a$  of  $(S, \cdot)$  is called **invertible** (w/e = identity)

if  $\exists b \in S$  s.t.  $ab = e = ba$

Def'n

A **group** is a set  $(G, \cdot)$  w/ a binary operation s.t.

i) it's associative

! closure under operation

ii)  $\exists$  an identity element  $e \in G$

iii) every element in  $G$  is invertible

If  $\cdot$  is commutative,  $G$  is called **an abelian group**

exists  $G = \{ \text{bijections } T: \mathbb{R}^2 \rightarrow \mathbb{R}^2 \text{ so that } T(\text{standard unit square } = S_1) = S_1 \}$

$\sim$  binary operation: composition

another name:  $D_8$

Thm:  $D_8$  contains exactly 8 elements

Proof?

claim If  $\varphi \in G$ , then  $\varphi$  can be expressed as a finite composition

then  $\varphi$  can be expressed as a finite composition  $\varphi_1 \circ \varphi_2 \circ \varphi_3 \dots$

where for each  $i$ ,  $\varphi_i = \begin{cases} \text{rotation by } 90^\circ \text{ counter-clockwise} \\ \text{reflection over a horizontal line of symmetry} \end{cases}$

$r^4 = h^2$  rotation for 4 times = reflection twice

Def'n

A **subgroup**  $H$  of a group  $(G, \cdot)$  is a subset of  $G$  which is also a **group** with respect to  $\cdot$ .

claim Given a group  $(G, \cdot)$  if  $H \subseteq G$ ,  $H$  is a subgroup of  $G$

$\Leftrightarrow$  i)  $\forall h_1, h_2 \in H, h_1 \cdot h_2 \in H$  closure

ii)  $\forall h \in H, h^{-1} \in H$  invertible

Def'n Given  $\{1, 2, 3, \dots, n\}$  for some  $n \in \mathbb{N}$ ,

define  $S_n = (\{\text{bijections } \tau: \{1, 2, 3, \dots, n\} \rightarrow \{1, 2, 3, \dots, n\}\}, \text{composition})$

Fact  $S_n$  is a group, called the "symmetric group on  $n$  elements".  
Terminology elements of  $S_n$  are called permutations  
exists 1 say  $n=5$ , the  $\tau: \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{matrix}$

$\tau = (\underline{1 \ 5 \ 3 \ 4})(2) \leftarrow \text{"cycle notation"}$   
 $1 \rightarrow 5, 5 \rightarrow 3, 3 \rightarrow 4, 4 \rightarrow 1 \text{ and } 2 \rightarrow \text{itself}$

caution  
inverse

cycle notation is not unique!  
 $(\underline{(1 \ 5 \ 3 \ 4)}(2))(\underline{(1 \ 4 \ 3 \ 5)}(2)) = \underbrace{(1)(2)(3)(4)(5)}_{\text{identity}}$

Let  $\tau \in S_n$ . Define  $M_\tau = n \times n$  matrix obtained from  $I_n$  after permuting rows of  $I_n$  via  $\tau$

e.g.  $\tau \in S_4, \tau = (1 \ 3 \ 4)$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

e.g.

if  $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$  compute  $M_\tau \cdot \vec{x} = \begin{pmatrix} x_4 \\ x_2 \\ x_1 \\ x_3 \end{pmatrix}$

observation

$$M_\tau \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} x_{\tau^{-1}(1)} \\ \vdots \\ x_{\tau^{-1}(n)} \end{pmatrix}$$

Thm

(i)  $\forall \tau \in S_n, \det(M_\tau) = \pm 1$

(ii) Given  $p, q \in S_n, M_{pq} = M_p \cdot M_q$

Def'n

Given  $\tau \in S_n$ , the sign of  $\tau$  is the sign of  $\det(M_\tau)$

$$d = p - a + q \cdot b$$

Def'n  
exists 1

greatest common divisor :  $\gcd(a, b)$

Euclidean algorithm:  $\gcd(314, 36)$

Def'n Given  $a, b \in \mathbb{Z}, a, b \neq 0, a \nmid b$  are relatively prime if  $\gcd(a, b) = 1$   
Favet corollary:  $\gcd(a, b) = \text{product of prime powers common to prime factorizations of } a \text{ & } b$   
a & b are relatively prime  $\Leftrightarrow \gcd(a, b) = 1 \Leftrightarrow a \nmid b$   
 $ra + sb = 1$

corollary: Suppose  $p = \text{prime} (\text{i.e. } 2, 3, 5, 7, 11, \dots)$  Then given  $a, b \in \mathbb{Z}$ , if  $a \nmid ab$ , then  $p \mid a$  or  $p \mid b$  (or both)

Thm If  $S \subseteq \mathbb{Z}$  is a subgroup of  $(\mathbb{Z}, +)$

then either  $S = \text{trivial subgroup}$

or  $\exists a \in \mathbb{Z}, a \neq 0$  so that  $S = a\mathbb{Z} = \{ \text{multiples of } a \}$

Pf Suppose  $S$  is a subgroup of  $(\mathbb{Z}, +)$

We know  $0 \in S$

if no other elements are in  $S$ ,  $S = \{0\}$ . so  $S = \text{trivial subgroup}$

Otherwise,  $\exists n \in \mathbb{Z}, n \neq 0 \nmid n \in S, n \notin S \Rightarrow -n \in S$  subgroup includes inverse

since one of  $n$  &  $-n$  has to be positive, assume  $n > 0$

Let  $a = \min \{ k \mid k > 0, k \in S \}$

choose  $k \in \mathbb{N}$ , then  $k \cdot a = a + a + \dots + a$  for  $k$  times

$k \cdot a \in S$ , since  $a \in S$  and  $S$  is closed under addition

$k \cdot a \in S \Rightarrow -k \cdot a \in S$   $S$  contains inverses

$\Rightarrow a\mathbb{Z} \subseteq S$

Now WTS  $S \subseteq a\mathbb{Z}$  to prove  $S = a\mathbb{Z}$

pick  $n \in S$  s.t.  $n = qa + r$ , for some  $q \in \mathbb{Z}$ ,  $0 \leq r < a$

$a\mathbb{Z} \subseteq S \Rightarrow qa \in S$ . Also,  $n \in S \Rightarrow n - qa \in S \Rightarrow r \in S$

$\Rightarrow r = 0$  because  $a$  is the minimum +

$\Rightarrow n = qa$

$\Rightarrow S \subseteq a\mathbb{Z}$   $\square$

intuition:

$a$  is the smallest component

Thm

Let  $G_i = (CG_i, \circ)$  a group & let  $I = \text{set } \nmid$  let  $\{H_i\}_{i \in I}$  be a family of subgroups of  $G_i$  indexed by  $I$ . Then  $\bigcap_{i \in I} H_i$  is a subgroup

" $\{h \in G_i \mid h \in H_i \forall i\}$ "

Pf

WTS:

i)  $\bigcap_{i \in I} H_i \neq \emptyset$ :  $e \in H_i \forall i \Rightarrow e \in \bigcap_{i \in I} H_i$

ii)  $\forall h_1, h_2 \in \bigcap_{i \in I} H_i \Rightarrow h_1, h_2 \in H_i \forall i : h_1 \circ h_2 \in H_i \forall i$

Def'n

Given  $a\mathbb{Z} \nsubseteq b\mathbb{Z}$ , consider  $S = a\mathbb{Z} \cap b\mathbb{Z}$ .  $S$  is a subgrp of it's in form

of  $m\mathbb{Z}$ , for some  $m$ :  $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ , so  $m \in a\mathbb{Z} \nsubseteq m \in b\mathbb{Z}$

$\Rightarrow m$  is a multiple of  $a \nmid b$ .  $m$  is called [least common multiple]

Def'n Let  $(G, \cdot)$  = any group  $\nexists x \in G$ . Then the cyclic subgroup generated by  $x$ , denoted  $\langle x \rangle$ , is all powers of  $x$ :

$$\langle x \rangle = \{ \dots, x^2, x^{-1}, e, x, x^2, x^3, \dots \}$$

Thm In  $G$ , let  $P(x) = \{ H \leq G \mid H = \text{subgroup}, x \in H \}$ . Then,  $\bigcap_{H \in P(x)} H = \langle x \rangle$   $\Rightarrow$  intersection

Proof For any  $H \in P(x)$ ,  $x \in H$  by defn of  $P(x)$

$$x \in H \Rightarrow x^2, \dots, x^{-1} \in H \text{ since } H \text{ is a subgroup}$$

$$x \in H \Rightarrow x^{-1}, x^2, x^3 = \dots \in H \text{ since } H \text{ has inverses}$$

$e \in H$  as well

$$\text{so } \{ \dots, x^2, x^{-1}, e, x, x^2, \dots \} = \langle x \rangle \subseteq H$$

$$\text{so } \langle x \rangle \subseteq \bigcap_{H \in P(x)} H$$

WTS  $\bigcap H \subseteq \langle x \rangle$

Let  $g \in \bigcap_{H \in P(x)} H$  WTS  $g \in \langle x \rangle$ , i.e.  $g = x^k$  for some  $k \in \mathbb{Z}$

Suppose  $g \neq x^k$  for any  $k \in \mathbb{Z}$

But  $\langle x \rangle \in P(x) \nsubseteq g \neq \langle x \rangle$

$\Rightarrow$  contradiction! So,  $g = x^k$  for some  $k \in \mathbb{Z} \Rightarrow g \in \langle x \rangle$   $\square$

$\langle x \rangle$  is the smallest subgp of  $G$  containing  $x$

Given  $x \in G$  = group. Let  $S_x \subseteq \mathbb{Z}$

$S_x = \{ k \in \mathbb{Z} \mid x^k = e \}$  Then  $S_x$  is a subgp of  $(\mathbb{Z}, +)$

Pf

$S_x \neq \emptyset$  since  $0 \in S_x$  ( $x^0 = e$ )

Suppose  $k_1, k_2 \in S_x$ , i.e.,  $x^{k_1} = x^{k_2} = e \Rightarrow x^{k_1} \cdot x^{k_2} = e \Rightarrow k_1 + k_2 \in S_x$   
 $x^k = e \Rightarrow x^{-k} = e^{-1} = e \Rightarrow -k \in S_x$

$S_x$  a subgp  $\Rightarrow S_x = n\mathbb{Z}$  for some  $n$

$n$  is called the order of  $x$  in  $G$ .  $x^n = e$  (since  $n \in \mathbb{Z} = S_x$ )

Note: assume  $n$  is positive. if not, replace it with  $-n$  as long as  $S_x \neq \{0\}$

In this case,  $n$  is the smallest positive # s.t.  $x^{n \text{ that number}} = e$

Note  $x^{n+1} = x$

$$x^n x = ex = x$$

$\Rightarrow$  when  $\text{order}(x) = n$

$$\langle x \rangle = \{ \dots, x^2, x^{-1}, \dots, x^2, \dots \} = \{ e, x, x^2, \dots, x^{n-1} \}$$

Def'n

Proposition

Def'n A **homomorphism** is a function  $\varphi: (G, \cdot) \rightarrow (G', \cdot)$   
 A  $g_1, g_2 \in G$ ,  
 $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$

general ex's

- i) If  $G, G'$  are any groups, let  $e'$  denote identity element of  $G'$ .  
 Then  $\varphi: G \rightarrow G'$  is a homomorphism, the "trivial homomorphism":  
 $\varphi(g_1, g_2) = e' = e'e' = \varphi(g_1)\varphi(g_2)$
- ii) If  $H = \text{subgp of } G$ , then  $i: H \xrightarrow{h \mapsto h} G$  a homomorphism, called "inclusion"

Lemma

- i) Given  $a_1, \dots, a_n \in G$ ,  $\varphi(a_1 \dots a_n) = \varphi(a_1) \dots \varphi(a_n)$
- ii) If  $e$  (resp,  $e'$ ) denotes identity in  $G$  (resp in  $G'$ ),  $\varphi(e) = e'$
- iii) If  $a \in G$ ,  $\varphi(a^{-1}) = \varphi(a)^{-1}$  (inverse map to inverses)

Def'n

Given  $\varphi: G \rightarrow G'$  a homomorphism,  
 image of  $\varphi$   $\text{Im } \varphi = \{g' \in G' \mid \exists g \in G \text{ s.t. } \varphi(g) = g'\}$   
 kernel of  $\varphi$  is  $\text{Ker } \varphi = \{g \in G \mid \varphi(g) = e'\}$

Lemma  
 Pf  $\text{Im } \varphi$  is a subgp of  $G'$  &  $\text{Ker } \varphi$  is a subgp of  $G$   
 For  $\text{Im } \varphi$

- ①  $\text{im } \varphi \neq \emptyset$  cuz  $e' \in \text{im } \varphi$  since  $\varphi(e) = e'$
- ② Suppose  $a'_1, a'_2 \in G'$  in  $\text{im } \varphi \Rightarrow \exists a_1, a_2 \in G$  s.t.  $\varphi(a_1) = a'_1, \varphi(a_2) = a'_2$   
 $a_1, a_2 \in G \nmid \varphi(a_1 \cdot a_2) = \varphi(a_1)\varphi(a_2) = a'_1 \cdot a'_2 \in \text{im } \varphi$
- ③  $a' \in \text{im } \varphi \Rightarrow \exists a \in G$  s.t.  $\varphi(a) = a'$   
 $\varphi(a^{-1}) = (\varphi(a))^{-1} = (a')^{-1} = a'^{-1} \in \text{im } \varphi$

Def'n A homomorphism  $\varphi: G \rightarrow G'$  is called an **isomorphism** if it's a bijection  
 i.e.  $\text{Im } \varphi = G'$ .  
 If  $\varphi$  is one-to-one  $\Leftrightarrow \ker \varphi = \{e\}$   
 $\hookrightarrow$  an isomorphism  $\varphi: G \rightarrow G'$  is a hom st.  $\ker \varphi = \{e\} \wedge \text{im } \varphi = G'$

ex. sl conjugation!

Let  $G$  = group,  $g \in G$ ,  $\varphi_g: G \rightarrow G$

define  $\varphi_g(a) = gag^{-1}$  = "the **conjugate** of  $a$  by  $g$ "  
 $\varphi_g$  is an isomorphism!

1)  $\varphi_g$  is a hom: Given  $a, b \in G$ ,  $\varphi_g(ab) = gag^{-1}bab^{-1} = gag^{-1}gabg^{-1}$

$$= (gag^{-1})(gbg^{-1}) = \varphi_g(a)\varphi_g(b)$$

2)  $\ker \varphi = \{e\}$ : suppose  $\varphi_g(a) = e \Rightarrow gag^{-1} = e$

$$\Rightarrow a = g^{-1}eg = g^{-1}g = e \Rightarrow \ker \varphi = \{e\}$$

3)  $\text{im } \varphi = G$

given  $a \in G$   $g^{-1}ag \in G$   $\varphi_g(g^{-1}ag) = gag^{-1} = a$

shg eH

Def'n A subgp  $H$  of a group  $G$  is called **normal** if  $\forall g \in G, gHg^{-1} = H$

Def'n Given a set  $S$ , an **equivalence reln** is a subset,  $E$ , of  $S \times S$ , satisfying:

$$\text{i)} \forall x \in S, (x, x) \in E$$

$$\text{ii)} \forall x, y \in S, \text{ if } (x, y) \in E, \text{ then } (y, x) \in E$$

$$\text{iii)} \forall x, y, z \in S, \text{ if } (x, y) \in E \text{ & } (y, z) \in E, \text{ then } (x, z) \in E$$

Whenever  $(x, y) \in E$ , we'll often write  $x \sim y$   
and we'll say  $x$  is equivalent to  $y$

Def'n Given a set  $S \nsubseteq X \in S$ , if an equivalence reln  $\sim$ , the **equivalence class** of  $X$ , denoted  $[x]$ , is  $[x] = \{y \in S \mid x \sim y\}$

Thm If  $S = \text{set}$ ,  $\sim = \text{equivalence reln}$ , then the equiv classes of  $\sim$  **disjointly partition**  $S$ , i.e. every element of  $S$  is contained in **EXACTLY** one equivalence class.

Given  $S$ ,  $\sim = \text{equiv reln on } S$ ,  $\bar{S} = \{[x] \mid x \in S\} = \boxed{\text{set of equiv classes}}$   
In this situation,  $\exists$  a map  $\pi : S \rightarrow \bar{S}$   
 $x \mapsto [x]$

Def'n  $G = \text{group}$ ,  $H = \text{subgroup of } G$ ,  $a \in G$

The **right coset** of  $H$  with respect to  $a$  is

$$Ha = \{g \in G \mid \exists h \in H \text{ s.t. } ha = hg\}$$

$$Ha = Hb \Leftrightarrow ab^{-1} \in H$$

Lemma 1)

Given  $G, H = \text{subgp}$ . the reln defined by  $a \sim b \Leftrightarrow ab^{-1} \in H$  is an equiv reln.

The equiv classes of the equiv reln are the right cosets of  $H$ .

3) The equivalence classes of  $\sim$  are the right cosets of  $H$   
i.e. given  $g \in G$   $[g] = \{a \in G \mid gna^{-1} = Ha\}$

4) Since equiv classes always disjointly partition a set, every element of  $G$  is contained in exactly one coset.

Lemma

If  $|G| < \infty$ ,  $H = \text{subgp}$ , every right coset of  $H$  has the same # of elements  $\downarrow$  i.e. given  $a, b \in G$ ,  $\text{size}(Ha) = \text{size}(Hb)$

$\forall a \in G$ ,  $\text{size}(Ha) = |H|$  since  $H$  is itself a right coset

Pf

Note

$\varphi: H \rightarrow Ha$  is a bijection  
 $h \mapsto ha$

onto:  $\forall g \in Ha$ ,  $\exists h \in H$  s.t.  $g = ha$ , so

one-to-one:  $\varphi(h_1) = \varphi(h_2)$

$$h_1a = h_2a \Rightarrow h_1 = h_2$$

cosets can be put in bijection  $\Leftrightarrow$  they have the same size

Lagrange

Theorem

Pf

If  $G$  is a finite group,  $H$  a subgp of  $G$ ,

$$\text{then } |H| \mid |G|$$

The right cosets of  $H$  share no elements in common

$\nmid$  They cover all of  $G$

AND.  $|Ha| = |H|$  by the last lemma.

$$\text{so } |G| = (\# \text{ of right cosets of } H) \cdot (|H|)$$

notation  $[G : H]$

"index of  $H$  in  $G$ "

Corollary

If  $a \in G$ , then  $\text{order}(a) \mid |G|$

Recall

given  $g \in G$ , the conjugation isomorphism for  $g$  is  $\psi_g: G \rightarrow G$   
 $a \mapsto gag^{-1}$

A subgroup  $H$  in  $G$  is called normal if

$$\forall g \in G, \quad \psi_g(H) \subset H \quad H \triangleleft G$$

Proposition:

Pf

If  $\varphi: G \rightarrow G'$  a hom, then  $\ker \varphi \trianglelefteq G$

WTS: Given  $a \in \ker \varphi \nsubseteq g \in G$ ,  $\psi_g(a) \in \ker \varphi$

$$gag^{-1}$$

$$\psi(gag^{-1}) = \psi(g)\psi(a)\psi(g^{-1}) = \psi(g)e'\psi(g^{-1}) = \psi(g)\psi(g)^{-1} = e' \in \ker \varphi$$

Then (The following are equivalent)

i)  $H \triangleleft G$

ii)  $\forall g \in G, gHg^{-1} = \{a \in G \mid \exists h \in H \text{ s.t. } a = ghg^{-1}\} = H$

iii)  $\forall g \in G, gH = Hg$

iv) Every left coset of  $H$  is a right coset of  $H$ .  
i.e. given  $aH$ ,  $\exists b \in G$ , s.t.  $aH = Hb$

Pf:

(i)  $\Rightarrow$  (ii)  $\varphi_{g(H)} \subset H$  is trivial

$$H \subset \varphi_{g(H)} \Rightarrow \varphi_{g^{-1}(H)} \subset H \nmid \varphi_{g^{-1}(H)} = g^{-1}Hg \text{ so } g^{-1}Hg \subset H$$

$$\forall h \in H, \exists h' \in H \text{ s.t. } g^{-1}hg = h' \Rightarrow h = gh'h'^{-1}$$

$$\Rightarrow H \subset gHg^{-1}$$

## Recall

Remember the rank-nullity thm from linear algebra:

$V, W = \text{finite dim vector spaces}, T: V \rightarrow W \text{ linear}$   
 $\dim(V) = \dim(\ker(T)) + \dim(\text{Range}(T))$

## Goal:

Do sth similar for groups!  
 i.e.  
 linear group

$v, w = \text{vector spaces}$   
 $T: v \rightarrow w \text{ linear}$

$\ker(T)$

$G, G' = \text{groups}$   
 $\varphi: G \rightarrow G'$  a homomorphism

$\ker(\varphi)$  i.e. normal subgp

intuition:

understand  $G'$  as  
 being a stack of  
 pancakes  
 $(\text{subgps } \subset \ker(\varphi))$   
 $G' = \text{collapse pancakes to}$   
 some point

## Thm

A subgp  $H$  of  $G$  is normal

$\Leftrightarrow \exists$  a group  $G'$  & a hom  $\varphi: G \rightarrow G'$  s.t.  $H = \ker(\varphi)$

Let's find  $G'$  s.t.  $\exists$  an onto hom  $\varphi: G \rightarrow G'$  with  $\ker(\varphi) = H$

Let  $\frac{G}{H}$  "G mod H" = {right cosets of  $H$  in  $G$ }

Fact  $\exists$  a binary operation on  $\frac{G}{H}$  turning  $\frac{G}{H}$  into a group

& this will be our  $G'$

$\nexists \varphi: G \rightarrow \frac{G}{H}$  [ $g \mapsto hg$ ]  $\rightarrow$  we defined  $\varphi$  as this  
 considering its domain & co-domain

$$\text{so. } \ker(\varphi) = \{g \in G \mid \varphi(g) = H\}$$

$$\text{so. } \ker(\varphi) = \{g \in G \mid hg = H\}$$

$$Ha = Hb \Leftrightarrow ab^{-1} \in H$$

$$\text{so. } Hg = H \Leftrightarrow g \in H$$

$$\therefore \ker(\varphi) = H$$

Given  $Ha, Hb$  in  $G/H$  define an operation •

$$Ha \cdot Hb = "HaHb" = \{g \in G \mid \exists h_1, h_2 \in H \text{ s.t. } g = h_1ah_2b\}$$

Actually, we showed that  $HaHb = HHab$  (TFAE)

$HHab \subset Hab$  since  $H$  is closed

$$\text{if } g \in HHab \Rightarrow g = h \cdot e \cdot a \cdot b \Rightarrow g \in HHab$$

$$\Rightarrow HHab = Hab$$

To Summarize:  $S = \text{Subspace of } V$

Given  $S \subseteq V$ ,  $\exists$  a decomposition of  $V$  into parallel copies of  $S$   $\nexists \exists$  a V.S.  $W$   $\nexists$  a linear map,  $T : V \rightarrow W$  so that  $T$  collapses the parallel copies to points and  $\ker(T) = S$ .

Our goal in the group theory setting:

Given  $H \triangleleft G$  ( $H$  is normal in  $G$ ),  $\exists$  a decomposition of  $G$  into right cosets of  $H$  in  $G$   $\nexists \exists$  a group  $G'$   $\nexists$  a homomorphism  $\varphi : G \rightarrow G'$  so that  $\varphi$  collapses the right coset of  $H$  to a point  $\nexists \ker(\varphi) = H$ .

$V$  is an abelian group  $\Rightarrow$  any subgp is normal!

Lemma Given  $H \triangleleft G$ , if  $Ha = Ha'$   $\nexists$   $Hb = Hb'$  then  $Hab = Hab'$   
WTS:  $ab(a'b')^{-1} \in H$

$$\begin{aligned} \text{pf: WTS } ab(a'b')^{-1} &\in H \\ \underbrace{ab(b')^{-1}(a')^{-1}}_{\substack{\in H \\ \text{H} \triangleleft G}}. \quad Hb = Hb' \Rightarrow b(b')^{-1} \in H. \\ a h(a)^{-1}. \quad ah \in aH = Ha & \\ \Rightarrow \exists h \in H \text{ s.t. } ah = h'a. & \\ \Rightarrow a h(a)^{-1} = h'(a(a')^{-1})^{-1}. \quad Ha = Ha' \Rightarrow a(a)^{-1} & \\ h'h'' \in H. \quad h'' \in H. & \\ Ha = Ha' & \end{aligned}$$

we want the cosets themselves matter instead of what produces them?

so far, we have that  $G'$  has a binary opn.

$$\begin{aligned} \varphi : G &\rightarrow G' \\ g &\mapsto hg \end{aligned}$$

(the stuff above)

$$\text{Given } a, b \in G, \varphi(ab) = Hab = HaHb = \varphi(a)\varphi(b)$$

$\Rightarrow \varphi$  "has the hom property". (we don't know  $G'$  is a group)

Note:  $\varphi$  is onto! Given  $Hg \in G/H$ ,  $\varphi(g) = Hg$  yet

↑  
(cosets)

Lemma If  $G$  is group,  $Y = \text{set with binary operation}$   
 $\nmid \varphi: G \rightarrow Y$  s.t.  $\varphi$  has the hom property ( $Y$  is not a group)  
 $\nmid$  suppose  $\varphi$  is onto. Then  $Y$  is a group.  $\nmid$   $\varphi$  is a hom  
 Pf Associativity: Given  $a, b, c \in Y$ ,  $\varphi$  onto  $\Rightarrow \exists a', b', c' \in G$  s.t.  $\varphi(a') = a$ ,  
 $\varphi(b') = b$ ,  $\varphi(c') = c$ .  
 $\varphi$  is hom  
 $\therefore (ab)c = (\varphi(a)\varphi(b))\varphi(c) = \varphi((a'b'))\varphi(c') = \varphi((a'b')c')$   
 $= \varphi(a'(b'c')) = \varphi(a')(\varphi(b')\varphi(c')) = \varphi(a')(bc) = a(bc)$   
 $\text{G is gp}$

10.5

Given a normal subgp  $H \triangleleft G$ ,

to construct a onto hom  $\varphi: G \rightarrow G'$  for some other gp  $G'$  s.t.

i)  $G' = G/H$  (only a group  $H$  is normal)

ii)  $\varphi: G \rightarrow G/H$  is the "natural" map, i.e.  $\varphi(g) = Hg$

iii) identity element of  $G/H$  is  $H$  ( $Hg \cdot H = HHg = Hg$ )

iv)  $\varphi^{-1}(H) = \ker \varphi = H$   
↑ an element  $G/H$       ↑ subset in  $G$

v) The cosets of  $H$  in  $G$  are in general, the pre-image sets  
of  $\varphi$ .

"fibers" = set of elements in  $G$   
all mapping to same place

briefly

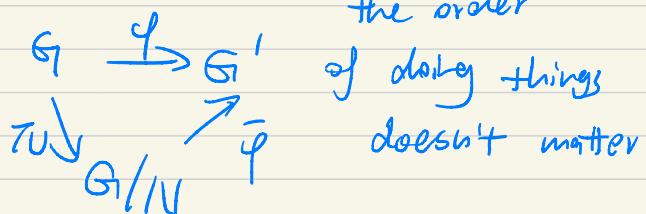
we described a machine which, when we inputted a normal subgp  $H \triangleleft G$ , outputted an onto hom  $\varphi: G \rightarrow G/H$

1<sup>st</sup>  
isomo  
theorem

Given  $\varphi: G \rightarrow G'$  an onto hom, let  $\ker \varphi = N$ . Then  $G/N$   
is isomorphic to  $G'$ .

Also,  $\exists$  an only isomo  $\bar{\varphi}: G/N \rightarrow G'$  that "commutes with"  
the natural map  $\pi: G \rightarrow G/N$ ,  $\pi(g) = Ng$

i.e.  $\varphi = \bar{\varphi} \circ \pi$



Pf Start with  $\varphi: G \rightarrow G'$  an onto hom. Define  $\bar{\varphi}: G/N \rightarrow G'$  by  $\bar{\varphi}(Ng) = \varphi(g)$

For this idea to actually make sense, we have to show that if  $Ng_1 = Ng_2$ , then  $\varphi(g_1) = \varphi(g_2)$  names don't matter  $\times 2$

$$Ng_1 = Ng_2 \Leftrightarrow g_1 g_2^{-1} \in N = \ker \varphi$$

$$\Rightarrow \varphi(g_1 g_2^{-1}) = e' \text{ (identity in } G') \Rightarrow \varphi \text{ is hom}$$

$$\Rightarrow \varphi(g_1) \varphi(g_2)^{-1} = e' \Rightarrow \varphi(g_1) = \varphi(g_2)$$

i)  $\bar{\varphi}$  is a hom:  $\bar{\varphi}(Ng_1, Ng_2) = \bar{\varphi}(Ng_1 g_2)$   $N$  is normal  $\rightarrow$  kernel of any hom is always a subgroup

$$= \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) = \bar{\varphi}(Ng_1) \bar{\varphi}(Ng_2)$$

ii)  $\bar{\varphi}$  is onto: Given  $g' \in G'$

Given  $g' \in G'$ , want to find some  $x \in G/N$  s.t.  $\bar{\varphi}(x) = g'$

$\varphi$  onto  $\Rightarrow \exists y \in G$  s.t.  $\varphi(y) = g'$ . Then  $\pi(y) = Ny$

$$\nmid \bar{\varphi}(Ny) = \varphi(y) = g'$$

iii)  $\bar{\varphi}$  is one to one: If  $\bar{\varphi}(Ng_1) = \bar{\varphi}(Ng_2)$

$$\Rightarrow \varphi(g_1) = \varphi(g_2) \Rightarrow \varphi(g_1) \varphi(g_2)^{-1} = e' \Rightarrow \varphi(g_1 g_2^{-1}) = e'$$

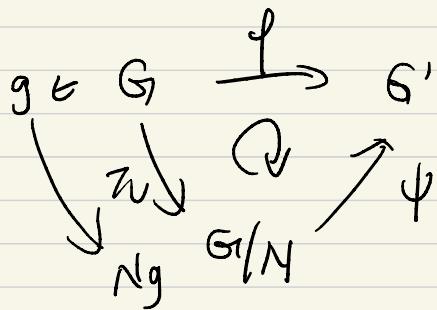
$$\Rightarrow g_1 g_2^{-1} \in \ker \varphi = N \Rightarrow Ng_1 = Ng_2$$

iv) commuting: Given  $g \in G$ , WTS that  $\varphi(g) = \bar{\varphi}(\pi(g))$ .

$$\pi(g) = Ng \quad \nmid$$

For uniqueness,  $\psi$  satisfies,  $\psi: G/N \rightarrow G'$ , an iso,

$$\varphi = \psi \circ \pi.$$



for this to work  $\psi$  has to send the coset  $Ng$  to  $\psi(g)$ . Because if not,  $\psi(g) \neq \psi(\pi(g))$ .

But, this is exactly how we defined  $\bar{\varphi}$ , so  $\bar{\varphi} = \psi$ .

ker  $\varphi$  is called the "commutator subgp"



Oct 12

Def'n

A **subring** of  $\mathbb{C}$  is a subset  $R \subset \mathbb{C}$ , closed under addition, subtraction, multiplication & containing 1

ex 1

"Gaussian integers",  $\mathbb{Z}[\text{i}] = \{a + bi \mid a, b \in \mathbb{Z}\}$

Given  $\alpha \in \mathbb{Z}$ , consider  $\mathbb{Z}[\alpha] = \text{subring generated by } \alpha$   
= smallest subring of  $\mathbb{Z}$  containing  $\alpha$

Note.. any subring of  $\mathbb{C}$  contains  $\mathbb{Z}$  as a subset  
(it contains 1 & it's closed under addition & subtraction)

$\mathbb{Z}[\alpha]$  = smallest subring of  $\mathbb{C}$  containing  $\alpha$   
 $\mathbb{Z}$  adjoint  $\alpha$  (so it also contains  $\mathbb{Z}$ )

If  $a_0, a_1, \dots, a_n \in \mathbb{Z}$ , then  $\underbrace{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0}_\text{polynomial p(x)} \in \mathbb{Z}[\alpha]$

so,  $\mathbb{Z}[\alpha]$  contains  $p(\alpha)$ , where  $p$  is any polynomial with integer coefficient.

claim: the polynomials are all of  $\mathbb{Z}[\alpha]$

proof:

let  $S = \{a_n\alpha^n + \dots + a_1\alpha + a_0 \mid n \in \mathbb{N} \setminus \{0, \dots, a_0, \dots, a_n \in \mathbb{Z}\}$

Then  $S$  is closed under addition  
multiplication & subtraction

Also,  $1 \in S \Rightarrow S$  is a subring of  $\mathbb{C}$   
 $\Rightarrow S \subset \mathbb{Z}[\alpha] \Rightarrow S = \mathbb{Z}[\alpha]$  cuz  $\mathbb{Z}[\alpha]$  is the smallest

Def'n

$\alpha \in \mathbb{C}$  is called **algebraic** if  $\exists$  a polynomial w/ integer coefficient  $p$   
s.t.  $p(\alpha) = 0$

Otherwise,  $\alpha$  is called **transcendental**.

If  $\alpha$  is transcendental,  $\mathbb{Z}[\alpha]$  is in 1-1 correspondence w/  
an polynomials w/ integer coeff's

i.e. if  $a_m\alpha^m + \dots + a_1\alpha + a_0 = b_m\alpha^m + \dots + b_1\alpha + b_0$

then  $m=n$ ,  $a_m=b_m, \dots, a_0=b_0$

$\star \Rightarrow m > n$

$$a_m\alpha^m + \dots + (a_n - b_n)\alpha^n + \dots + (a_0 - b_0) = 0$$

so  $p(x) = a_m x^m + \dots + (a_n - b_n)x^n + \dots + (a_0 - b_0)$  is a poly's with  
 $\mathbb{Z}$  coeff's s.t.  $p(\alpha) = 0$ . But  $\alpha$  is transcendental  $\Rightarrow p(x) \neq 0$

Defn A **ring** is a set  $R$ , together with 2 binary operations,  
called "addition" & "multiplication"  
satisfying: (i)  $(\underline{R}, +)$  is an abelian group (identity = "0")  
 $\quad \quad \quad R^+$   
(ii) multiplication is commutative  
associative  
(iii)  $\exists$  an identity element called "1",  
 $\forall a, b, c \in R, (a+b)c = ac + bc$

A subring of  $R$  is a subset  $S \subset R$ ,  
closed under addition, subtraction, multiplication & containing 1.

Oct 14

Def'n If  $r \in R^{\text{ring}}$  {  $\exists s \in R$  st.  $rs = 1$ .  $r$  is called a **unit** in  $R$

Def'n If  $F$  is a ring where every non-zero element is a unit, then  $F$  is called a **field**.

Lemma If  $R$  is a ring which  $1=0$ , then  $R = \{0\}$

Pf

Let  $a \in R$ ,

$$\begin{aligned} a \cdot 1 &= a \quad \text{by def'n of multi} \\ \text{But } 1=0 \Rightarrow a \cdot 0 &= a \\ &\stackrel{a \cdot (0+0)}{=} a \cdot 0 + a \cdot 0 \\ 0 &= a \cdot 0 = a \end{aligned}$$

If  $R$  is any ring, we can form a new ring called  $R[\pi]$  = {poly's w/ coeff's in  $R$ }

Def'n A ring homomorphism  $\varphi: R \rightarrow R'$  is a **map**  
s.t. If  $a, b \in R$ ,  $\varphi(a+b) = \varphi(a) + \varphi(b)$ ,  
 $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ ,  
 $\varphi(1) = 1_{R'}$

generalized evaluation

Substitution Principle Let  $\varphi: R \rightarrow R'$  be a ring hom

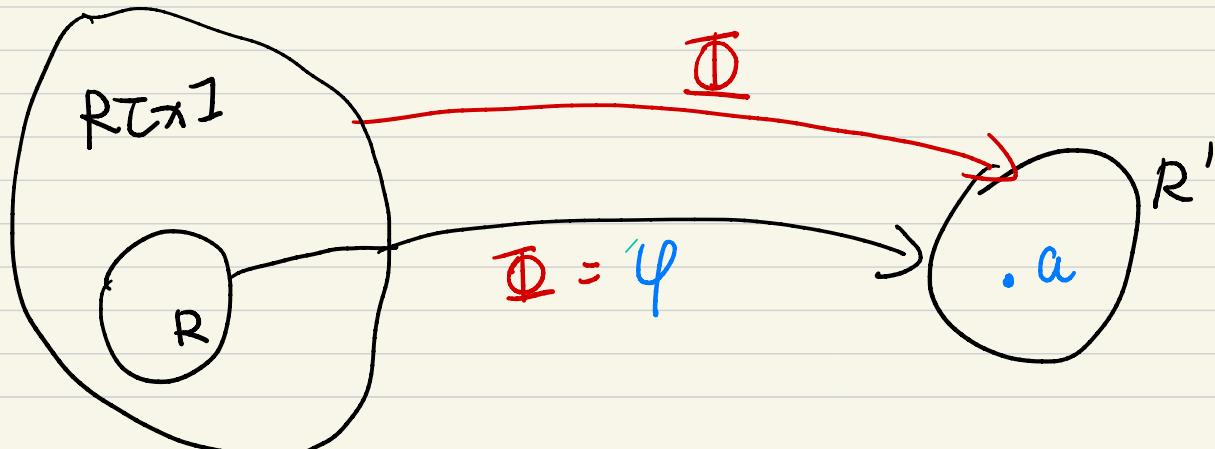
let  $R[\pi]$  be the ring of poly's w/ coeff's in  $R$ .

Then given "your fav"  $a \in R'$

$\exists$  ! ring hom  $\underline{\Phi}: R[\pi] \rightarrow R'$  s.t.  $\underline{\Phi}|_R = \varphi$

i)  $\underline{\Phi}$  (constant poly =  $r = \text{ring element}$ ) =  $\varphi(r)$

ii)  $\underline{\Phi}(x) = a$



Oct 16

Intuition Every ring hom is the restriction of a unique\* generalized evaluation  
the only unique one once you choose  $a \in R'$

Pf

Given  $\varphi: R \rightarrow R' \nsubseteq R'$ , define  $\mathbb{D}_a: R[x] \rightarrow R'$  by  
 $\mathbb{D}_a(a_n x^n + \dots + a_1 x + a_0) = \varphi(a_n)a^n + \dots + \varphi(a_1)a + \varphi(a_0)$

①  $\mathbb{D}_a$  is a ring hom

Check that  $\mathbb{D}_a$  is a ring hom:

$$\text{WTS } \mathbb{D}_a(p(x)q(x)) = \mathbb{D}_a(p(x))\mathbb{D}_a(q(x))$$

$$\mathbb{D}_a(p(x)+q(x)) = \mathbb{D}_a(p(x)) + \mathbb{D}_a(q(x)) \quad \star$$

$$\mathbb{D}_a(1_R) = 1_{R'} \quad \leftarrow \text{works because } \mathbb{D}_a(1) = \varphi(1) = 1 \text{ since } \varphi \text{ is a ring hom. ALSO, if } r \in R, \mathbb{D}_a(r) = \varphi(r) \text{ by the formula, \& this verifies (i).}$$

$$\begin{aligned} \text{If } p(x) &= a_n x^n + \dots + a_0 \\ q(x) &= b_m x^m + \dots + b_0 \end{aligned} \quad \text{then } \mathbb{D}_a(p+q) = \mathbb{D}_a(a_n x^n + \dots + (a_m+b_m)x^m + \dots + (a_0+b_0))$$

$$= \varphi(a_n)a^n + \dots + \varphi(a_m+b_m)a^m + \dots + \varphi(a_0+b_0)$$

$$\stackrel{\varphi \text{ is a ring hom}}{=} \varphi(a_n)a^n + \dots + (\varphi(a_m) + \varphi(b_m))a^m + \dots + (\varphi(a_1) + \varphi(b_1))a + \varphi(a_0) + \varphi(b_0)$$

$$= \mathbb{D}_a(p) + \mathbb{D}_a(q).$$

24.34 / 00:59:40 40 2.0x [G]

Let  $f(x) = \sum_{i=1}^n a_i x^i$ ,  $g(x) = \sum_{j=1}^m b_j x^j$ . Then  $\mathbb{D}_a(f) = \varphi(f)$  by the formula, \& this verifies (ii).

$$\begin{aligned} \mathbb{D}_a(fg) &\stackrel{\text{by def'n of } \mathbb{D}_a}{=} \mathbb{D}_a \left( \sum_{i=1}^n \sum_{j=1}^m a_i b_j x^{i+j} \right) \stackrel{\star}{=} \sum_{i=1}^n \sum_{j=1}^m \mathbb{D}_a(a_i b_j x^{i+j}) \\ &= \sum_{i=1}^n \sum_{j=1}^m \varphi(a_i b_j) a^{i+j} \stackrel{\varphi \text{ is a ring hom}}{=} \sum_{i=1}^n \sum_{j=1}^m \varphi(a_i) \varphi(b_j) a^{i+j} = \mathbb{D}_a(f)\mathbb{D}_a(g) \end{aligned}$$

② uniqueness

Uniqueness: Suppose  $w: R[x] \rightarrow R'$  some ring hom s.t.

$$w(r) = \varphi(r) \quad \forall r \in R \quad \nexists \quad w(x) = a \quad \text{since } w \text{ is a ring hom}$$

$$\begin{aligned} \text{Then } w(a_n x^n + \dots + a_1 x + a_0) &= w(a_n) w(x^n) + \dots + w(a_1) w(x) + w(a_0) \\ &= \varphi(a_n) a^n + \dots + \varphi(a_1) a + \varphi(a_0) \\ &= \mathbb{D}_a(a_n x^n + \dots + a_1 x + a_0). \end{aligned}$$

Thm If  $R$  = ring, then  $(R[x])_{[y]} \cong R[x, y]$   
Pf  $R$  is a subring of  $R[x]$  &  $R[x]$  is a subring of  $(R[x])_{[y]}$   
So,  $R$  is a subring of  $(R[x])_{[y]}$

Consider the map  $\varphi: R \rightarrow (R[x])_{[y]}$  (inclusion)  
 $r \mapsto r$  sends to itself

Sub principle:  $\exists!$  ring hom  $\Phi: R[x, y] \rightarrow (R[x])_{[y]}$   
claim:  $\Phi$  is a bijection

$R[x]$  is a subring of  $R[x, y]$ .

$\exists$  inclusion:  $R[x] \hookrightarrow R[x, y]$

so by sub principle:

$$\tau: (R[x])_{[y]} \rightarrow R[x, y]$$

Oct 19

Def'n An **ideal** of a ring  $R$  is a non-empty set  $I \subseteq R$  s.t.

- i)  $I$  is closed under  $+$
- ii) Given  $r \in R$   $\nexists s \in I$ ,  $rs \in I$

Lemma Given  $\varphi: R \rightarrow R'$  a ring hom.  
then  $\ker \varphi$  is an ideal of  $R$   
 $\{r \in R \mid \varphi(r) = 0_{R'}\}$

Pf. Note  $\varphi(0_R) = 0_{R'} \Rightarrow \ker \varphi \neq \emptyset$

$\forall a, b \in \ker \varphi$

$$\varphi(a+b) = \varphi(a) + \varphi(b) = 0_{R'} \Rightarrow a+b \in \ker \varphi$$

$\forall r \in R \quad \nexists s \in \ker \varphi$

$$\varphi(sr) = \varphi(s)\varphi(r) = 0_{R'} \cdot \varphi(r) = 0_{R'} \Rightarrow rs \in \ker \varphi$$

$$0_{R'} \cdot a = 0_R$$

Lemma  $I$  is an ideal  $\Rightarrow I \neq \emptyset$

$\{$  any linear comb  $rs_1 + \dots + rs_k$  of  $s_i \in I \mid r \in R\}$  is in  $I$

crt Given  $a \in R$ . its "multiples" form an ideal

$$\{ra \mid r \in R\}$$

"principal ideal" generated by  $a$ , denoted as  $(a)$ .

An ideal is **proper** if  $I \neq \{0_R\}$ ; if  $I \neq R$

Caution: Proper ideals are NOT subrings!!

if  $1_R \in I$ , then  $I = R$

Prop. Every ideal in  $F[x]$  is principal  
 $\uparrow$  field

A ring in which every ideal is principal is called  
a "principal ideal domain" (PID).

i.e. if  $F = \text{field}$ , then  $F[x]$  is a PID

Poly's A poly  $a_n x^n + \dots + a_1 x + a_0$  is **monic** if  $a_n = 1$

Poly division If  $R = \text{ring}$ ,  $f \in R[x]$   $\{ f \text{ is monic},$   
 $g \in R[x], \text{ then } \exists \{ \text{poly's } q(x) \mid r(x) \in R[x] \text{ s.t.}$   
 $g(x) = f(x)q(x) + r(x), \quad \{ \deg(r) < \deg(f) \}$

Pf Fix  $I = \text{ideal in } F[x]$ . WTS  $I = (f(x))$

for some  $f \in I$ , If  $I = (g)$ ,  $I$  is principal, choose  $f = 0$

so assume  $I \neq 0 \Rightarrow \exists$  nonzero poly's in  $I$

choose  $f \in I$  s.t.  $\deg(f)$  is minimal among all possible poly's in  $I$

Suppose  $f(x) = a_n x^n + \dots + a_1 x + a_0$

$F = \text{field} \Rightarrow \exists$  a multi inverse of  $a_n$ . Multiply  $f$  by  $a_n^{-1}$

(we are still in  $I$ ) we get  $\tilde{f}(x) = x^n + a_{n-1} a_n^{-1} x^{n-1} + \dots + a_1 a_n^{-1} x + a_0 a_n^{-1}$

$\deg(\tilde{f}) = \deg(f)$ . so it's minimal degree AND monic

claim:  $I = (\tilde{f})$

$(\tilde{f}) \subset I$ , WTS  $I \subset (\tilde{f})$

choose  $g(x) \in I$ . polynomial division

$$g = \tilde{f}q + r \Rightarrow g - \tilde{f}q \in I \Rightarrow r \in I$$

contradict

unless  $r(x) = 0$

$$\Rightarrow g = q\tilde{f} \Rightarrow I \subset (\tilde{f})$$

Very basic lemma

If  $R$  is any ring,  $\exists!$  ring hom  $\varphi: \mathbb{Z} \rightarrow R$ .

It's given by  $\varphi(n) = l_R + l_R + \dots + l_R$ , if  $\varphi(-n) = -\varphi(n)$

The **characteristic** of  $R$  is the non-negative number  $n$  generating the kernel of  $\varphi: \mathbb{Z} \rightarrow R$

i.e. smallest # of times you have to add  $l_R$  to itself in  $R$ , to get  $0_R$ .

$R/I = \{1+a \mid a \in R\}$  has a group structure since  $I$  is normal

Does it have a ring structure??

Oct 21

Thm.

$\exists!$  way of turning  $R/I$  into a ring

s.t. natural map  $\pi: R \rightarrow \frac{R}{I}$  is a ring hom w/  $\ker = I$

$$r \mapsto \bar{r} = r + I$$

$$\{\text{wsets } I+r \mid r \in R\}$$

Pf sketch

$I+a, I+b \in R/I$

$$(I+a) \cdot (I+b) := I+ab$$

WTS  $I+a' = I+a$  &  $I+b' = I+b$ , then  $I+ab = I+a'b'$

$a' \in I+a'$  thus  $a' \in I+a$

$$a' = i_1 + a$$

$$b' = i_2 + b$$

$$a'b' = (i_1 + a)(i_2 + b) = i_1i_2 + i_2a + i_1b + ab$$

$\underbrace{i_2a + i_1b}_{\in I}$

$$\Rightarrow a'b' - ab \in I \Rightarrow I+a'b' = I+ab$$

multi identity:  $I + 1_R$

add identity:  $I$

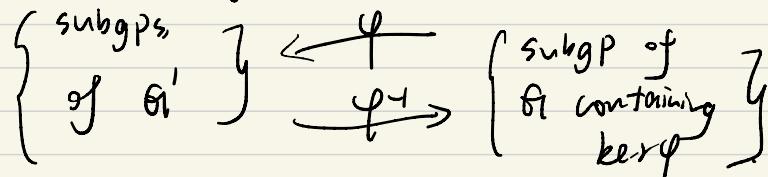
If  $\pi: R \rightarrow R/I$  is a ring hom

$$\text{then } \ker(\pi) = I$$

Correspondence  
Thm

Let  $\varphi: G \rightarrow G'$  an onto gp hom

Then  $\exists$  a bijective correspondence

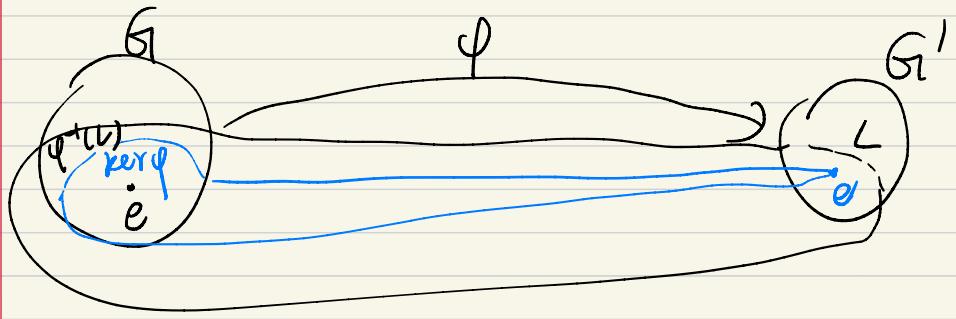


given by if  $H$  is a subgp of  $G'$

containing  $\ker \varphi$ , send  $H$  to  $\varphi(H)$

And if  $L$  is a subgp of  $G'$ , send  $L$  to

$$\varphi^{-1}(L) = \{g \in G \mid \varphi(g) \in L\}$$



$\psi: R \rightarrow R'$  onto ring hom w/ kernel  $K \subset R$

Then  $\exists$  bijective corr between ideals in  $R'$

↓ ideals in  $R$ , containing  $K$ ,

If  $I$  in  $R$  corr to  $I'$  in  $R'$

$$\text{then } \frac{R}{I} \cong \frac{R'}{I'}$$

1st iso thm for rings

Let  $\phi: R \rightarrow R'$ , a ring hom w/ kernel  $K \subset R$

$I$  be an ideal in  $R$ .

Let  $\pi: R \rightarrow \frac{R}{I}$  be the natural map

If  $I \subseteq K$ .  $\exists$  ring hom  $f: \frac{R}{I} \rightarrow R'$  s.t.

If  $f$  is onto  $\{ I = K, f \text{ is an isomo}$

Oct 23

$R/(a_1, \dots, a_n)$  the same as putting  $(a_1, \dots, a_n)$  as 0

Given  $I = (a, b)$ , we want to understand  $R/(a, b)$

$\exists$  a <sup>onto</sup> ring hom  $\pi: R \rightarrow R/(a)$   $\ker(\pi) = (a)$

$$r \mapsto r + (a)$$

correspondence then

$\Rightarrow \exists$  a way to partner ideals in  $R/(a)$   
with ideals in  $R$  containing  $(a)$ .

$\swarrow$   
 $I$  is the ideal in  $R$  containing  $(a)$   
 $= (a, b)$

$$\frac{R}{I} \approx \left( \frac{R/(a)}{\pi(I)} \right) \quad \pi((a, b)) = \pi((b))$$

$$\frac{R}{(a, b)} \approx \left( \frac{R/(a)}{\pi((b))} \right)$$

ex 1  $\mathbb{Z}[i]/(i-2)$  ( $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ )

strategy: onto hom  $\Rightarrow$   $1^{\text{st}}$  iso then  $\nmid$  corresp then

onto  $\varphi_i: \mathbb{Z}[x] \rightarrow \mathbb{Z}[i]$   
 $p(x) \mapsto p(i)$   
 $\ker \varphi_i = (x^2 + 1)$

$$1^{\text{st}} \text{ iso then } \Rightarrow \mathbb{Z}[x]/(x^2 + 1) \approx \mathbb{Z}[i]$$

$$\mathbb{Z}[x]/(x^2+1, x-2)$$

① mod out  $\mathbb{Z}[x]$  by  $(x-2)$

an onto hom:  $\varphi_2: \mathbb{Z}[x] \rightarrow \mathbb{Z}$   
 $p \mapsto p(2)$

$$\ker \varphi_2 = (x-2)$$

Then we want to mod  $\mathbb{Z}$  out by  $\varphi_2(x^2+1) = 5$

$$\mathbb{Z}[x]/(x^2+1, x-2) \cong \mathbb{Z}/5\mathbb{Z}$$

Oct 26

Adjoining

$R = (R, +, \cdot)$  we want to add a new element called " $i$ " satisfying  $i^2 = -1$

new element a relation

Define  $R[i] = \{a+bi \mid a, b \in R\}$

$\Downarrow$   
R adjoin  $i$

Proposition

$R = \text{ring}$ ,  $f(x) = \text{monic Poly in } R[x]$

suppose  $(f(x)) >_0$ , let  $n = \deg(f)$

Then let  $R[\alpha]$  denote the quotient ring  $\frac{R[x]}{(f(x))}$

= the ring obtained by adjoining element " $\alpha$ " to  $R$  s.t.  $f(\alpha) = 0$

a) The set  $(1, \alpha, \dots, \alpha^{n-1})$  is a basis for  $R[\alpha]$  over  $R$   
i.e. for any  $\lambda \in R[\alpha]$ ,  $\lambda = r_0 \cdot 1 + r_1 \alpha + \dots + r_{n-1} \alpha^{n-1}$   
for some unique  $r_0, r_1, \dots, r_{n-1}$

b) Addition in  $R[\alpha]$  corr. to vector addition

c) Multiplication of linear combinations is given by:  
if  $\beta_1, \beta_2 \in R[\alpha]$ , let  $g_1(x), g_2(x)$  be poly's s.t.  $\beta_1 = g_1(\alpha), \beta_2 = g_2(\alpha)$   
Use poly division

$$g_1 g_2 = f q + r \quad \text{where } \deg(r) < n$$

$$\text{Then } \beta_1 \beta_2 = r(\alpha)$$

Def'n A ring  $R$  is called an integral domain if such a larger ring exists. i.e. if  $a, b \in R \setminus \{0_R\} \Rightarrow ab = 0_R \Leftrightarrow a=0$  or  $b=0$

non- $\exists$

$\mathbb{Z}_n$   
non-prime, e.g.: 6

If  $R = \text{any ring}$ , place an equiv rel'n on  $R \times R - \{0_R\}$

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$

$$\frac{a}{b} \frac{c}{d} := \frac{ac}{bd}$$

This forms a field, called field of fractions of the integral domain  $R$

Oct 28

Thm

creating fields from rings.

Given  $R = \text{ring}$ , philosophically we might imagine creating a field from  $R$  in two ways

i) add elements, yielding some field  $F$  s.t.  $R \subset F$  is subring

ii) kill elements, yielding a field  $F$  as  $R/I$

Note, if  $R$  has zero divisors, (i) is not available

Thus (i) is an integral domain.

Given  $R = \text{integral domain}$ , consider  $\sim$  on  $R \times (R - \{0\})$  as:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

Then  $F(R) = \text{"field of fractions"}$

WTS: if  $(a, b) \sim (a', b')$ ,  $(c, d) \sim (c', d')$

$$\text{then } (ad + bc, bd) = (a'd' + b'c', b'd')$$

Proof: WTS:  $(ad + bc)b'd' = bd(a'd' + b'c')$

Note:  $F(R)$  is a field  $\Leftrightarrow$  every non-zero element is invertible

↳ ring axioms are satisfied.

$[1(0, 1)]$  is the  $0$ -element

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = 1$$

Mapping Principle:

If  $F$  is a field containing  $R = \text{integral domain}$  as a subring, then  $\exists$  an injective ring hom

$$\psi: F(R) \rightarrow F, \text{ given by } \psi([a, b]) = \psi\left(\frac{a}{b}\right) = ab^{-1}$$

Quick terminology for integral domains:

- $u$  is a unit if an element in  $R$  w/ a mult<sup>-1</sup> inverse
- $a$  divides  $b$  if  $\exists q \in R$  s.t.  $b = aq$
- a  $\neq$  unit is a proper divisor of  $b$   
if  $\exists q \in R$ ,  $q \neq$  unit s.t.  $b = aq$
- $a \nmid b$  are associates if each divides the other,  
or, if  $b = ua$ ,  $u =$  unit
- $a$  is irreducible if a  $\neq$  unit & has no proper divisors
- $a$  is prime if  $a \neq$  unit if whenever  $p \mid ab$ ,  
 $p \mid a$  or  $p \mid b$

Lemma

$$R = \text{integral domain}$$

then  $u$  is a unit  $\Leftrightarrow (u) = R$

$a$  divides  $b$   $\Leftrightarrow (b) \subset (a)$

$a$  is a proper divisor of  $b$   $\Leftrightarrow b \notin (a) \subset R$

$a \nmid b$  are associates  $\Leftrightarrow (a) = (b)$

$a$  is irreducible  $\Leftrightarrow (a) \neq R$  &  $\nmid$  an ideal  $(c)$   
s.t.  $(a) \subset (c) \neq R$

$a \mid b$

## Maximal ideals

$R = \text{any ring.}$

A maximal ideal  $M$  in  $R$  is an ideal

$M \neq R$  s.t. if  $I$  contains  $M$

either  $I = M$  or  $I = R$

Proposition:  $R/I$  is a field  $\Leftrightarrow I$  is a maximal ideal

Pf:

Lemma:  $R$  is a field  $\Leftrightarrow R$  contains precisely 2 ideals.

Assume  $I$  is maxil in  $R$

Consider the natural map  $\pi: R \rightarrow R/I$  (onto ring hom)

corr. theorem  $\Rightarrow \{\text{ideals in } R/I\} \longleftrightarrow \{\substack{\text{ideals of } R \\ \text{containing} \\ \ker \pi = I}\}$

$I$  maximal  $\Rightarrow$  only ideals in  $R/I$  are 0-ideal  $\{ \frac{R}{I} \}$

By lemma,  $R/I$  is a field.

$R/I$  is a field  $\Rightarrow$  no proper ideals in  $R/I$

corr. thm  $\Rightarrow$   $\#$  proper ideals in  $R$  containing  $I$

$\Rightarrow I$  is maximal.

Prop  
a)

Let  $\varphi: R \rightarrow R'$  surjective ring hom.

$$\varphi(r+s) = \varphi(r) + \varphi(s)$$

$$\varphi(rs) = \varphi(r)\varphi(s)$$

$$\varphi(1_R) = 1_{R'}$$

$$\text{let } I = \ker \varphi = \{ r \in R \mid \varphi(r) = 0_{R'} \}$$

recall: kernel of any ring hom is ideal

Then  $R'$  is a field ( $\Rightarrow I$  is a maximal ideal)

Proof

A ring is a field  $\Leftrightarrow$  it contains precisely 2 elements

$$\begin{matrix} \text{or } \\ \text{or } \end{matrix} \left. \begin{matrix} 0_R \\ 1_R \end{matrix} \right\} R \text{ as ideals}$$

( $\Leftarrow$ ) Suppose  $R$  contains no other ideals  $\{ 0_R, r \neq 0_R \}$   
 $\Rightarrow (r) \neq \{ 0_R \}$   
 $\Rightarrow (r) = R$

$$\text{so, } 1_R \in (r)$$

so  $\exists x \in R$  st.

$$1_R = xr \Rightarrow x \text{ is multi inverse}$$

$\Rightarrow r$  is invertible

( $\Rightarrow$ )

let  $J$  be an ideal

$$\text{Wts: } J = \{ 0_R \} \text{ or } R$$

Suppose  $J \neq \{ 0_R \}$

Then  $\exists r \in J, r \neq 0_R$

$R$  is a field  $\Rightarrow r$  has a multi inverse,  $x$

$J$  is an ideal  $\Rightarrow xr \in J \Rightarrow 1_R \in J \Rightarrow s \cdot 1_R \in J$

$$\Rightarrow J = R$$

$\nwarrow$  arbitrary

## correspondence theorem

If onto hom,  $\exists$  bijective correspondence

$$\left\{ \begin{array}{l} \text{ideals in } R \\ \text{containing } \ker\varphi \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{ideals in } R' \\ \text{in } R' \end{array} \right\}$$

$$\begin{array}{ccc} I & \longleftrightarrow & \varphi(I) \\ \varphi^{-1}(J) & \longleftrightarrow & J \end{array}$$

ideals in  $R'$  correspond  
ideals in  $R$  contain  $\ker\varphi$ .

$$\begin{array}{ccc} I & \longrightarrow & \varphi(I) \\ \varphi^{-1}(J) & \longleftarrow & J \end{array}$$

So if  $\ker\varphi$  is a maximal ideal,  $\nexists$  any proper ideals in  $R$   
properly containing  $\ker\varphi \Rightarrow \nexists$  any ideals in  $R'$  between  $0_{R'} \nsubseteq R'$ .  
 $\Rightarrow R'$  is a field. Conversely,  $R' = \text{field} \Rightarrow \nexists$  any proper ideals in  $R'$ .  
 $\Rightarrow \nexists$  any proper ideals of  $R$  containing  $\ker\varphi \Rightarrow \ker\varphi$  is maximal.

b)  $I$  is maximal  $\Leftrightarrow R/I$  is a field

$$\begin{aligned} \{r+I | r \in R; r+I = r'+I\} &= r+I \\ r+r'^{-1} \in I & \\ r-r' \in I & \end{aligned}$$

Pf: (2) onto ring hom  $\pi: R \rightarrow R/I$ ,  $\ker \pi = I$

from (a):  $R/I$  is a field

(3)  $R/I$  is a field  $\Rightarrow \nexists$  any proper ideal in  $R/I$

correspondence  $\Rightarrow \nexists$  any proper ideals in  $R$ , containing  $\ker \pi$

$\Rightarrow \ker \pi$  is maximal

c) the zero ideal of  $\mathbb{F}$  or  $\mathbb{Q}$  of  $R$  is maximal  $\Leftrightarrow R$  is a field

Pf: Suppose  $\{0_R\}$  is max'l  $\Rightarrow \nexists$  a proper ideal, properly containing  $\{0_R\} \Rightarrow R$  is a field. Conversely, if  $R$  is a field, it doesn't contain a proper ideal,  $\neq \{0_R\} \Rightarrow \{0_R\}$  is max'l.

Nov 13

Reminder

If  $R = \text{ring}$ ,  $r \in R$  is called **irreducible**  
if  $\nexists x, y \in R$ , neither of which are units

(neither  $x$  nor  $y$  is multi-invertible)

s.t.  $r = xy$   $\Rightarrow$   $s \notin \text{unit}$

$s \in R$  is **prime** if whenever  $s|xy$ ,  $s|x$  or  $s|y$

Question.

If  $f$  is reducible in  $\mathbb{Q}[x]$ ,  
is  $f$  reducible in  $\mathbb{Z}[x]$ ?

Lemma

- $r(x) = b_1x + b_0 \in \mathbb{Z}[x]$  divides  $f \in \mathbb{Z}[x]$ ,  
 $f = a_nx^n + \dots + a_0$ , then  $b_1 | a_n$  &  $b_0 | a_0$ .
- Assume  $b_1 \neq 0$ . Then  $r(x) = b_1x + b_0$  divides  $f \in \mathbb{Z}[x]$   
 $\Rightarrow -\frac{b_0}{b_1}$  is a root of  $f$  i.e.  $f(-\frac{b_0}{b_1}) = 0$
- A rational root of a monic poly in  $\mathbb{Z}[x]$  is an integer  
 $\Rightarrow$  coeff of highest term is 1

Proof

a) i.e.  $f = r(x) \cdot q(x)$  **l sum poly**  
 $a_0 = q_0 b_0 \Rightarrow b_0 | a_0$   
 $a_n = b_1 q_m \Rightarrow b_1 | a_n$

b) idea:  $f(-\frac{b_0}{b_1}) = 0 \Rightarrow (x - \frac{b_0}{b_1})$  is a factor of  $f$  in  $\mathbb{Q}[x]$

c) A rational root of a monic integer poly is an integer

Pf: suppose  $\frac{a}{b}$  is a root of  $f \in \mathbb{Z}[x]$

i.e.  $f(\frac{a}{b}) = 0 \Rightarrow b|a$  divides  $f$   
 $\Rightarrow b|a_n \Rightarrow b = \pm 1 \Rightarrow \frac{a}{b} \in \mathbb{Z}$

Def'n A poly is primitive if  $a_n > 0 \wedge \gcd(a_n, \dots, a_0) = 1$

Lemma Let  $f \in \mathbb{Z}[x]$ ,  $\deg(f) > 0 \wedge a_n > 0$ .

Then TFAE:

i)  $f$  is primitive

ii)  $\forall$  prime numbers  $p \in \mathbb{Z}$ ,  $p$  doesn't divide  $f$  as elements of  $\mathbb{Z}[x]$

iii) if  $\psi_p: \mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x]$  given mod  $p$  on each coeff.  
then  $f \notin \ker(\psi_p) \wedge p$

Prop.

a)  $n \in \mathbb{Z}$  is prime in  $\mathbb{Z}[x]$   $\Leftrightarrow n$  is prime in  $\mathbb{Z}$

b)

Gauss's Lemma:

The product of primitive Poly's primitive

Pf.

claim: If  $f(x)$  is prime, it's irreducible

Pf: suppose,  $\exists a(x), b(x)$  s.t.  $f(x) = a(x)b(x)$  ( $a, b \neq 1$ )

$f$  prime  $\Rightarrow f$  divides either  $a$  or  $b$

assume it's a

$$f | a \Rightarrow a = fc \quad f = fcb$$

$$1 = cb \quad (from \mathbb{Q})$$

$b$  is unit.

a) Suppose  $n$  is prime in  $\mathbb{Z}[x]$

claim:  $n$  is irreducible in  $\mathbb{Z}[x]$

Note:  $\mathbb{Z}[x]$  is integral domain (i.e. no zero divisor)

$$fg = 0$$

$$f=0 \text{ or } g=0$$

Lemma: If  $R$  is an integral domain  $\forall r \in R$  is prime  
 $\Rightarrow r$  is irreducible

Now assume  $n$  is prime in  $\mathbb{Z}$ , suppose  $n \mid fg$

wts:  $n \mid f$  or  $n \mid g$

$\mathbb{Z}/n\mathbb{Z}[x]$  integral domain  $\Rightarrow \psi_n(f) = 0$  or  $\psi_n(g) = 0$   
(it's a field)  $n \mid f$   $n \mid g$

b) suppose  $f, g$  are primitive.

$\Rightarrow$  leading coeff are positive

$\Rightarrow$  no prime divides all coeff's of  $f$   $\nwarrow$  same p?

Recall  $p$  divides  $fg \Leftrightarrow p|f$  or  $p|g$

Lemma.  $c \in \mathbb{Z} \Leftrightarrow f \in \mathbb{Z}[x] \setminus \{c = \text{gcd coeff's of } f\}$

Nov 18

Thm

a) Let  $f(x) = \text{primitive } f g \in \mathbb{Z}[x]$ . Then if  $f \mid g$  in  $\mathbb{Q}[x]$ , then  $f \mid g$  in  $\mathbb{Z}[x]$

b) If  $f, g \in \mathbb{Z}[x]$  share a common non-constant factor in  $\mathbb{Q}[x]$ , then so in  $\mathbb{Z}[x]$

Pf

a) i.e.  $\exists h(x) \in \mathbb{Q}[x]$  s.t.  $f_0 \cdot h = g$

WTS:  $h \in \mathbb{Z}[x]$

Recall that  $\exists!$  a way to express  $h(x)$  as  $h(x) = c \cdot h_0(x)$  where  $c \in \mathbb{Q}$ ,  $h_0(x)$  primitive

$$g = f_0 \cdot (c h_0)$$

$$g = c f_0 h_0 \quad \text{primitive}$$

$\exists!$  to express  $g(x)$  as  $g(x) = c' \cdot g_0(x)$  where  $c' \in \mathbb{Q}$   
 $g_0(x)$  is prim AND since  $g \in \mathbb{Z}[x]$ ,  $c' = \pm \text{gcd}(c, \text{coeff}(g))$

Uniqueness  $\Rightarrow c = c' \quad \{ f_0 h_0 = g_0 \}$

b) Assume  $f, g \in \mathbb{Z}[x]$  share a non-constant common factor

By Monday,  $\exists!$  way to express  $h \in \mathbb{Q}[x]$

as  $h(x) = c \cdot h_0(x)$ ,  $c \in \mathbb{Q}$

$h_0$  primitive.

By assumption,  $h \nmid f \wedge h \nmid g$  in  $\mathbb{Q}[x]$ .

so  $h_0 \nmid f \wedge h_0 \nmid g$  in  $\mathbb{Q}[x] \xrightarrow{\text{ca}} h_0 \nmid f \wedge h_0 \nmid g$  in  $\mathbb{Z}[x]$

Thm. WTS:  $f(x)$  is irreducible  $\Rightarrow f$  is prim  $\wedge$   
 $f$  is irreducible in  $\mathbb{Q}[x]$

Assume  $\exists h, g \in \mathbb{Q}[x]$  s.t.  $f = h(x)g(x)$

$\exists!$  ways to express  $h \nmid g$  as  $h = c_1 h_0(x)$   $c_1, c_2 \in \mathbb{Q}$   
 $g = c_2 g_0(x)$   $h_0, g_0 = \text{prim poly}$

$$f = c_1 c_2 [h_0(x) g_0(x)] = 1 \cdot f$$

Prop: Let  $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ , let  $p = \text{prime} \#$ ,  
 Suppose  $p \nmid a_n$ . Then if  $\psi_p(f) = (a_n \bmod p)x^n + \dots + (a_0 \bmod p) \in \mathbb{Z}_{p\mathbb{Z}}[x]$   
 is irreducible in  $\mathbb{Z}_{p\mathbb{Z}}[x]$ , then  $f$  also is in  $\mathbb{Z}[x]$  (actually, even  
 in  $\mathbb{Q}[x]$ ).

Note: For any  $n$ ,  $\exists$   $\infty$  number of poly's in  $\mathbb{Q}[x]$  w/  $\deg \leq n$ .  
BUT,  $\exists$  finite # of poly's in  $\mathbb{Z}_{p\mathbb{Z}}[x]$  w/  $\deg \leq n$ .

Pf. Assume  $f$  is irreducible in  $\mathbb{Q}[x]$ .

i.e.  $\deg(g), \deg(h) > 0$

$\nexists f = gh$  q. g, h  $\in \mathbb{Q}[x]$ , By all of our hard work,

can assume  $g, h \in \mathbb{Z}[x]$

Note:  $\deg(f) = \deg(g) + \deg(h)$

$$\deg(\psi_p(g(x))) \leq \deg(g(x))$$

$$p \nmid a_n \Rightarrow \deg(\psi_p(f)) = \deg(f)$$

$$\psi_p \text{ is a ring hom } \Rightarrow \psi_p(f) = \psi_p(g) \psi_p(h)$$

$$\deg(\psi_p(g)) \leq \deg(g) > 0 \quad \nexists \deg(\psi_p(h)) \leq \deg(h) > 0$$

$$\nexists \deg(f) = \deg(\psi_p(f)) \quad \nexists \psi_p(f) = \psi_p(g) \psi_p(h)$$

$$\Rightarrow \deg(\psi_p(f)) = \deg(\psi_p(g)) + \deg(\psi_p(h))$$

$$\deg(f) >$$

Note. converse fails!

i.e.  $\exists$  irreducible  $f(x) \in \mathbb{Q}[x]$  that's reducible in  $\mathbb{Z}/p\mathbb{Z}[x]$

A list of reducibility test!

i)

rational root test

If  $\frac{a}{b} \in \mathbb{Q}$  is a root of  $f$  ( $\Rightarrow bx-a$  is a factor of  $f$ ). Then  $a|c_0 \wedge b|c_n$

ii)

Deg 2 or 3 test: If  $\deg f = 2$  or 3 then  $f$  reducible in  $\mathbb{Q}[x] \Rightarrow f$  has a root in  $\mathbb{Q}$   
(also works for  $\mathbb{Z}/p\mathbb{Z}$ )

iii)

integer test:  $f$  irreducible over  $\mathbb{Q} \Leftrightarrow$  over  $\mathbb{Z}$

iv)

mod  $p$  test.

$\psi_p(f) \in \mathbb{Z}/p\mathbb{Z}[x]$  irreducible over  $\mathbb{Z}/p\mathbb{Z}$   
 $\Rightarrow f$  irreducible in  $\mathbb{Z}$

v)

Eisenstein:

$p$  s.t.  $p \nmid c_n, p \mid c_{n-1}, \dots, c_1 \nmid p^2 \nmid c_0$

then  $f$  is irreducible

Nov 11

Pf

Eisenstein's criterion:

Assume  $f$  is reducible over  $\mathbb{Q}$

$\Rightarrow \exists g, h \in \mathbb{Z}[x]$  s.t.  $f = gh$

Let  $\bar{f} = \psi_p(f) = (a_0 \bmod p)x^n + \dots + (a_n \bmod p) \in \mathbb{Z}/p\mathbb{Z}[x]$

$p | a_0, \dots, a_{n-1} \Rightarrow \bar{f} = (a_n \bmod p)x^n = \bar{a}_n x^n$

$\psi_p$  is a ring hom  $\Rightarrow \bar{f} = \bar{g} \bar{h}$

$\mathbb{Z}/p\mathbb{Z}$  = field so if  $ck=0$ , one of  $c, k$  is 0

$$\bar{g} = c_g x^r \quad ; \quad \bar{h} = c_h x^s$$

$\downarrow$

constant term,  $g_0$  of  $g$ , has to be a multiple of  $p$

$\begin{matrix} g_0 h_0 = a_0 \\ \uparrow \uparrow \\ \text{a multiple of } p \end{matrix}$  is a multiple of  $p^2$

Def'n If  $K$  = field  $\nsubseteq F$   $K$  is a subfield

we say that  $K$  is a field extension of  $F$   
 $\nsubseteq$  we write  $K/F$

Def'n Suppose  $\alpha \in K$ ,  $K/F$ .  $\alpha$  is algebraic over  $F$

if  $\exists$  a monic poly  $f \in F[x]$  s.t.  $f(\alpha) = 0_K$

if  $\alpha$  is not alg. over  $F$ ,  $\alpha$  is called transcendental over  $F$

Lemma Given  $\alpha \in K$ ,  $K/F$ ,  $\alpha$  is algebraic over  $F$

$\Leftrightarrow \psi_\alpha : F[x] \rightarrow K$  is not one-to-one

where  $\psi_\alpha(p(x)) = p(\alpha)$

Pf:  $\psi_\alpha$  not one-to-one  $\Leftrightarrow \ker(\psi_\alpha) \neq \{0\} \Leftrightarrow \exists f \in F[x]$   
s.t.  $\psi_\alpha(f) = 0$

so suppose  $\alpha \in K$  is algebraic over  $F$

$F[x] = \text{PID}$  (principal ideal domain)

$$\ker(\varphi_\alpha) = (f(x_1)), \quad f \in F[x]$$

Proposition

assume  $\alpha \in K$  algebraic over  $F$

Then TFAE for a given monic poly  $f \in F[x]$ :

- i)  $f$  = monic poly of smallest deg in  $F[x]$  s.t.  $f(\alpha) = 0$
- ii)  $f$  is irreducible in  $F[x]$  &  $f(\alpha) = 0$
- iii)  $(f(x_1)) = \ker(\varphi_\alpha)$  &  $(f(x_1))$  is maximal
- iv)  $f(\alpha) = 0$  & if  $g \in F[x]$  s.t.  $g(\alpha) = 0 \Rightarrow f | g$

(i)  $\Rightarrow$  (ii) :

suppose  $f$  = monic poly of smallest deg s.t.  $f(\alpha) = 0$

suppose  $f = gh$ ,  $g, h \in F[x]$ .  $f(\alpha) = 0 \Rightarrow g(\alpha)h(\alpha) = 0$

$$\Rightarrow g(\alpha) = 0 \text{ or } h(\alpha) = 0$$

$$f = gh \Rightarrow \deg(f) = \deg(g) + \deg(h)$$

$\Rightarrow$  if either  $\deg(g)$  or  $\deg(h) >$

both  $\deg(g)$  &  $\deg(h)$  is  $< \deg(f)$

$\Downarrow$   
contradicts  $f$  is smallest

(ii)  $\Rightarrow$  (iii) Assume  $f(\alpha) = 0$  &  $f$  is irreducible over  $F$

WTS  $(f(x_1))$  is maximal in  $F[x]$ .

If not,  $\exists$  ideal  $I$  in  $F[x]$  s.t.  $(f(x_1)) \subsetneq I \subsetneq F[x]$

$$(f) \subset (g) \Rightarrow f \in (g) \Rightarrow \exists r \text{ s.t. } f = rg$$

$$\text{if } \deg(r) = 0, r = \text{unit} \quad \text{if } g = r^{-1} \cdot f \Rightarrow g \in (f)$$

$g = f$   
contrad

Nov 30

## Field extension

irreducible monic poly  $f(x)$  w/ root in  $F$

imagine "adjoining" an abstract element  $\alpha$ , s.t.  $f(\alpha) = 0$

then  $F(\alpha)$  is the smallest field containing both  $F$  &  $\alpha$

$F(\alpha) \supseteq K$  would be a field extension of  $F$

last time Given  $K/F$ ,  $\alpha \in K$

suppose  $\alpha$  = algebraic over  $F$

i.e.  $\exists f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in F[x]$  s.t.  $f(\alpha) = 0$

Then  $\exists$  a poly.,  $g(x)$  s.t.

i)  $g$  = monic poly of smallest deg w/  $g \in F[x]$

i.e.  $g(\alpha) = 0$

ii)  $g$  is irreducible over  $F$

iii)  $(g(x))$  = ideal generated by  $g$  in  $F[x]$ , is maximal

iv) if  $f(\alpha) = 0$ , then  $g \mid f$

$g$  is the irredu. poly for  $\alpha$  over  $F$

degree of  $\alpha$  is the deg of  $g$

$F(\alpha) \subseteq K$

"smallest sub-field of  $K$  containing  $F \cup \alpha$

$\varphi_\alpha : F[x] \rightarrow K$

$p(x) \mapsto p(\alpha)$

$\text{Im}(\varphi_\alpha) = \{x \in K \mid x = b_n \alpha^n + b_{n-1} \alpha^{n-1} + \dots + b_0\}$

$F[\alpha] = \text{ring! (integral domain!)$

$F = \text{field so } F[x]$  is an integral domain

$F[\alpha] \cong F[x]/(f)$

$F(\alpha)$  is just a field of fractions of  $F[\alpha]$ ?

Prop Let  $\alpha \in K$ ,  $K/F$ ,  $\alpha = \text{alg. over } F \setminus f(\alpha) = \text{irreducible}$   
 poly for  $\alpha$  over  $F$ . Then consider:

$$\psi: \frac{F[x]}{(f)} \rightarrow F[\alpha] \text{ given by}$$

$$\psi(p(x) + (f)) = p(\alpha)$$

Then  $\psi_\alpha$  is an iso

so  $F[\alpha]$  is actually a field

because  $(f)$  is maximal

$\Rightarrow F[x]/(f)$  is a field

$$F[\alpha] = F[\alpha]$$

not true when  $F \neq \text{field}$

Pf

$(f)$  maximal  $\Rightarrow F[x]/(f)$  is a field

consider  $\phi_\alpha: F[x] \rightarrow K$   
 $p(x) \mapsto p(\alpha)$

$\phi_\alpha$  is onto

isomo then  $\Rightarrow \frac{F[x]}{\ker(\phi_\alpha)} \cong F[\alpha]$

$$\ker(\phi_\alpha) = (f)$$

$$F[x] \xrightarrow{\phi_\alpha} F[\alpha]$$

$$\pi \downarrow_{\frac{F[x]}{(f)}} \quad \uparrow \exists \psi, \text{ an iso}$$

$$\psi(p(x) + (f)) = \phi_\alpha(p) \Rightarrow \psi = \phi_\alpha$$

Does this make sense?

$$\text{if } p(x) + (f) = q(x) + (f)$$

$$p + (f) = q + (f)$$

$$\Rightarrow p - q \in (f)$$

$$\Rightarrow p - q = g(x)f(x)$$

$$\Rightarrow (p - q)(\alpha) = g(\alpha)f(\alpha) = 0$$

$$p(\alpha) = q(\alpha)$$

From 11.5.1 in Artin

$F[\alpha]$  is a vector space over  $\mathbb{F}$

$(1, \alpha, \dots, \alpha^{n-1})$  is a basis for  $F[\alpha]$  over  $\mathbb{F}$

$$n = \deg(f)$$

$\Rightarrow F[\alpha]$  is a vector space over  $\mathbb{F}$  of dimension =  $\deg(\alpha)$

Dec 2

Def'n Given  $K/F$ , the degree of  $K$  over  $F$ ,  $\deg_F K$ ,  
is  $\dim_F(K) = \dim_K F$  as a  $F$ -vector space

$\deg_F K = 2$   $K/F$  is called a quadratic extension

$= 3$  - - - cubic extension

Prop If  $\alpha \in K$ ,  $K/F$ ,  $\alpha = \text{alg. over } F$

Then  $[F(\alpha):F] = \deg \text{ of irred poly for } \alpha \text{ over } F$

Lemma i)  $K/F$  has degree 1  $\Rightarrow K = F$

ii)  $\alpha \in K$  has degree 1 over  $F \Leftrightarrow \alpha \in F$

If  $\dim_F K = 1$ , any non zero element of  $K$  is a basis

so  $1 \in K$  is a basis. so all of  $K$  is of the form  $(\text{sth in } F) \cdot \underbrace{1}_{\in F}$

If  $F = K \Rightarrow \{1\}$  is a basis for  $K$  over  $F \Rightarrow \deg_F K = 1$

ii) w.l.o.g  $\alpha \in K$  has deg 1 over  $F \Leftrightarrow \alpha \in F$

$\deg \alpha \text{ over } F = \deg \text{ of irred poly for } \alpha \text{ over } F$

$\alpha$  has deg 1  $\Leftrightarrow$  this poly is  $x - \alpha \Rightarrow \alpha \in F$

If  $\alpha \notin F$ , then  $x - \alpha$  is the irred poly for  $\alpha$  over  $F$

Prop Assume characteristic( $F$ )  $\neq 2$ , i.e.  $1+1 \neq 0$ .

Then any quadratic extension  $K$  over  $F$  can be obtained

by adjoining a square root, i.e.  $K = F(S)$ , where  $S^2 = \alpha, \forall \alpha \in F$

Then  $F(S)$  is a quadratic extension

Pf

Let  $\alpha \in K$ ,  $\alpha \notin F$ , where  $K = \text{quadratic extension of } F$

claim:  $(1, \alpha)$  is linearly independent over  $F$

$\exists \gamma_1, \gamma_2 \in F$  s.t.  $\gamma_1 \cdot 1 + \gamma_2 \alpha = 0$

$\Rightarrow \gamma_2 \cdot 1 = -\gamma_1$ . If  $\gamma_2 = 0 \Rightarrow 0 = -\gamma_1 \Rightarrow \gamma_1 = 0$

$\Rightarrow \gamma_2 \neq 0$ ,  $\gamma_2 \in F \Rightarrow \gamma_2^{-1} = F \Rightarrow \alpha = -\gamma_2^{-1} \gamma_1$

$[K:F]=2 \Rightarrow (1, \alpha)$  is a basis!

$\Rightarrow \alpha^2$  has to be a linear combo of  $(1, \alpha)$

so  $\exists b, c \in F$  s.t.  $\alpha^2 = b\alpha + c \Rightarrow \alpha$  is a root of  $f(x) = x^2 - bx - c$

$\alpha \notin F \Rightarrow f$  is irreducible over  $F$

Quadratic formula:  $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$  solves  $ax^2 + bx + c = 0$

This works over any field so long as  $2 \neq 0$

set  $s = \pm \sqrt{b^2 - 4ac}$ , claim:  $s \in K$

# Dec 4

Recap: If  $\text{char}(F) \neq 2$ , i.e.  $1+1 \neq 0 \nmid$  if  $K/F$  is a quadratic

field extension then  $\exists s \in K, s \notin F$  b/w  $s^2 \in F \setminus \{F(s)\}$

1) pick some  $\alpha \in K$ ,  $\alpha \notin F$  ( $\alpha$  exists because  $K=F \Leftrightarrow [K:F]=1$ )

2)  $(1, \alpha)$  is linearly independent, i.e. if  $x_1, x_2 \in F$ ,

$$\text{then } x_1 \cdot 1 + x_2 \cdot \alpha = 0$$

$$\Rightarrow x_1 = x_2 = 0$$

b) Given  $f(x) = ax^2 + bx + c$ , where  $f \in F[x]$ .

so long as  $\text{char}(F) \neq 2, a \cdot (1+1)^{-1} \cdot (-b \pm \sqrt{b^2 - 4ac})$

solves  $f(x)=0$

c) In our situation,  $f(x) = x^2 - bx - c$

claim:  $\exists s \in K$  s.t.  $s^2 = b^2 - 4c$

d)  $s = 2\alpha - b$  satisfies  $s^2 = b^2 + 4c$

claim:  $s \in F(\alpha)$

similarly //  $\alpha \in F(s)$  (because  $\alpha = 2^{-1} \cdot (s + b)$ )

$F(\alpha) \subseteq F(s)$

$F(s) \subseteq F(\alpha) \Rightarrow F(\alpha) = F(s)$

However,  $F(\alpha) = K$ , since it's a 2 diml subspace  
of  $K$ , which is itself only 2 diml  
 $\Rightarrow F(s) = K$

Thm  $F \subset K \subset L$  fields

$$\text{Then } [L:F] = [L:K][K:F]$$

Pf. Let  $B = (\beta_1, \dots, \beta_n)$  = basis for  $L$  as a  $K$ -vector space  
and let  $A = (d_1, \dots, d_m)$  = basis for  $K$  as an  $F$ -vector space.

We'll show  $\{d_i \beta_j\}_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$  is a basis for  $L$  as an  $F$ -vector space

1)  $\{d_i \beta_j\}$  is a spanning set for  $L$  over  $F$

2)  $\{d_i \beta_j\}$  are linearly independent over  $F$

(1)  $\{d_i \beta_j\}$  is a spanning set for  $L$  over  $F$

Let  $y \in L$ . Since  $(\beta_1, \dots, \beta_n)$  spans  $L$  as a  $K$ -vector space,  $\exists b_1, \dots, b_n \in K$  s.t.  $y = b_1 \beta_1 + \dots + b_n \beta_n$ . Since  $K = F$ -v.s.,  $\exists$ , for each  $i$ ,  $\exists a_{i,1}, \dots, a_{i,m} \in F$  s.t.  $b_i = a_{i,1} d_1 + \dots + a_{i,m} d_m$ .

$$\begin{aligned} \Rightarrow y &= (a_{1,1} d_1 + \dots + a_{1,m} d_m) \beta_1 + \dots + (a_{n,1} d_1 + \dots + a_{n,m} d_m) \beta_n \\ &= \sum_{i,j} a_{i,j} d_i \beta_j \end{aligned}$$

(2)  $\{d_i \beta_j\}$  are linearly independent over  $F$ .

Assume  $\exists$  a linear combo  $\sum_{i,j} a_{i,j} d_i \beta_j = 0$ . WTS:  $a_{i,j} = 0 \forall i, \forall j$ .  
Since  $\beta_j$  is linearly ind. over  $K$ , for each  $j$ ,  $\sum_i a_{i,j} d_i = 0$ .

Since  $L$  lin. ind. over  $F$ ,

$$a_{i,i} = 0 \forall i$$

Dec 7

consequences from last time

- a)  $F \subset K$ ,  $K/F$  is a finite extension of deg  $n$   
 $\nexists \alpha \in K$ . Then  $\alpha$  is algebraic over  $F$ .  $\nexists \deg(\alpha) | n$

$$\deg(\alpha) = [F(\alpha) : F]$$

$$[K : F] = n = [K : F(\alpha)] [F(\alpha) : F]$$

- b)  $F \subset F' \subset L$   $\nexists \alpha \in L$  algebraic over  $F$ .

Then  $\alpha$  is also algebraic over  $F'$

If  $\deg_{F'}(\alpha) = d$ , then  $\deg_{F'}(\alpha) \leq d$

$\alpha$  is a root of  $f \in F[x] \Rightarrow f$  is a multiple  
of whatever the irred. poly  $(g)$  is for  $\alpha$  in  $F'[x]$

$\Rightarrow f = g(x)h(x)$  for some  $h \in F[x] \Rightarrow \deg$

$\Rightarrow \deg(g) \leq \deg(f)$

- c) If  $K = F(\alpha_1, \dots, \alpha_n)$ ,  $\alpha_1, \dots, \alpha_n$  alg. over  $F$

then  $[K : F] < \infty$

$$= [K : F_{n-1}] [F_{n-1} : F_{n-2}] \cdots [F_1 : F]$$

- d) If  $K/F$ , then alg. elements in  $K/F$  form a subfield

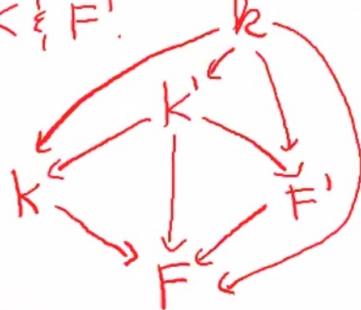
WTS:  $\alpha, \beta \in K$  alg. over  $F$ , then  $\alpha + \beta \nexists \alpha\beta$  is also  
alg. over  $F$ .

$\alpha + \beta \nexists \alpha\beta$  are both elements of  $F(\alpha, \beta)$

since  $[F(\alpha, \beta) : F] < \infty$  by c)

by (a) any element in a finite extension over  $F$  is alg. over  $F$

Lemma: Let  $K$  = extension of  $F$ ,  $\nsubseteq$  let  $K \nsubseteq F' \subset K$ , both finite extensions of  $F$ . Let  $K'$  = subfield of  $K$  generated by  $K \setminus F'$ .



$$[K':F] = N, [K:F] = m$$

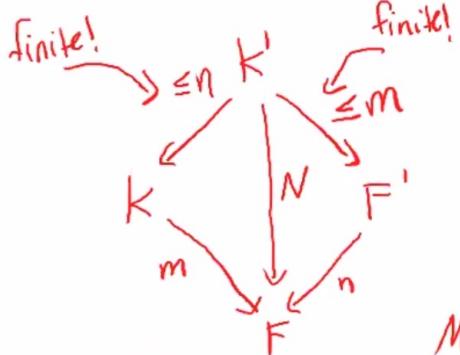
$$[F':F] = n. \text{ Then}$$

$$m, n \mid N, \nmid N \leq nm, \nmid$$

if  $\gcd(m, n) = 1$ , then  $N = nm$ .

pf of lemma:

The green consequences  $\Rightarrow$  any finite extension is generated by a finite # of alg. elements.



$K'/K$  is a finite extension, because

$K' =$  field generated by 2 finite extensions over  $F \Rightarrow K'/F$  is finite  $\Rightarrow$

$K'/K$  is finite. Similarly,  $K'/F'$  finite as well.

Multiplicative formula  $\Rightarrow$

$$N = [K':F] = [K':K][K:F] = [K':K] \cdot m$$

$$\Rightarrow m \mid N. \text{ Similarly, } n \mid N.$$

Now, suppose  $F'$  is generated by one element,  $\beta$ , over  $F$ , i.e.,  $F' = F(\beta)$ .

Then  $K' = K(\beta)$ . Why? Well,  $K = F(\text{some stuff})$ ,  $F' = F(\beta)$ .

$$K' = F(\text{some stuff}, \beta) = K(\beta).$$

in sequence, b)  $\Rightarrow \deg_K \beta = [K':K] \leq \deg_F \beta = n$   
 $\Rightarrow N \leq nm$

argument  $\Rightarrow [K':F]$  is divisible by  $\text{lcm}(m, n)$

which if  $\gcd(m, n) = 1$ , is  $mn$

Dec 9

Lemma:

(a)  $\gamma$  is a root of  $f \in F[x] \Leftrightarrow$  the coeffs of  $f$  yield a linear dependence for powers of  $\gamma$ . i.e.,

$$f(x) = a_n x^n + \dots + a_0, \quad f(\gamma) = 0 \Leftrightarrow \underbrace{a_n \gamma^n + \dots + a_1 \gamma + a_0}_\text{a linear dependence} = 0$$

(b) Suppose  $\alpha, \beta$  alg. over  $F$ ;  $\deg_F(\alpha) = d_1, \deg_F(\beta) = d_2$ .

Then the  $d_1 d_2$  monomials  $\alpha^i \beta^j$  ( $1 \leq i \leq d_1, 1 \leq j \leq d_2$ ) span

$F(\alpha, \beta)$

as an  $F$ -vector space.

Lemma  $\Rightarrow$  we can always find a poly which has  $\alpha + \beta$  as a root, once we have irred. poly's for  $\alpha \notin \beta$ .

How? Given the minimal poly's for  $\alpha \notin \beta$ , we have their degrees. So let  $\deg \alpha = d_1, \deg \beta = d_2$ . Given

$\gamma \in F(\alpha, \beta)$ , (b)  $\Rightarrow$  you can express each of

(e.g.,  $\gamma = \alpha + \beta$ )  $1, \gamma, \gamma^2, \dots, \gamma^n$  as linear combo's

of  $\{\alpha^i \beta^j\}_{\substack{1 \leq i \leq d_1 \\ 1 \leq j \leq d_2}}$ . So, when  $n = d_1 d_2$ ,

we have more vectors than elements in the spanning set.

Note: we always have

$$\tilde{\pi}: \mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$$

$$\xrightarrow{\deg f > 0} (x^2 + 1)$$

This means  $\mathbb{Q}$  can be considered as a subfield of  $\mathbb{Q}[x]/(x^2 + 1)$

Claim:  $F = \text{field}, I = (f(x))$  in  $F[x]$ , then

$$\tilde{\pi}: F[x] \rightarrow F[x] \xrightarrow{(f(x))} \text{is 1-1 WHEN we restrict to constants.}$$

i.e., if  $a_1, a_2 \in F$ , then  $a_1 \neq a_2 \Rightarrow \tilde{\pi}(a_1) \neq \tilde{\pi}(a_2)$

If  $\tilde{\pi}(a_1) = \tilde{\pi}(a_2)$ ,  $a_1 + (f) = a_2 + (f) \Leftrightarrow a_1 - a_2 \in (f)$

$\Rightarrow (f) = F[x] \Leftrightarrow f$  is itself a constant.

Dec 11

Lemma

$F = \text{field}$ ,  $f(x) \in F[x]$  irreducible over  $F$

Then in the field  $K = F[x]/(f(x))$

$[\pi(x)]$  is a root of  $f(x)$

$$\pi: F[x] \rightarrow F[x]/(f(x)) = K$$

$$x \mapsto x + (f(x)) = \pi(x)$$

Suppose  $f(x) = a_n x^n + \dots + a_0$   $a_i \in F$

$$(a_n + (f)) (x + (f))^n + (a_{n-1} + (f)) (x + (f))^{n-1}$$

$$+ \dots + (a_0 + (f)) = \underbrace{0}_{(f)} \in K$$

$F[x]/(f(x))$  has an element that is a root of  $f(x)$

Definition

$F = \text{field}$ , a poly  $f \in F[x]$  splits completely

over some field extension  $K$  if  $f$  factors  
into linear pieces w/ coeff in  $K$

Lemma  $F = \text{field}$ ,  $f = \text{monic poly in } F[x]$ ,  $\deg(f) > 0$ ,

Then  $\exists$  a field extension  $K$  in which  $f$   
splits completely

## Finite Fields

Let  $p = \text{prim}$ . Let  $r \in \mathbb{N}$ ,  $q = p^r$

- a)  $\exists$  a field of order  $q$ . Any 2 fields of order  $q$  are isomorphic.
- b) If  $F = \text{finite field}$ ,  $|F| = q$  for some  $p, r$ .
- c) If  $|F| = q$ , then every element is a root of  $x^q - x$
- d) The irreducible factors of  $x^q - x$  in  $\mathbb{Z}/p\mathbb{Z}$  are exactly the irreducible polys of  $F[x]$ ,  $|F| = p^r$  satisfying property that their degree divides  $r$
- e) Let  $F^\times = gp$  of multi units in  $F$   
 $= gp$  of order  $q-1$   
It's a cyclic gp.
- f)  $F = \text{finite field}$ ,  $|F| = p^r$   
then  $F$  contains a subfield of size  $p^k$   
 $\Leftrightarrow k | r$

If  $\exists$  a field  $K$  of size  $p^r = q$

then  $\exists \alpha \in K, \alpha^q - \alpha = 0$

If such a  $K$  exists,  $|K^\times| = q-1$ .

so given  $\alpha \in K$ ,

Lagrange's thm  $\Rightarrow$  order of  $\alpha$

= smallest int  $n$  s.t.  $\alpha^n = 1$

has to divide  $q-1$

$$\Rightarrow q-1 = mn, m \in \mathbb{Z}$$

$$\therefore \alpha^{q-1} = \alpha^{mn} = (\alpha^n)^m = 1$$

$$\Rightarrow \alpha^{q-1} - 1 = 0 \xrightarrow[\text{by } \alpha]{\text{multiply}}$$

Why does  $K$  exist??

Idea: If  $K$  exists, by (c), we know its elements are roots of  $x^q - x$ . By all of our work on abstract field extensions,  $\exists$  a field extension  $L$  of

$\mathbb{Z}/p\mathbb{Z}$  in which  $x^q - x$  splits completely. So all of the roots of  $x^q - x$  live in  $L$ .

15.7.11 ← Lemma: These roots (there are  $q$  of them) form a subfield of  $L$ .

