21-373 11/15/2020

Summary of Material Since Midterm 1 (Group Theory)

Group Actions [orbit(x) $\subseteq S$ $= \{g\cdot x \mid g\in G\}$, $G_x = \{g\in G \mid g\cdot x = x\}$]

Suppose G acts on S. Then $\forall x \in S$

(S: set, not necessarily a group)

(Fundamental Theorem) size of orbit $\boxed{|\text{orbit}(x)| = [G : G_x]}$ index of stabilizer

(Proof sketch: $h\cdot x \longrightarrow hG_x$, $f(hG_x) = h\cdot x$.
$h_1G_x = h_2G_x \Leftrightarrow h_1^{-1}h_2 \in G_x$
$(h_1^{-1}h_2)\cdot x = x \Rightarrow h_2x = h_1x$)

In particular, if G acts on itself by $g\cdot x = gxg^{-1}$,

$[G : G_x] = \{g\in G \mid gxg^{-1} = x\} : C_G(x)$, centralizer of x

(Class Equation: $\boxed{|G| = |Z(G)| + \sum_{g\notin Z(G)} [G : C_G(g)]}$ for the action by conjugation.

(Proof sketch: $x\sim y \Leftrightarrow x \in \text{orbit}(y)$ partitions G, $x \in Z(G) \Rightarrow \text{orbit}(x) = \{x\}$ $\because gxg^{-1} = gg^{-1}x = x$)
Then apply orbit-stabilizer.

let $S_0 = \{x\in S \mid (\forall g\in G)\, g\cdot x = x\}$

$\boxed{\text{If } |G| = p^n, \text{ } p \text{ prime, then } |S| \equiv |S_0| \bmod p.}$

(proof sketch: Recall class equation. $C_G(g) \leq G \Rightarrow p \mid |G_G(g)|$
In general $p \mid G_x$. Since $|S| = |S_0| + \sum |S_*|$, $|S_*| \equiv 0 \bmod p$, $|S_0| \equiv |S| \bmod p$.

Applications: $\boxed{|G| = p^n,\ p \text{ is prime. } Z(G) \neq \{1\},\ |Z(G)| \equiv 0 \bmod p \Rightarrow |Z(G)| \geq p.}$

Cauchy's and Sylow's (1st) Theorem

Let G be finite group, p prime.

(Cauchy) If $p \mid |G|$, then $\exists\ H \leq G$, $|H| = p$.

(Sylow) If $p^k \mid |G|$, then $\exists\ H_k \leq G$, $|H_k| = p^k$.

Proofs.

Cauchy

(Unorthodox) - using group actions on specific sets

$S = \{(a_0, \dots, a_{p-1}) \mid a_i \in G, \prod_{i=0}^{p-1} a_i = 1_G\}$ (sequence!)

$H = \mathbb{Z}/p\mathbb{Z}$ acts on S by rotation.

Show that $S_0 = \{(a, \dots a) \mid \prod a = a^p = 1\}$

S_0 is non-empty, $|S_0| \equiv |S| = |G|^{p-1}$,

$\Rightarrow |S_0| \equiv 0 \bmod p$, $|S_0| \geq p$.

So there exists $a \neq 1$, $H = \{1, a, \dots a^{p-1}\} \leq G$.

(Induction)

Sylow

Combinatorial Lemma: For p prime, $m, n \in \mathbb{N}$, $(p, m) = 1$.

$\binom{mp^n}{p^n} \equiv m \bmod p$. $G = \mathbb{Z}/p^n\mathbb{Z}$, $B = \{1, 2, \dots mp^n\}$.

$S = \{X \subseteq G \times B \mid |X| = p^n\}$

$g \cdot (a, b) = (g + a, b)$. $S_0 = \{U(a,b) \mid U(g+a,b) = U(a,b)\}$.

So $S_0 = \{X \in S \mid b\}$, $b \in B$. ($\uparrow$ preserve $|X| = p^n$.)

$|S_0| = m$!

$S = \{X \subseteq G : |X| = p^k\}$. $|S| = \binom{mp^n}{p^k}$.

$\exists X \in S$ (representative), $p \nmid [G : G_X]$. $|G_X| \geq p^k$ by Lagrange.

pick $a_0 \in X$, show $f : G_X \to X$, $f(g) = g \cdot a_0$ (left coset)

Show f well-defined and injective

$\therefore |G_X| \leq p^k$

Need: $[N_G(H) : H] \equiv [G : H] \bmod p$ for $|H| = p^k$. (I.H.)

H acts on $S = \{gH\}$, left cosets, $S_0 : (hg)H = gH$ (trivial)

$h \cdot gH = (hg)H$ $g^{-1}hg \in H$

Since $p \mid [G : H]$, then $N_G(H) \supsetneq H$. $\therefore g \in N_G(H)$

$\varphi : N_G(H) \to N_G(H)/H$ (shrink by factor p^k) contains group of size p

OR case on whether $p \mid |Z(G)|$ (2nd proof)

Extensions

(Cauchy $\to$ Sylow)

- If $|G| = p^n$, p prime, $\forall k \in n$, $\exists\ H_k \leq G$, $|H_k| = p^k$.

Induction + Natural homomorphism. Show $\exists\ H \leq G$, s.t. $|H| = p$, $H \trianglelefteq G$.

use Cauchy guarantee on $|Z(G)| = kp$.

(Sylow $\to$ Cauchy)

- Sylow identifies subgroup of size $|P| = p^n$. Show existence also of subgroup order p.

Take $b \neq 1 \in G$. $\langle b \rangle = p^k$, $k \leq n$ by Lagrange. Take $a = b^{(p^{k-1})}$. $a^p = b^{p^{k-1} \cdot p} = b^{(p^k)} = 1$

$\therefore \langle a \rangle \leq G$, $|\langle a \rangle| = p$.

*2

Normal Subgroups

$N \trianglelefteq G \Leftrightarrow (\forall g \in G, \forall n \in N, gNg^{-1} \in N) \Leftrightarrow (\forall g \in G, gN = Ng)$.

Note: • for $\varphi: G \to H$, $\ker(\varphi) \trianglelefteq G$.

• For any $M \leq G$, $M \leq N_G(M)$

• $N \leq G$, $N_G(N) = G \Leftrightarrow N \trianglelefteq G$

• Normal subgroups generate the quotient group G/N.

• $H \leq Z(G) \Rightarrow H \trianglelefteq G$. (e.g. $\mathbb{Z}/n\mathbb{Z}$).

• $N \trianglelefteq G \Leftrightarrow \varphi: G \to G/N$ natural homomorphism.

• $H \trianglelefteq G$, $H \leq N \leq G \Rightarrow H \trianglelefteq N$.

Isomorphism Theorems

see also p135 regarding characteristic subgroups $\sigma(H) = H$ for $\sigma \in \mathrm{Aut}(G)$

K char H, $H \trianglelefteq G \Rightarrow K \trianglelefteq G$

(1) $\varphi: G \to H$ surjective homomorphism $\Leftrightarrow G/\ker\varphi \cong H$.

def. $\psi: G/\ker\varphi \to H$ by $\psi(aN) \to \varphi(a)$. $aN = cN \Leftrightarrow a c^{-1} \in N = \ker\varphi$

$\varphi(a c^{-1}) = \varphi(a)\varphi(c)^{-1} = 1$

$\therefore \varphi(a) = \varphi(c)$

$\psi(aN \cdot bN) = \psi(ab)N$

$= \varphi(ab) = \varphi(a)\varphi(b) = \psi(aN)\psi(bN)$

ψ surjective by assumption

ψ injective since $\ker\psi = \{aN \mid \varphi(a) = 1\} = \{aN \mid a \in \ker\varphi\}$

$= N = \{1 \in G/N\}$.

• G is infinite cyclic $\Rightarrow G \cong (\mathbb{Z}, +)$.

• G is finite cyclic $\Rightarrow G \cong \mathbb{Z}/k\mathbb{Z}$.

Suppose $G = \langle a \rangle$, $a^k = 1$. $\varphi: \mathbb{Z} \to G$, $\varphi(z) = a^z$.

$\ker(\varphi) = \{x \mid x \equiv 0 \bmod k\}$

$= k\mathbb{Z}$.

(2) Given $A, B \leq G$, if $A \leq N_G(B)$ then

(a) $AB \leq G$ $a \cdot b_1 = b_2 \cdot a$

$(a_1 b_1)(a_2 b_2) = b_3 a_1 a_2 b_2$

$= b_3 a_3 b_2 = a_4 b_4 b_2 = a_4 b_5$.

OR $HK \leq G$ iff $HK = KH$

we can show $AB = BA$.

(b) $B \trianglelefteq AB$ $AB \leq N_G(B)$ sufficient.

(c) $A \cap B \trianglelefteq A$ Use 1st Isomorphism!

$\varphi: A \to AB$, $\varphi(a) = aB$

$\ker\varphi = \{a \mid aB = B\} = \{a \mid a \in B\} = A \cap B$.

$\ker\varphi \trianglelefteq A$.

(d) $AB/B \cong A/A \cap B$

set of sets

$A/A\cap B \cong AB$, $AB = \bigcup_{a \in A} aB$ in fact $\bigcup_{a \in A} Ba$

$\varphi: A \to AB/B$

$\gamma: AB \to AB/B$ $\ker(\varphi\gamma) = A \cap B$.

(3) $H, K \trianglelefteq G$, $H \leq K \Rightarrow K/H \trianglelefteq G/H$, $G/K \cong (G/H)/(K/H)$

def $\varphi: G/H \to G/K$ by $\varphi(aH) = aK$. $\ker(\varphi) = \{aH \mid aK = K \Leftrightarrow a \in K\} = K/H$.

$\ker(\varphi) = K/H \trianglelefteq G/H$.

Def. p-groups. TFAE: for p prime, G finite,

(1) $\forall a \in G, \exists n \in \mathbb{N}, |\langle a \rangle| = p^n$

(2) $\exists n \in \mathbb{N}, |G| = p^n$.

Sylow's p-groups P is a Sylow p-subgroup of G provided

(1) P is a p-group for some prime p

(2) P is maximal: if H is p-group and $P \leq H \leq G$, then $H \leq P$.

* A Sylow p-group always exists, as a consequence of Sylow's 1st Theorem identifying a subgroup of size p^n if $|G| = mp^n$, $(m,p)=1$.

2nd Sylow's Theorem Let G be finite, p prime, $p \mid |G|$.
$P, Q \leq G$ both Sylow-p-subgroups $\Rightarrow \exists\, g \in G$, $Q = gPg^{-1}$.
(all Sylow-p-subgroups are isomorphic)

Proof sketch: let Q act on $S := \{xP \mid x \in G\}$ by left mult.

show $xP \in S_0 \Rightarrow x^{-1}Qx = P$. $(x^{-1}Qx) \in P$)

lastly show that S_0 is non-empty.

3rd Sylow's Theorem Let G be finite, p prime, $p \mid |G|$. $S = \{P \leq G \mid P \text{ is Sylow } p\text{-subgroup}\}$.
Then $|S| \equiv 1 \bmod p$.

Sylow 2nd implies that $Q \in S \Rightarrow Q = gPg^{-1}$ for some reference P. but $\in$ is true too, because every group of size p^n is Sylow-p!

Define action of P on S by $h \cdot (gPg^{-1}) = h(gPg^{-1})h^{-1}$.

Show that $Q \in S_0 \Rightarrow P \leq N_G(Q)$

Since $Q \trianglelefteq N_G(Q)$, P and Q are Sylow-p-subgroups of $N_G(Q)$.
(=)

So $P = xQx^{-1} = Q$! $P = Q$, so $|S_0| \equiv 1 \bmod p$,

$|S| \equiv 1 \bmod p$.

21-373 Midterm 2 Review

Ring Theory

(a commutative division ring (every element has multiplicative inverse) is a field)

In most cases, we care about commutative rings with identity.

Note: • Identity exists + Distributive ⇒ Addition is commutative.

Pf: $(1+1)(a+b) = (1+1)\cdot a + (1+1)\cdot b = a + (a+b) + b$

$\updownarrow$

Also, $(1+1)(a+b) = 1\cdot(a+b) + 1\cdot(a+b) = a + (b+a) + b$

- $\forall a \in R,\ a\cdot 0 = 0\cdot a = 0$ [Pf. $a\cdot(0+0) = a\cdot 0 + a\cdot 0 = a\cdot 0$]
- $(-a)b = -(ab)$, $a(-b) = -(ab)$, $(-a)(-b) = ab$
  $(a_1 - a_2)b = a_1 b - a_2 b$

  ↓ [Pf. $a(-b) + a(b) = a(-b+b) = a\cdot 0 = 0$] then by uniqueness of inverse gp.

Ideals $I \subseteq R$ is an ideal, provided

(1) $(I,+) \leq (R,+)$

(b) $\forall r \in R,\ \forall a \in I,\ r\cdot a \in I$

Every ideal is a subring of R. $r\cdot(a_1, a_2) = (r\cdot a_1)a_2 = a_3\cdot a_2 \in I$.

* for $\varphi: R_1 \to R_2$ ring homomorphism, $\ker(\varphi)$ is an ideal. If R_1 is a field, then $\ker(\varphi) \subsetneq R_1 \Rightarrow \ker(\varphi) = \{0\}$ $\Leftrightarrow \varphi$ is injective.

* R is a field $\Leftrightarrow$ Ideals of R are $\{0\}$ and R.
  ($\Leftarrow$) consider $(a) = \{ra \mid r \in R\}$, $a \neq 0$, $(a) = R$ by assumption
  so $1 \in (a)$. $1 = ra$, so $r = a^{-1}$.

Subring generated by ideal $(A) := \bigcap_{J \text{ ideal of } R,\ J \supseteq A} R = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R, n \in \mathbb{N}, a_i \in A \right\}$

($\subseteq$) Show ↓ ideal, $\supseteq A$

($\supseteq$) each $r_i a_i$ ✓ additive subgroup ✓

Zero-divisors $a \in R - \{0\}$ s.t. $\exists\, b \in R - \{0\}$, $a\cdot b = 0$

integral domain any R that does not contain an integral domain

*5

Maximal and Prime Ideals

Maximal ideal I : No $J \subsetneq R$ s.t. $J \supsetneq I$

(By Zorn's Lemma, every proper ideal in a ring with identity is contained in a maximal ideal)
↓ show existence of maximal subgroup in any chain

Prime ideal I : $\forall a,b \in R-\{0\}$, $ab \in I \Rightarrow a \in I \vee b \in I$.

eg. $3\mathbb{Z}, 5\mathbb{Z}$...

eg. multiples of primes
if p divides ab...

Note that $\mathbb{Q}$ contains no maximal subgroup.
e.g. take any element and divide as close to 0 as you can by 2...

I maximal $\Rightarrow$ I is prime.

(If $R=\mathbb{Z}$, $I \subseteq \mathbb{Z}$ prime, then it is also maximal)
$[\mathbb{Z} : I] = p$, so cannot exist S s.t. $[\mathbb{Z} : S][S : I] = p$

Pf. I maximal $\Leftrightarrow$ R/I field.

($\Rightarrow$) contradiction. if I maximal and R/I not field, $\varphi^{-1}[J] \supsetneq I$ for $\{I\} \subsetneq J \subsetneq R/I$. Since I max, $\varphi^{-1}[J] = R$, contains 1. So J contains $1+I$.

($\Leftarrow$) if I not maximal and R/I field, $\varphi[J] = R/I \Rightarrow \exists\, b \in J$ s.t. $1-b \in I$
but $1-b \in J$ also
$\therefore 1 \in J$.

$(a+I)\oplus(b+I) := (a+b)+I$
$(a+I)\odot(b+I) := ab+I$

R/I field $\Rightarrow$ R/I integral domain. (def)

I prime $\Leftrightarrow$ R/I integral domain $\Rightarrow$ (R/I not i.d. — contrapositive.) $\therefore \exists\, a+I, b+I$, $a,b \notin I$, $(a+I)(b+I) = ab+I = I$
$ab \in I$ ✓
So I is not prime.

Note. R/I field $\Rightarrow$ I prime.

but I prime $\not\Rightarrow$ R/I field.
(counter-example: $\{0\}$ prime in $\mathbb{Z}$, but $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ not field)

($\Leftarrow$) contrapositive: $ab \in I$, but $a \notin I$ and $b \notin I$.
So $(a+I)\cdot(b+I) = ab+I = I$ $\therefore$ R/I contains zero divisors, not integral domain.

Misc Lemmas. Suppose R_1, R_2 are rings, $\varphi: R_1 \to R_2$ surjective homomorphism.

(a) If $I \subseteq R_1$ ideal, then $\varphi[I]$ is ideal of R_2.
Pf. → Given $a,b \in \varphi[I]$, $a+b = \varphi(a')+\varphi(b') = \varphi(a'+b') = \varphi(c') = \varphi[I]$ ($c' \in I$)
$a-b$... (similarly)
→ $r\cdot a = \varphi(r')\varphi(a') = \varphi(r'a')$ ...

(b) If $J \subseteq R_2$ ideal, then $\varphi^{-1}[J]$ is ideal of R_1.
→ Given $a,b \in \varphi^{-1}[J]$, exists c', b' ($a = \varphi^{-1}[a']$, $b = \varphi^{-1}[b']$) $\in J$
$\varphi(a+b) = \varphi(a)+\varphi(b) = c' \in J$, so $a+b \in \varphi^{-1}[J]$.
$R\cdot(a+b)$...

*6

21-373 Final Review 12/11/2020

Group Theory → $H \leq G$, $ab^{-1} \in H$ for all $a, b \in G$

→ $ab^{-1} \in H \Rightarrow a \in Hb$ (right coset of b)

$Ha \cap Hb \neq \emptyset \Rightarrow Ha = Hb$.

$a^{-1}b \in H \Leftrightarrow b \in aH$ (left coset) is equivalence relation

→ Partition of G via cosets: $\exists X \subseteq G$, $a \neq b \in X \Rightarrow Ha \neq Hb$

(X: set of representatives), and $G = \bigcup_{a \in X} Ha$ (disjoint union)

→ Idea of partition appears in group actions:

when G acts on S, $x, y \in S$. $x \sim y \in G \Rightarrow x = gy$ for some $g \in G$. ($\sim$: eq relation)

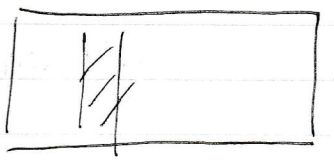
The eq class of x is $\{g \cdot x \mid g \in G\}$ ($\text{orbit}(x)$).

$\text{orbit}(x) \cap \text{orbit}(y) \neq \emptyset \Rightarrow \text{orbit}(x) = \text{orbit}(y)$

~~# number of orbits~~

~~size of each orbit~~

$|\text{orbit}(x)| = [G : G_x]$



$\text{orbit}(x)$ contains is of the same size

There is $A \subseteq S$ s.t. $x \neq y \Rightarrow \text{orbit}(x) \cap \text{orbit}(y) = \emptyset$

$S = \bigcup_{x \in A} \text{orbit}(x)$

Lagrange's Theorem: $|G| = [G : H] \cdot |H|$

($M \cdot |Ha| = |H|$ since $f(x) = xa$)

Consequence of Lagrange. If $|G| = $ prime, then $\exists a \in G$, $\langle a \rangle = G$.

G acting on S

Examples. (1) $S = \{X \mid X \subseteq G\}$

(2) $S = \{X \subseteq G \mid |X| = p^n\}$ Sylow 1

action by left multiplication $g \cdot X = \{gh \mid h \in X\}$ $(g \in G, X \subseteq G)$

(3) $S = \{H \mid H \leq G\}$ HW2 exercise

(4) $S = \{(a_1, \dots, a_p) \mid a_i \in G, \prod a_i = 1\}$ $G = \mathbb{Z}/n\mathbb{Z}$ acts on S.
sequence, proves Cauchy

$g \cdot X = \{ghg^{-1} \mid h \in X\}$ action by inner automorphisms
Sylow 2

(*) $S = G$. G acts on G by inner automorphism.
$gX = gxg^{-1}$. Used to prove that

$|G| = p^n$, p prime $\Rightarrow p \mid |Z(G)|$, $Z(G) \neq \{1\}$.

Conjugacy Class Equation. $|G| = |Z(G)| + \sum_i [G : C_G(g_i)]$.

$x \in Z(G) \Leftrightarrow |\text{orbit}(x)| = \{x\} = 1$.

(Generalization) Suppose G is p group ($|G| = p^n$) p prime acting on a finite S.
Then $|S| = |S_0| \bmod p$ where $S_0 = \{x \in S \mid (\forall g \in G) g \cdot x = x\}$

↳ we used this to prove Sylow's First Theorem.

21-373 Final Review

Homomorphisms. $\varphi: G \to H$ homomorphism.

$$\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$$

Lemma (1) $\varphi(1_G) = 1_H$ [$\varphi[1_G \cdot 1_G] = \varphi[1_G]\varphi[1_G] = \varphi[1_G]$ can cancel ✓]

(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Example. $A \in GL(n, F)$ $\det A \in F - \{0\}$.

Fact $\det(A \cdot B) = \det(A) \cdot \det(B)$

Def: $\varphi: G \to H$ homomorphism. $\ker(\varphi) := \{g \in G \mid \varphi(g) = 1_H\} \leq G$.

$SL(n, F) := \ker(\det)$

Def. $N \trianglelefteq G$ if (a) $N \leq G$, and

(b) $\forall g \in G, \forall n \in N, gng^{-1} \in N$

Fact

$\ker(\varphi) \trianglelefteq G$; $Z(G) \trianglelefteq G$, $H \leq Z(G) \Rightarrow H \trianglelefteq G$.

Fact $N \leq G$, $N \trianglelefteq G$, $\forall a \in G$, $Na = aN$. ($aNa^{-1} = N$)

Theorem $N \trianglelefteq G$, $G/N := \{aN \mid a \in G\}$, the operator $*$ on G/N given by $(aN) * (bN) := (ab)N$ is a group operation

$1_{G/N} = N$.

#9

Fact. $\varphi: G \to H$ surjective homomorphism.

(1) $H' \leq H$ then $\varphi^{-1}[H'] \leq G$.

(2) $G' \leq G$ then $\varphi[G'] \leq H$.

In particular, this is interesting when H is G/N.

Fact $N \trianglelefteq G$ then $\varphi: G \to G/N$ given by $\varphi(g) = gN$ is a surjective homomorphism (canonical/natural homomorphism)

Application Theorem. $|G| = p^n$, p prime.

$\forall\ k < n$, $\exists\ H_k \leq G$, $|H_k| = p^k$.

Proof. Idea: we know $Z(G) \geq 1$.

$p \mid |Z(G)| \Rightarrow$ (Cauchy) $\exists\ a \in Z(G)$, $|\underbrace{\langle a \rangle}_{H}| = p$.

As $H \trianglelefteq G$, consider $G \to G/H$, $\varphi(g) := gH$.

$|G/H| = [G:H]$. Since $|H| \geq p$, $[G:H] = \frac{|G|}{|H|} = p^{n-1} \leq |G|$

We use inductive hypothesis to find $H' \leq G/H$ of size p^k.

Let $H'' = \varphi^{-1}[H']$ has cardinality $[H'] = p^{k+1}$.

21-373 Final Review 12/11/2020

Rings

- Integral domain (cancellation property $a \in R-\{0\} \cdot ax=ay \Rightarrow x=y$)

- $I \subseteq R$ ideal. (a) $(I,+) \leq (R,+)$

(b) $\forall r \in R, \forall a \in I, r \cdot a \in I$.

Theorem. R commutative with $1 \neq 0$.

If the only ideals of R are $\{0\}$ and R, then R is a field.

Proof Idea. Take $a \in R-\{0\}$

(a) $=\{r \cdot a \mid r \in R\}$ ideal, as $a \neq 0$

(a) $\neq \{0\}$ by assumption, (a) $= R$. since $1 \in R$, $\exists r \in R$, $1 = r \cdot a$.

- $\{$finite integral domain$\} \subseteq \{$field$\}$

- I is prime $\quad ab \in I \rightarrow a \in I \vee b \in I$.

maximal... $\neg \exists J \subsetneq R$ ideal, $J \supsetneq I$.

- Theorem. R commutative, $1 \neq 0$. I ideal $\subsetneq R$.

I is maximal $\Leftrightarrow$ R/I is a field. [$\varphi : R \to R/I$]

$\varphi(a) = a + I$.

- Theorem. R commutative, $1 \neq 0 \in R$, ideal.

R/I is integral domain $\Leftrightarrow$ I prime.

*11

R is PID $\Leftrightarrow$ Integral Domain $\wedge$ $\forall I \subseteq R$ ideal, $\exists a \in I$, $(a) = I$.

Theorem. R PID, I ideal, then I max $\Leftrightarrow$ prime

$\in$ new/important.

- Ring of fractions
- UFD - factorization

  irreducible vs prime. ($\cong$)

  PID $\subseteq$ UFD.

, coset calculus

21-373 Final Review 12/11/2020

Rings

- Integral domain (Cancellation property $a \in R - \{0\} \cdot ax = ay \Rightarrow x = y$)

- $I \subseteq R$ ideal. (a) $(I, +) \leq (R, +)$

(b) $\forall r \in R, \forall a \in I, r \cdot a \in I$.

Theorem. R commutative with $1 \neq 0$.

If the only ideals of R are $\{0\}$ and R, then R is a field.

Proof Idea. Take $a \in R - \{0\}$

$(a) = \{r \cdot a \mid r \in R\}$ ideal, as $a \neq 0$

$(a) \neq \{0\}$ by assumption, $(a) = R$. Since $1 \in R$, $\exists r \in R$, $1 = r \cdot a$.

- $\{\text{finite integral domain}\} \subseteq \{\text{field}\}$

- I is prime $ab \in I \rightarrow a \in I \vee b \in I$.

maximal... $\neg \exists J \subsetneq R$ ideal, $J \supsetneq I$.

- Theorem. R commutative, $1 \neq 0$. I ideal $\subsetneq R$.

I is maximal $\Leftrightarrow$ R/I is a field. [$\varphi : R \to R/I$]

$\varphi(a) = a + I$.

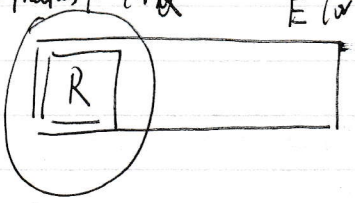
- Theorem. R commutative, $1 \neq 0 \in R$, ideal.

R/I is integral domain $\Leftrightarrow$ I prime.

*11

21-373 (Supp' / Revision)

Ring of fractions F (or $\mathbb{Q}$)



Steven Ledford

$q = rd^{-1}$

(Book) p261 R, Q, S (field)

Q is smallest ring containing R in which all elements of $D \subseteq Q$ become units.

if $R \subseteq S$, all non-zero elements of R have inverses in S, and $\varphi \upharpoonright R = id_R$.

('D')

- Define Equivalence Class in $A = \{(x,y) \mid x \in R, y \in R - \{0\}\}$

  Then define F_R (or $\mathbb{Q}$) $= \{[(x,y)] \mid (x,y) \in A\}$

- Show that Q is a field.

  All $R - \{0\} \cong \{[(r,1)]\}$ have inverses in Q.

  $\frac{rd}{d}$ has inverse $\frac{d}{rd}$.

  Then elements of Q can be (represented) written as $q = rd^{-1}$, $d \in R - \{0\}$

  if $Q \neq 0$, then $r \neq 0$, so $r \in R - \{0\}$ as well, and has an inverse.

  So $q^{-1} = dr^{-1}$.

  ↑ able to appear in denominator

- Show that Q is 'minimal'.

  Interpret $\frac{a}{b}$ as a multiplied by the inverse of b

Lecture: $\varphi([a,b]) := \frac{a}{b}$

if Q and S are different objects, $\Phi(rd^{-1}) = \varphi(r)\varphi(d)^{-1}$.

s.t. $\exists \varphi : Q \to S$, def. (in the case of lecture, $\varphi(r) = r$)

#13

Field of Fractions of a Polynomial Ring.

Suppose F is a field and consider the polynomial ring $F[x]$. The field of fractions consists of all ratios of two polynomials with coefficients in F,

$$\widetilde{F(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x] \right\}$$

E.g. $\frac{2x-3}{x^2-5x+6} \in \mathbb{Q}(x) = \mathbb{Q}(x)$.

Basically my scribbles

- A gcd always exists in a PID. (in integers, we define gcd to be the smallest integer $d \geq 0$ s.t. $ax+by=d$ has solutions for x and y).

of (a,b)

- Show that $I = \{ax+by \mid x,y \in R\}$ is an ideal and has a generator d, $(d)=I$, which is a gcd.

  - write $d = ax_0+by_0$.

  wts: (1) $d \mid a$, $d \mid b$.

  $a, b \in I$
  $\therefore \exists r_a, r_b$ s.t. $r_a \cdot d = a$
  $r_b \cdot d = b$.

  (2) if $\exists\ d'$ s.t. $d' \mid a, d' \mid b$, then $d \mid d'$.

  $a = d'x'$, $b = d'y'$.

  Then $d = ax_0 + by_0$
  $= d'x'x_0 + d'y'y_0$
  $= d'(x'x_0 + y'y_0)$

  $\therefore d' \mid d$.