Def'n Let S = set, a $\boxed{\text{binary operation}}$ on S is a function $f: \underbrace{S \times S}_{\text{domain}} \to \underbrace{S}_{\text{co-domain}}$

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

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

Def'n A binary operation $f: S \times S \to S$ is $\boxed{\text{associative}}$ if $\forall a,b,c \in S$, $f(f(a,b),c) = f(a, f(b,c))$

in new notation: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

allows us to be less careful when writing down long "products"

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

$f(A,B) = A \cdot B$ ← matrix multiplication, which is associative

key fact: composition of functions transformations is associative

Def'n A binary operation is $\boxed{\text{commutative}}$ if $\forall a,b \in S$, $a \cdot b = b \cdot a$

ex's) $(\mathbb{R}, +)$ - real number addition

Def'n Given S equipped w/ a binary operation, $\cdot$, we say $(S, \cdot)$ has an $\boxed{\text{identity element}}$ if $\exists e \in S$ s.t. $\forall a \in S$, $a \cdot e = a = e \cdot a$ → doesn't change identity

Def'n An element a of $(S, \cdot)$ is called $\boxed{\text{invertible}}$ (w/ e = identity) if $\exists b \in S$ s.t. $ab = e = ba$

Def'n A $\boxed{\text{group}}$ is a set $(G, \cdot)$ w/ a binary operation s.t.

! closure under operation

i) it's associative

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

iii) every element in G is invertible

If $\cdot$ is commutative, G is called $\boxed{\text{an abelian group}}$

ex's) $G = \left\{ \begin{array}{l} \text{bijections } T: \mathbb{R}^2 \to \mathbb{R}^2 \text{ so that } T(\text{standard unit square} = \mathcal{S}_1) = \mathcal{S}_1 \\ \text{binary operation: composition} \end{array} \right\}$

another name: D_8

Thm: D_8 contains exactly 8 elements

Proof?

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

then φ can be expressed as a finite composition $\varphi_1 \circ \varphi_2 \circ \varphi_3 \cdots$

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

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

Def'n A $\boxed{\text{subgroup}}$ H of a group $(G, \cdot)$ is a subset of G which is also a group with respect to $\cdot$

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

$\Leftrightarrow$ 1) $\forall h_1, h_2 \in H$, $h_1 \cdot h_2 \in H$ closure

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

Def'n Given $\{1,2,3,\dots,n\}$ for some $n \in \mathbb{N}$,
define $S_n = \left(\{\text{bijections } \tau : \{1,2,3,\dots,n\} \to \{1,\dots,n\}\}, \text{composition}\right)$

Fact S_n is a group, called the "$\boxed{\text{symmetric group on } n \text{ elements}}$"

Terminology elements of S_n are called $\boxed{\text{permutations}}$

ex 1 say $n=5$, the τ : $\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 2 & 4 & 1 & 3 \end{matrix}$

$\tau = \underbrace{(1\ 5\ 3\ 4)}(2)$ ⇐ "cycle notation"

1 to 5, 5 to 3, 3 to 4, 4 to 1 and 2 to itself

caution cycle notation is not unique!

inverse $\underbrace{((1\ 5\ 3\ 4)(2))}_{\tau}\underbrace{((1\ 4\ 3\ 5)(2))}_{\tau^{-1}} = \underbrace{(1)(2)(3)(4)(5)}_{\text{identity}}$

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

exs $\tau \in S_4$, $\tau = (1\ 3\ 4)$

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

ex 1

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

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

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 $\boxed{\text{sign}}$ of τ is the sign of $\det(M_\tau)$

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

Def'n $\boxed{\text{greatest common divider}}$: $\gcd(a,b)$

ex 1 Euclidean algorithm: $\gcd(314, 136)$

Def'n Given $a, b \in \mathbb{Z}$, $a, b \neq 0$, a & b are $\boxed{\text{relatively prime}}$ if $\gcd(a,b) = 1$

Fact $\gcd(a,b)$ = product of prime powers common to prime factorizations of a & b

corollary: a & b are relatively prime $\Leftrightarrow \gcd(a,b) = 1 \Leftrightarrow a\mathbb{Z} + b\mathbb{Z} = 1$

$ra + sb = 1$

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

Thm If $S \subseteq \mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$
then either $S =$ 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 $S =$ trivial subgroup
Otherwise, $\exists n \in \mathbb{Z}, n \neq 0$ & $n \in S$, $n \in S \Rightarrow -n \in S$ 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 $k \cdot a = a + a + \cdots + a$ 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
$\Rightarrow a\mathbb{Z} \subseteq S$

intuition: a is the smallest component

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, $n \in S \Rightarrow n - qa \in S \Rightarrow r \in$
$\Rightarrow r = 0$ because a is the minimum +
$\Rightarrow n = qa$
$\Rightarrow S \subseteq a\mathbb{Z}$ □

Thm Let $G = (G, \cdot)$ a group & let $I =$ set & let $\{H_i\}_{i \in I}$ be a family of subgroups of G indexed by I. Then $\bigcap_{i \in I} H_i$ is a subgroup

$\bigcap_{i \in I} H_i = \{h \in G \mid h \in H_i \ \forall i\}$

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

Def'n Given $a\mathbb{Z}$ & $b\mathbb{Z}$, consider $S = a\mathbb{Z} \cap b\mathbb{Z}$. S is a subgrp & it's a form of $m\mathbb{Z}$, for some m : $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. so $m \in a\mathbb{Z}$ & $m \in b\mathbb{Z}$
$\Rightarrow m$ is a multiple of a & b. m is called $\boxed{\text{least common multiple}}$

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

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

$\Rightarrow$ intersection

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

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

$x \in H \Rightarrow x^2, \ldots, x^{\cdots} \in H$ since H is a subgroup

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

$e \in H$ as well

so $\{\ldots, x^2, x^{-1}, e, x, x^2 \ldots\} = \langle x \rangle \leq H$

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

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

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 $\langle x \rangle \in P(x)$ & $g \notin \langle x \rangle$

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

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

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

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

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

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

$x^k = e \Rightarrow x^{-k} = e^{-1} = e \Rightarrow -k \in S_x$

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

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

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. $x^{\text{that number}} = e$

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

$x^n x = ex = x$

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

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

Def'n A $\boxed{\text{homomorphism}}$ is a function $\varphi : (G, \cdot) \to (G', \cdot)$
$\forall g_1, g_2 \in G,$
$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

general ex's
i) If G, G' are any groups, let e' denote identity element of G'.
Then $\varphi : G \to G'$ is a homomorphism, the "trivial homomorphism"
$$\varphi(g_1 g_2) = e' = e'e' = \varphi(g_1)\varphi(g_2)$$

ii) If H = subgp of G, then $i : H \to G$, $h \to h$ a homomorphism, called "inclusion"

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

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

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

① $\operatorname{im}\varphi \neq \phi$ cuz $e' \in \operatorname{im}\varphi$ since $\varphi(e) = e'$

② Suppose $a_1', a_2' \in G'$ in $\operatorname{im}\varphi \Rightarrow \exists a_1, a_2 \in G$ s.t. $\varphi(a_1) = a_1'$, $\varphi(a_2) = a_2'$
$a_1 a_2 \in G$ & $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2) = a_1' a_2' \in \operatorname{im}\varphi$

③ $a' \in \operatorname{im}\varphi \Rightarrow \exists a \in G$ s.t. $\varphi(a) = a'$
$\varphi(a^{-1}) = (\varphi(a))^{-1} = (a')^{-1} = a'^{-1} \in \operatorname{im}\varphi$

Def'n A homomorphism $: G \to G'$ is called an $\boxed{\text{isomorphism}}$ if it's a bijection

i.e. $\mathrm{Im}\varphi = G'$.

lemma φ is one to one $\Leftrightarrow$ $\ker\varphi = \{e\}$

$\Rightarrow$ an isomorphism $\varphi: G \to G'$ is a hom st. $\ker\varphi = \{e\}$ & $\mathrm{im}\,\varphi = G'$

ex.s1 conjugation:

Let G = group. $g \in G$. $\varphi_g : G \to G$

define $\varphi_g(a) = gag^{-1}$ = "the $\boxed{\text{conjugate}}$ of a by g"

claim. φ_g is an isomorphism!

1) φ_g is a hom: Given $a, b \in G$, $\varphi_g(ab) = gabg^{-1} = ga(g^{-1}g)bg^{-1}$

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

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) $\mathrm{im}\varphi = G$

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

$shg^{-1} \in H$

Def'n A subgp H of a group G is called $\boxed{\text{normal}}$ if $\forall g \in G$, $\varphi_g(H) = H$

Def'n Given a set S, an $\boxed{\text{equivalence rel'n}}$ is a subset, E, of $S \times S$, satisfying:

i) $\forall x \in S$, $(x,x) \in H$

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

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

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

Def'n Given a set S & $x \in S$, & an equivalence rel'n $\sim$, the $\boxed{\text{equivalence class}}$ of X, denoted $[x]$, is $[x] = \{y \in S \mid x \sim y\}$

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

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

Def'n G = group, H = subgroup of G, $a \in G$
The $\boxed{\text{right coset}}$ of H with respect to a is
$Ha = \{g \in G \mid \exists\, h \in H \text{ s.t. } ha = g\}$

Lemma 1) $Ha = Hb \iff ab^{-1} \in H$

Lemma 2) Given G, H = subgp. the rel'n defined by $a \sim b \iff ab^{-1} \in H$ is an equiv rel'n.
The equi class of the equival rel'n are the right cosets of H.

3) The equivalence class of $\sim$ are the right cosets of H
i.e. given $g \in G$ $[g] = \{a \in G \mid g \sim a\} = Hg$

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

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

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

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

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

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

$h_1 a = h_2 a \Rightarrow h_1 = h_2$

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

Lagrange Theorem If G is a finite group, H a subgp of G, then $|H| \mid |G|$

Pf The right cosets of H share no elements in common

& They cover all of G

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

so $|G| = (\underbrace{\text{\# of right cosets of } H}_{\text{notation } [G:H]}) \cdot (|H|)$

$[G:H]$ " "index of H in G"

Corollary If $a \in G$, then order$(a) \mid |G|$

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

A subgroup H in G is called normal if $\forall g \in G$, $\varphi_g(H) \subset H$ $\quad H \lhd G$

Preposition: If $\varphi : G \to G'$ a hom, then $\ker \varphi \lhd G$

Pf WTS: Given $a \in \ker\varphi$ & $g \in G$, $\underbrace{\varphi_g(a)}_{gag^{-1}} \in \ker\varphi$

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

Thm (The following are equivalent)

i) $H \lhd G$

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) ⇒ (ii) $\varphi_g(H) \subset H$ is trivial

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

$\forall h \in H, \exists h' \in H$ 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 = finite dim vector spaces, $T: V \to W$ linear
$\dim(V) = \dim(\ker T) + \dim(\mathrm{Range}(T))$

Goal: Do sth similar for groups! i.e.

linear	group
v, w = vector spaces	G, G' = groups
$T: v \to w$ linear	$\varphi: G \to G'$ a homomorphism
$\ker(T)$	$\ker(\varphi)$ i.e. normal subgp

intuition:
→ understand G as being a stack of pancakes (subgps ($\ker(\varphi)$))
G' = collapse pancakes to some point

Thm A subgp H of G is normal
$\Leftrightarrow \exists$ a group G' & a hom $\varphi: G \to G'$ s.t. $H = \ker(\varphi)$

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

Let G/H "G mod H" = {right cosets of H in G}

Fact $\exists$ a binary operation on G/H turning it into a group
& this will be our G'
& $\exists \varphi\ G \to G/H$ [$(g \mapsto Hg)$] ⇒ we defined φ as this considering its domain & co-domain

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

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

$Ha = Hb \Leftrightarrow ab^{-1} \in H$
so $Hg = H \Leftrightarrow g \in H$
$\ker(\varphi) = H$

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

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

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

$HHab \subset Hab$ since H is closed

if $g \in Hab \Rightarrow g = h \cdot e \cdot a \cdot b \Rightarrow g \in HHab$
$\Rightarrow HHab = Hab$

To Summarize:

Given $S \subseteq V$, (S = Subspace of V) $\exists$ a decomposition of V into parallel copies of S & $\exists$ a V.S. W & a linear map, $T: V \to W$ 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 & $\exists$ a group G' & a homomorphism $\varphi: G \to G'$ so that φ collapses the right coset of H to a point & $\ker(\varphi) = H$.

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

Lemma Given $H \triangleleft G$, if $Ha = Ha'$ & $Hb = Hb'$ then $Hab = Ha'b'$

WTS: $ab(a'b')^{-1} \in H$

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

Pf: WTS $ab(a'b')^{-1} \in H$

$$\begin{aligned} ab(a'b')^{-1} &= \underbrace{ab(b')^{-1}}(a')^{-1}. \quad Hb = Hb' \Rightarrow b(b')^{-1} = h \in H. \\ &= ah(a')^{-1}. \quad ah \in aH \underset{H \triangleleft G}{=} Ha \end{aligned}$$

$\Rightarrow \exists\, h' \in H$ s.t. $ah = h'a$.

$\Rightarrow ah(a')^{-1} = \underbrace{h'a(a')^{-1}}_{h'h''} \in H.$ $\quad Ha = Ha' \Rightarrow a(a')^{-1} = h'' \in H.$

$Ha = Ha'$

So far, we have that G' has a binary op'n.

$\varphi: G \to G'$
$g \mapsto Hg$

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

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

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

Lemma If G is group, Y = set with binary operation & $\varphi: G \to Y$ s.t. φ has the hom property (Y is not a group) & suppose φ is onto. Then Y is a group & φ is a hom

Pf Associativity: Given $a, b, c \in Y$, φ onto $\Rightarrow \exists a', b', c' \in G$ s.t. $\varphi(a') = a$, $\varphi(b') = b$, $\varphi(c') = c$.

φ is hom

So, $(ab)c = (\varphi(a')\varphi(b'))\varphi(c') = \varphi((a'b'))\varphi(c') = \varphi((a'b')c')$

G is gp

$= \varphi(a'(b'c')) = \varphi(a')(\varphi(b')\varphi(c')) = \varphi(a')(bc) = a(bc)$

10.5

Given a normal subgp $H \triangleleft G$,
to construct a onto hom $\varphi: G \to G'$ for some other gp G' s.t.

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

ii) $\varphi: G \to G/H$ 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 φ.

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

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

1st isomo theorem — Given $\varphi: G \to G'$ an onto hom, let $\ker\varphi = N$, Then G/N is isomophic to G'.

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

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

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G' \\ G/N \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

the order of doing things doesn't matter

Pf

Start with $\varphi : G \to G'$ an onto hom. Define $\bar{\varphi} : G/N \to G'$ ker
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 x2

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

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

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

N is normal → kernel of any hom is always a subgp

i) $\bar{\varphi}$ is a hom: $\bar{\varphi}(Ng_1, Ng_2) = \bar{\varphi}(Ng_1 g_2)$

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

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

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

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

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

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 $\varphi(g) = \bar{\varphi}(\pi(g))$.

$\pi(g) = Ng$ &

For uniquesness, ψ satisfies, $\psi : G/N \to G'$, an iso,

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

$$
\begin{tikzcd}
g \in G \arrow[r, "\varphi"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowright"] & G' \\
Ng \quad G/N \arrow[ur, "\psi"'] &
\end{tikzcd}
$$

for this to work ψ has to send the coset

Ng to $\varphi(g)$. Because if not, $\varphi(g) \neq \psi(\pi(g))$.

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

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

Oct 12

Def'n A $\boxed{\text{subring}}$ of $\mathbb{C}$ is a subset $R \subset \mathbb{C}$, closed under addition, subtraction, multiplication & containing 1

ex1 "Gaussian integers", $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

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

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 α
(& so it also contains $\mathbb{Z}$)

$\mathbb{Z}$ adjoin α

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

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

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 $\boxed{\text{algebraic}}$ if $\exists$ a nonzero polynomial w/ integer coefficient p s.t. $p(\alpha) = 0$

Otherwise, α is called $\boxed{\text{transcendental}}$

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

i.e. if $\underbrace{a_m\alpha^m + \dots + a_1\alpha + a_0 = b_n\alpha^n}_{✩} + \dots + b_1\alpha + b_0$

then $m = n$, $a_m = b_m$ .... $a_0 = b_0$

✩ $\Rightarrow m > n$

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

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 α is transcendental $\Rightarrow p(x) = 0$

Def'n A $\boxed{\text{ring}}$ is a set R, together with 2 binary operation,
called "addition" & "multiplication"

satisfying: (i) $\underbrace{(R, +)}_{R^+}$ is an abelian group (identity = "0")

(ii) multiplication is commutative
associative
& $\exists$ an identity element called "1"

(iii) $\forall a, b, c \in R$, $(a+b)c = ac + bc$

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

Oct 14

Def'n If $r \in R$ ($=$ ring) & $\exists\, s \in R$ s.t. $rs = 1$, r is called a $\boxed{\text{unit}}$ in R

Def'n If F is a ring where every non-zero element is a unit, then F is called a $\boxed{\text{field}}$.

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

Pf Let $a \in R$,

$a \cdot 1 = a$ by def'n of multi

But $1 = 0 \Rightarrow a \cdot 0 = a$

$$= a \cdot (0+0) = a \cdot 0 + a \cdot 0$$

$$0 = a \cdot 0 = a$$

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

Def'n A ring homomorphism $\varphi : R \to R'$ is a $\boxed{\text{map}}$ s.t. $\forall\, a, b \in R$,

$$\varphi(a+b) = \varphi(a) + \varphi(b);$$
$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$
$$\varphi(1) = 1_{R'}$$

generalized evaluation

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

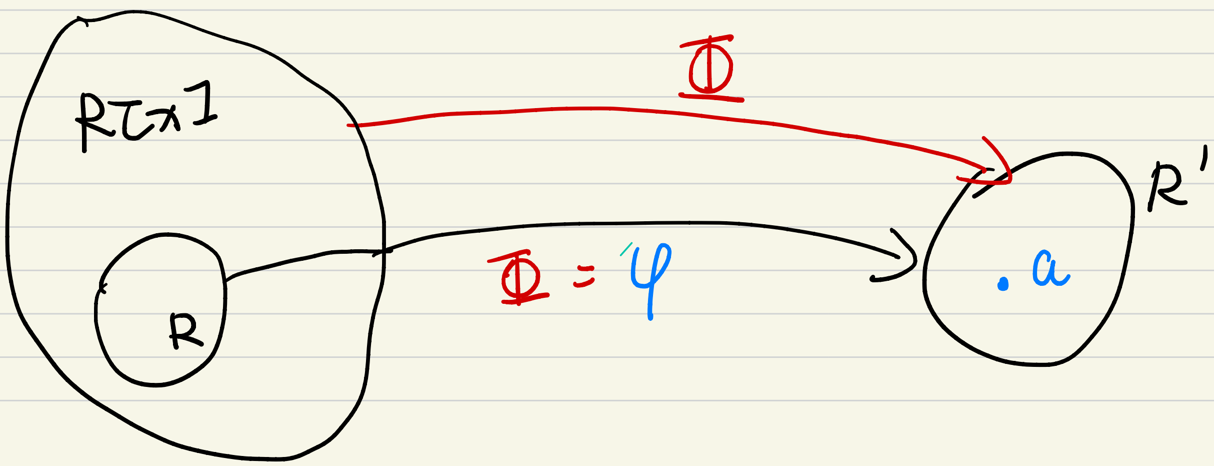
let $R[x]$ be the ring of poly's w/ coeff's in R.

Then given your fav $a \in R'$

$\exists!$ ring hom $\Phi : R[x] \to R'$ s.t. $\Phi_a|_R = \varphi$

i) Φ(constant poly $= r =$ ring element$) = \varphi(r)$

ii) $\Phi(x) = a$



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 $\varphi : R \to R'$ & $a \in R'$, define $\Phi_a : R[x] \to R'$ by

$\Phi_a(a_n x^n + \dots + a_1 x + a_0) = \varphi(a_n)a^n + \dots + \varphi(a_1)a + \varphi(a_0)$

① Φ_a is a ring hom

Check that Φ_a is a ring hom:

WTS $\Phi_a(p(x)\, q(x)) = \Phi_a(p(x))\, \Phi_a(q(x))$

$\Phi_a(p(x)+q(x)) = \Phi_a(p(x)) + \Phi_a(q(x))$ ☆

$\Phi_a(1_R) = 1_{R'}$ ⟵ works because $\Phi_a(1) = \varphi(1) = 1$ since φ is a ring hom. Also, if $r \in R$, $\Phi_a(r) = \varphi(r)$ by the formula, & this verifies (i).

If $p(x) = a_n x^n + \dots + a_0$, $q(x) = b_m x^m + \dots + b_0$, then $\Phi_a(p+q) \overset{n>m}{=} \Phi_a(a_n x^n + \dots + (a_m + b_m)x^m + \dots + (a_0 + b_0))$

$= \varphi(a_n)a^n + \dots + \varphi(a_m+b_m)a^m + \dots + \varphi(a_1+b_1)a + \varphi(a_0+b_0)$

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

$= \Phi_a(p) + \Phi_a(q)$.

$\Phi_a(r) = \varphi(r)$ by the formula, & this verifies (i).

Let $f(x) = \sum_{i=1}^{n} a_i x^i$, $g(x) = \sum_{j=1}^{m} b_j x^j$. Then

$\Phi_a(fg) \overset{\downarrow\downarrow}{=} \Phi_a\left(\sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j x^{i+j}\right) \overset{(☆)}{=} \sum_{i=1}^{n}\sum_{j=1}^{m} \Phi_a(a_i b_j x^{i+j})$

$\overset{\text{by def'n of } \Phi_a}{=} \sum_{i=1}^{n}\sum_{j=1}^{m} \varphi(a_i b_j)\, a^{i+j} \underset{\varphi \text{ is a ring hom}}{=} \sum_{i=1}^{n}\sum_{j=1}^{m} \varphi(a_i)\varphi(b_j)\, a^{i+j} = \Phi_a(f)\Phi_a(g)$

② uniqueness

Uniqueness: Suppose $w : R[x] \to R'$ some ring hom s.t. $\boxed{w(r) = \varphi(r)}$ $\forall r \in R$ & $\boxed{w(x) = a}$

Then $w(a_n x^n + \dots + a_1 x + a_0) \overset{\text{since } w \text{ is a ring hom}}{=} w(a_n)\,w(x^n) + \dots + w(a_1)w(x) + w(a_0)$

$= \varphi(a_n)a^n + \dots + \varphi(a_1)a + \varphi(a_0)$

$= \Phi_a(a_n x^n + \dots + a_1 x + a_0)$.

Thm If R = ring, then $(R[x])[y] \simeq R[x,y]$

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 $\varphi : R \to (R[x])[y]$ (inclusion)

$r \mapsto r$ sends to itself

Sub principle: $\exists !$ ring hom $\Phi : R[x,y] \to (R[x])[y]$

claim: Φ is a bijection

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

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

so by sub principle

$T : (R[x])[y] \to R[x,y]$

Oct 19

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

i) I is closed under $+$

ii) Given $r \in R$ & $s \in I$, $rs \in I$

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

Pf. Note $\varphi(0_R) = 0_{R'} \Rightarrow \ker\varphi \neq \phi$
If $a, b \in \ker\varphi$

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

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

Lemma I is an ideal $\Leftrightarrow I \neq \phi$
& any linear comb $r_1s_1 + \cdots + r_ks_k$ of $s_i \in I$ & $r_i \in R$ is in I

ex1 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 $\boxed{\text{proper}}$ 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
↑ field

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

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

Poly's A poly $a_nx^n + \cdots + a_1x + a_0$ is $\boxed{\text{monic}}$ if $a_n = 1$

poly division If R = ring, $f \in R[x]$ & f is monic,
$g \in R[x]$, then $\exists!$ poly's $q(x)$ & $r(x) \in R[x]$ s.t.
$g(x) = f(x)q(x) + r(x)$, & $\deg(r) < \deg(f)$

Pf

Fix I = ideal in $F[x]$. WTS $I = (f(x))$ for some $f \in I$. If $I = \{0\}$, 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 $f(x) = a_n x^n + \cdots + a_1 x + a_0$

F = field $\Rightarrow \exists$ a multi inverse of a_n. Multiply f by a_n^{-1} (we are still in I) we get $\tilde{f}(x) = x^n + a_{n-1}a_n^{-1}x^{n-1} + \cdots + a_1 a_n^{-1} x + a_0 a_n^{-1}$

$\deg(\tilde{f}) = \deg(f)$, 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

$\Downarrow$

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

$\Downarrow$

contradicts

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 $\varphi: \mathbb{Z} \to R$.
It's given by $\varphi(n) = 1_R + 1_R + \cdots + 1_R$, $\varphi(-n) = -\varphi(n)$

The $\boxed{\text{characteristic}}$ of R is the non-negative number n generating the kernel of $\varphi: \mathbb{Z} \to R$
i.e. smallest # of times you have to add 1_R to itself in R, to get 0_R.

$R/I = \{I + a \mid a \in R\}$ 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 $\pi: R \to \frac{R}{I}$ is a ring hom w/ $\ker = I$
$r \mapsto I+r$
$\{\text{cosets } I+r \mid r \in R\}$

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 $a \in I+a$

$a' = i_1 + a$ $\qquad$ $b' = i_2 + b$

$$a'b' = (i_1+a)(i_2+b) = \underbrace{i_1 i_2 + i_2 a + i_1 b}_{\in I} + ab$$

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

multi identity: $I + 1_R$

add identity: I

If $\pi: R \to R/I$ is a ring hom then $\ker(\pi) = I$

Correspondence Thm Let $\varphi: G \to G'$ an onto gp hom

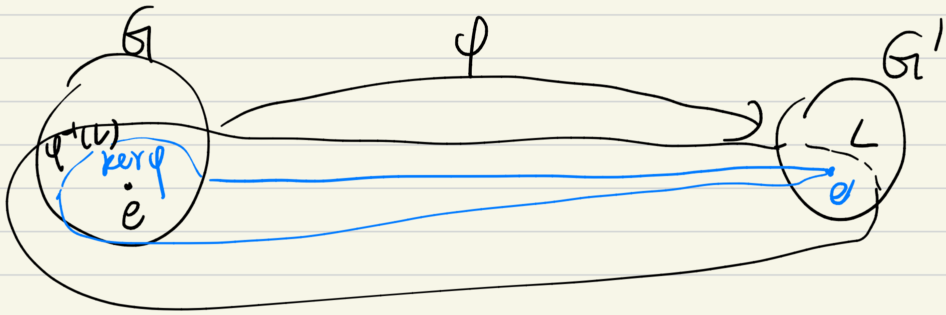
Then $\exists$ a bijective correspondence

$$\begin{Bmatrix}\text{subgps} \\ \text{of } G'\end{Bmatrix} \underset{\varphi^{-1}}{\overset{\varphi}{\rightleftarrows}} \begin{Bmatrix}\text{subgp of} \\ G \text{ containing} \\ \ker\varphi\end{Bmatrix}$$

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 it to

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



$\varphi: R \to R'$ 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'

then $\frac{R}{I} \simeq \frac{R'}{I'}$

1^{st} iso thm for rings

Let $f: R \to R'$, a ring hom w/ kernel $K \subset R$

I be an ideal in R.

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

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

If f is onto & $I = K$, $\bar{f}$ 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 $\overset{\text{onto}}{\text{ring}}$ hom $\pi : R \to R/(a)$ $\quad \ker(\pi) = (a)$

$r \longmapsto r + (a)$

correspondence thm

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

I is the idea in R containing (a)
$= (a, b)$

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

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

ex1 $\mathbb{Z}[i]/(i-2)$ $\quad (\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\})$

strategy: onto hom $\Rightarrow$ 1st iso thm & corresp thm

onto $\varphi_i : \mathbb{Z}[x] \to \mathbb{Z}[i]$

$p(x) \longmapsto p(i)$

$\ker \varphi_i = (x^2+1)$

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

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

① mod out $\mathbb{Z}[x]$ by $(x-2)$

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

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

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

$$\mathbb{Z}[i] / (i-2) \approx \mathbb{Z} / 5\mathbb{Z}$$

Oct 26

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

new element — a relation

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

R adjoin i

Proposition R = ring, $f(x)$ = monic poly in $R[x]$

suppose $(f(x)) > 0$, let $n = \deg(f)$

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

= the ring obtained by adjoining element "α" 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
$$g_1 g_2 = fq + r \quad \text{where } \deg(r) < n$$
Then $\beta_1 \beta_2 = r(\alpha)$

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

non-ex $\mathbb{Z}_n$ ← composite, eg: 6

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

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

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

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

This forms a field, called <u>field of fractions</u> of the integral domain R

Oct 28

Thm

creating fields from rings.

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

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

Then $F(R)$ = "field of fractions"

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

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 $\iff$ every non-zero element is invertible & ring axioms are satisfied.

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

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

Mapping Principle:

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

$\varphi : F(R) \to \mathcal{F}$, given by $\varphi([a,b]) = \varphi(\frac{a}{b}) = ab^{-1}$

Quick terminology for integral domains:

- u is a unit is an element in R w/ a multi 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 & b are associates if each divides the other.
  or, iff $b = ua$, $u =$ unit
- a is irreducible iff $a \neq$ unit & has no proper divisors
- a is prime iff $a \neq$ unit if whenever $p | ab$, $p|a$ or $p|b$

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

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

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

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

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

a is

Maximal ideals

R = 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 max'l in R

Consider the natural map $\pi : R \to R/I$ onto ring hom

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

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 $\Rightarrow$ $\nexists$ proper ideal in R containing I

$\Rightarrow$ I is maximal.

Prop d)

Let $\varphi: R \to R'$ surjective ring hom

$\varphi(r+s) = \varphi(r)+\varphi(s)$
$\varphi(rs) = \varphi(r)\varphi(s)$
$\varphi(1_R) = 1_{R'}$

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 $\iff$ I is a maximal ideal

Proof

A ring is a field $\iff$ it contains precisely 2 elements
$\{0_R\}$ & R as ideals

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

So, $1_R \in (r)$
so $\exists x \in R$ s.t.
$1_R = xr \Rightarrow x$ is multi inverse
$\Rightarrow r$ is invertible.

($\Rightarrow$) let J be an ideal
WTS: $J = \{0_R\}$ 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 $\Rightarrow xr \in J \Rightarrow 1_R \in J \Rightarrow s \cdot 1_R \in J$
arbitrary
$\Rightarrow J = R$

correspondence theorem

$\forall$ onto hom, $\exists$ bijective correspondence

$$\left\{ \begin{matrix} \text{ideals in } R \\ \text{containing } \ker\varphi \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{ideals} \\ \text{in } R' \end{matrix} \right\}$$

$$I \longmapsto \varphi(I)$$

$$\varphi^{-1}(J) \longleftarrow\!\!\shortmid\; J$$

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

$$I \longmapsto \varphi(I)$$

$$\varphi^{-1}(J) \longleftarrow\!\!\shortmid\; J$$

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 $0_{R'}$ & R'. $\Rightarrow R'$ is a field. Conversely, $R' =$ 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

$\{r+I \mid r \in R;$ $r+I = r'+I$
$r+r'^{-1} \in I$
$r-r' \in I$

Proof: $\Rightarrow$ onto ring hom $\pi: R \to R/I$, $r \to r+I$, $\ker\pi = I$

from (a): R/I is a field

$\Leftarrow$ 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 $\{0_R\}$ 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 = ring, $r \in R$ is called $\boxed{\text{irreducible}}$
if $\nexists$ $x, y \in R$, neither of which are units
(neither x nor y is multi invertible)
s.t. $r = xy$

$s \in R$ is $\boxed{\text{prime}}$ if 1) $s \neq$ unit 2) 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

a) If $r(x) = b_1 x + b_0 \in \mathbb{Z}[x]$ divides of $f \in \mathbb{Z}[x]$, $f = a_n x^n + \cdots + a_0$, then $b_1 | a_n$ & $b_0 | a_0$

b) Assume $b_1 \neq 0$. Then $r(x) = b_1 x + b_0$ divides $f \in \mathbb{Z}[x]$
$\Leftrightarrow$ $-b_0/b_1$ is a root of f i.e. $f(\frac{-b_0}{b_1}) = 0$

c) A rational root of a monic poly in $\mathbb{Z}[x]$ is an integer
monic: coeff of highest term is 1

Proof

a) i.e. $f = r(x) \cdot q(x)$ ← some 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: $f(-b_0/b_1) = 0 \Leftrightarrow (x - \frac{b_0}{b_1})$ is a factor of f in $\mathbb{Q}[x]$

c) A rational root of a monic integer poly is an integer
Pf: suppose a/b is a root of $f \in \mathbb{Z}[x]$
i.e. $f(\frac{a}{b}) = 0 \Rightarrow bx - a$ divides f
$\Rightarrow b | a_n \Rightarrow b = \pm 1 \Rightarrow \frac{a}{b} \in \mathbb{Z}$

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

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

i) f is primitive
ii) $\forall$ prime numbers $p \in \mathbb{Z}$, p doesn't divide f as elemets of $\mathbb{Z}[x]$
iii) if $\psi_p : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ given mod p on each coeff.
then $f \notin \ker(\psi_p)$ $\forall p$

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. $f(x) = a(x)b(x)$ $(a, b \neq \pm 1)$

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

assume it's a

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

$1 = cb$ (c 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)

$fg = 0$

$f = 0$ or $g = 0$

Lemma: If R is an integral domain & $r \in R$ is prime

r is irreducible

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

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

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

$n \mid f$ $\qquad n \mid g$

b) suppose f, g are primitive.

$\Rightarrow$ leading coeff are positive

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

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

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

Nov 18

Thm

a) Let $f_0(x)$ = primitive & $g \in \mathbb{Z}[x]$. Then if $f_0 | g$ in $\mathbb{Q}[x]$, then $f_0 | g$ 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

$$g = f_0 \cdot (c\, h_0)$$
$$g = c\, \underbrace{f_0 h_0}_{\text{primitive}}$$

$\exists!$ to express $g(x)$ as $g(x) = c' \cdot g_0(x)$ where $c' \in \mathbb{Q}$

$g_0(x)$ is prim AND since $g \in \mathbb{Z}[x]$, $c' = \pm \gcd(\text{coeff' in } g)$

Uniqueness $\Rightarrow$ $c = c'$ & $f_0 h_0 = g_0$

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, $h | f$ & $h | g$ in $\mathbb{Q}[x]$,

so $h_0 | f$ & $h_0 | g$ in $\mathbb{Q}[x]$ $\overset{(a)}{\Longrightarrow}$ $h_0 | f$ & $h_0 | g$ in $\mathbb{Z}[x]$

Thm. WTS: $f(x)$ is irreducible $\Rightarrow$ f is prim & 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 & g as $h = c_1 h_0(x)$, $g = c_2 g_0(x)$ $c_1, c_2 \in \mathbb{Q}$, h_0, g_0 = prim poly

$$f = \boxed{c_1 c_2}\, \boxed{h_0(x)\, g_0(x)} = \boxed{1} \cdot \boxed{f}$$

Prop: Let $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$, let p = prime #, suppose $p \nmid a_n$. Then if $\varphi_p(f) = (a_n \bmod p)x^n + \dots + (a_0 \bmod p) \in \mathbb{Z}/p\mathbb{Z}[x]$ 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, $\exists$ ∞ number of poly's in $\mathbb{Q}[x]$ w/ $\deg \le n$.
BUT, $\exists$ finite # of poly's in $\mathbb{Z}/p\mathbb{Z}[x]$ w/ $\deg \le n$.

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

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

& $f = gh$ & $g, h \in \mathbb{Q}[x]$, By all of our hard work, can assume $g, h \in \mathbb{Z}[x]$

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

$\deg(\varphi_p(g(x))) \le \deg(g(x))$

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

φ_p is a ring hom $\Rightarrow \varphi_p(f) = \varphi_p(g)\varphi_p(h)$

$\deg(\varphi_p(g)) \le \deg(g) > 0$ & $\deg(\varphi_p(h)) \le \deg(h) > 0$

& $\deg(f) = \deg(\varphi_p(f))$ & $\varphi_p(f) = \varphi_p(g)\varphi_p(h)$

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

$\overset{\Downarrow}{\deg(f)}$ > 0

Note. converse fails!

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

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 $a \mid c_0$ & $b \mid c_n$

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:

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

$\Rightarrow f$ irreducible in $\mathbb{Z}$

v) Einstein:

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

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

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

φ_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

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

$\downarrow$

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

$g_0 h_0 = a_0$, is a multiple of p^2

a multiof p

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

we say that K is a $\boxed{\text{field extension}}$ of F

& we write K/F

Def'n Suppose $\alpha \in K$, K/F. α is $\boxed{\text{algebraic over } F}$

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

if α is not alg. over F, α is called $\boxed{\text{transcendental over } F}$

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

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

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

Pf: φ_α not one to one $\Leftrightarrow \ker(\varphi_\alpha) \neq \{0\} \Leftrightarrow \exists\, f \in F[x]$

s.t. $\varphi_\alpha(f) = 0$

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

$F[x]$ = PID (principal ideal domain)

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

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) $(f(x)) = \ker\varphi_\alpha$ & $(f(x))$ is maximal

iv) $f(\alpha) = 0$ & if $g \in F[x]$ s.t. $g(\alpha) = 0 \Rightarrow f \mid g$

(i) $\Rightarrow$ (ii):

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

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

$\Rightarrow g(\alpha) = 0$ or $h(\alpha) = 0$

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

$\Rightarrow$ if either $\deg(g)$ or $\deg(h) > 0$

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

contrad

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

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

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

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

$g = f$

contrad

Nov 30

Field extension

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

imagine "adjoining an abstract element α, satisfy $f(\alpha)=0$

the $F(\alpha)$ is the smallest field containg both F & α

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

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

suppose α = algebraic over F

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

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

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

s.t. $g(\alpha)=0$

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 irred. poly for α over F

degree of α is the deg of g

$F(\alpha) \subseteq K$

"smallest subfield of K containing F & α

Remember $\varphi_\alpha : F[x] \to K$

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

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

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

F = field so $F[x]$ is an integral domain

$F[\alpha] \cong F[x]/\text{sth.}$

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

Prop Let $\alpha \in K$, K/F, α = alg. over F & $f(x)$ = irreducible poly for α over F. Then consider:

$$\psi : F[x]/(f) \to F[\alpha] \quad \text{given by}$$

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

Does this make sense?

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

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

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

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

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

$\parallel$

$p(\alpha) - q(\alpha)$

Then ψ_α is an isomo

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 $F \neq$ field

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

consider $\varphi_\alpha : F[x] \to K$

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

φ_α is onto

1st isomo thm $\Rightarrow F[x]/\ker(\varphi_\alpha) \cong F[\alpha]$

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

$$\begin{tikzcd}
F[x] \arrow[rr, "\varphi_\alpha"] \arrow[dr, "\pi"'] & & F[\alpha] \\
& F[x]/(f) \arrow[ur, "\exists \psi,\ \text{an iso}"'] &
\end{tikzcd}$$

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

From 11.5.5 in Artin

$F[\alpha]$ is a vector space over F

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

$n = \deg(f)$

$\Rightarrow F(\alpha)$ is a vector space over 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'n of K 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, α = alg. over F

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

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

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

Pf 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 $\underbrace{(\text{sth in } F)}_{\in F} \cdot 1$

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

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

deg α over F = deg of irred poly for α over F

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

If $\alpha \in F$, then $x - \alpha$ is the irred poly for α 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. $K = F(\delta)$, where $\delta^2 = d$, $d \in F$

Then $F(\delta)$ is a quadratic extension

Pf Let $\alpha \in K$, $\alpha \notin F$, wher K = quadratic extension of F

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

$\exists x_1, x_2 \in F$ s.t. $x_1 \cdot 1 + x_2 \alpha = 0$

$\Rightarrow x_2 \alpha = -x_1$. If $x_2 = 0 \Rightarrow 0 = -x_1 \Rightarrow x_1 = 0$

$\Rightarrow x_2 \neq 0$, $x_2 \in F \Rightarrow x_2^{-1} \in F \Rightarrow \alpha = -x_2^{-1} x_1$

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

$\Rightarrow \alpha^2$ has to be a liner 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: $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ solves $ax^2 + bx + c = 0$

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

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

Dec 4

Recap: If $char(F) \neq 2$, i.e. $1+1 \neq 0$, & if K/F is a quadratic field extension. then $\exists\, \delta \in K, \delta \notin F$ but $\delta^2 \in F$ & $K = F(\delta)$

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

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

then $x_1 \cdot 1 + x_2 \cdot \alpha = 0$

$\Rightarrow x_1 = x_2 = 0$

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

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

solves $f(x) = 0$

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

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

8) $\delta = 2\alpha - b$ satisfies $\delta^2 = b^2 + 4c$

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

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

$\Downarrow$

$F(\alpha) \subseteq F(\delta)$

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

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

$\Rightarrow F(\delta) = K$

Thm $F \subset K \subset L$ fields

Then $[L:F] = [L:K][K:F]$

Pf. Let $\mathcal{B} = (\beta_1, \ldots, \beta_n)$ = basis for L as a K-vector space and let $\Lambda = (\alpha_1, \ldots, \alpha_m)$ = basis for K as an F-vector space.

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

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

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

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

Let $\gamma \in L$. Since $(\beta_1, \ldots, \beta_n)$ spans L as a K-vector space, $\exists$ $b_1, \ldots, b_n \in K$ s.t. $\gamma = b_1\beta_1 + \ldots + b_n\beta_n$. Since $K = F$-V.S., $\exists$, for each i, $\exists$ $a_{i,1}, \ldots, a_{i,m}$ s.t. $b_i = a_{i,1}\alpha_1 + \ldots + \alpha_{i,m}\alpha_m$.

$$\Rightarrow \gamma = (a_{1,1}\alpha_1 + \ldots + a_{1,m}\alpha_m)\beta_1 + \ldots + (a_{n,1}\alpha_1 + \ldots + a_{n,m}\alpha_m)\beta_n$$

$$= \sum_{i,j} a_{i,j}\alpha_i\beta_j$$ ☺

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

Assume $\exists$ a linear combo $\sum_{i,j} a_{i,j}\alpha_i\beta_j = 0$. WTS: $a_{i,j} = 0$ $\forall i, \forall j$.

Since $\mathcal{B}$ is linearly ind. over K, for each j, $\sum_i a_{i,j}\alpha_i = 0$.

Since Λ lin. ind. over F, $a_{i,j} = 0$ $\forall i$

Dec 7

consequences from last time

a) $F \subset K$, K/F is a finite extension of deg n
{ $\alpha \in K$. Then α is algebric over F. { $\deg(\alpha) | n$

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

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

b) $F \subset F' \subset L$ { $\alpha \in L$ algebraic over F.
Then α is also algebric over F'
If $\deg_F(\alpha) = d$, then $\deg_{F'}(\alpha) \le d$
α is a root of $f \in F[x] \Rightarrow f$ is a multiple of whatever the irred. poly (g) is for α in $F'[x]$
$\Rightarrow f = g(x)h(x)$ for some $h(x) \in F'[x] \Rightarrow \deg$
$\Rightarrow \deg(g) \le \deg(f)$

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 $\alpha + \beta$ { $\alpha\beta$ is also alg. over F.

$\alpha + \beta$ { $\alpha\beta$ 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, & let K & $F' \subset k$, both finite extensions of F. Let K' = subfield of k generated by K & F'.

$$\begin{tikzcd}
 & k \arrow[dl, bend right] \arrow[d] \arrow[dr] \arrow[ddd, bend left=60] & \\
 & K' \arrow[dl] \arrow[dd] \arrow[dr] & \\
K \arrow[dr] & & F' \arrow[dl] \\
 & F &
\end{tikzcd}$$

Let $[K':F] = N$, $[K:F] = m$, $[F':F] = n$. Then $m, n \mid N$, & $N \le nm$, & if $\gcd(n,m) = 1$, then $N = nm$.

Pf of lemma: The green Consequences $\Rightarrow$ any finite extension is generated by a finite # of alg. elements.

$$\begin{tikzcd}
 & K' \arrow[dl, "\le n"'] \arrow[dd, "N"] \arrow[dr, "\le m"] & \\
K \arrow[dr, "m"'] & & F' \arrow[dl, "n"] \\
 & F &
\end{tikzcd}$$

finite! finite!

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 $\Rightarrow$

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

$\Rightarrow m \mid N$. Similarly, $n \mid N$.

Now, suppose F' is generated by one element, β, over F, i.e., $F' = F(\beta)$. Then $K' = K(\beta)$. why? Well, $K = F(\text{some stuff})$, $F' = F(\beta)$.

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

consequence (b) $\Rightarrow$ $\deg_K \beta = [K':K] \le \deg_\beta F = n$

$\Rightarrow N \le nm$

argument $\Rightarrow$ $[K':F]$ is divisible by $\operatorname{lcm}(m,n)$ which if $\gcd(m,n) = 1$, is mn

Dec 9

Lemma:

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

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

(b) Suppose α, β alg. over F & $\deg_F(\alpha) = d_1$, $\deg_F(\beta) = d_2$. Then the $d_1 d_2$ monomials $\alpha^i \beta^j$ $(1 \le i \le d_1, 1 \le j \le d_2)$ span $\boxed{F(\alpha, \beta)}$ 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 α & β.

How? Given the minimal poly's for α & β, 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., $\gamma = \alpha+\beta$) $\quad 1, \gamma, \gamma^2, \dots, \gamma^n$ as linear combo's of $\{\alpha^i \beta^j\}_{\substack{1\le i \le d_1 \\ 1 \le j \le d_2}}$. So, when $n = d_1 d_2$, we have more vectors than elements in the spanning set.

Note: we always have

$$\pi : \mathbb{Q}[x] \to \mathbb{Q}[x]/(x^2+1)$$

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

$\deg f > 0$

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

$$\pi : F[x] \to F[x]/(f(x))$$

is 1-1 WHEN we restrict to constants.

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

If $\pi(a_1) = \pi(a_2)$, $a_1 + (f) = a_2 + (f) \Leftrightarrow \underset{\substack{\neq \\ 0}}{a_1 - a_2} \in (f)$

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

Dec 11

Lemma F = field, $f(x) \in F[x]$ irreducible over F

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

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

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

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

suppose $f(x) = a_n x^n + \cdots + a_0 \quad a_i \in F$

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

$+ \cdots + (a_0 + (f)) = 0 \in K$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \rotatebox{90}{=} (f)$

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

Definition F = field; a poly $f \in F[x]$ splits completely over some field extension K if f factor into linear pieces w/ coeff in K

Lemma F = field, f = monic poly in $F[x]$, $\deg(f) > 0$. Then $\exists$ a field extension K in which f splits completely

Finite Fields

Let p = 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 = finite field. $|F| = q$ for some p, r.

c) If $|F| = q$, the 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 = finite field, $|F| = p^r$

then F contains a subfield of size p^k

$\Leftrightarrow$ $k \mid r$

Pf of (c)

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 α

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

has to divide $q-1$

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

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

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

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

$$\begin{array}{c} \| \\ \boxed{K} \end{array}$$