

Hwk 8 #12

$$R = \mathbb{Z}\sqrt{-5}$$

$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, so R is not a UFD

i) (2) , (3) , $(1 \pm \sqrt{-5})$ are not prime ideals.

[[I prime $ab \in I \Rightarrow a$ or $b \in I$,

$6 \in (2)$, but $1 \pm \sqrt{-5}$ are not in (2) . So (2) is not prime, similar for others.

ii) $(2, 1 \pm \sqrt{-5})$, $(3, 1 \pm \sqrt{-5})$ are all prime ideals.

Problem #11 states that if -5 is a square mod p ($-5 = x^2$), then $(p, x \pm \sqrt{-5})$ is a prime ideal.

Namely $\frac{R}{I} \cong \mathbb{Z}_p$ here $-5 \equiv 1 \pmod{3} = 1^2$

So can apply this to get $(3, 1 \pm \sqrt{-5})$ is prime. $(2, 1 \pm \sqrt{-5})$ is prime in the same way.

$$\text{iii) } (2) = (2, 1 + \sqrt{-5}) \cdot (2, 1 - \sqrt{-5})$$

$$(3) = (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$$

$$\text{iv) } (6) = (2) \cdot (3) = (2, 1 + \sqrt{-5}) \cdot (2, 1 - \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$$

$$= (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) = (2, 1 - \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) \cdot (2, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$$

is a unique decomposition into prime (maximal) ideals.

{Euclidean domains $F[x]$, \mathbb{Z} , $\mathbb{Z}[i]$ } \subset {PID}

{PID} \subset {UFD} \subset {Dedekind domains}

§5 Groups

Definition 5.1

A group G is a set together with a binary operation $G \cdot G \rightarrow G$ such that

i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

ii) There exists a neutral element $e : g \cdot e = g = e \cdot g$

ii) Inverse: For all $g \in G$, \exists inverse $g^{-1} : gg^{-1} = g^{-1}g = e$

If $gh = hg \forall g, h \in G$, we call G abelian.

Examples 5.2

i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are all groups (abelian)

In fact $(R, +)$ for any ring R is an abelian group, ie. $(\mathbb{Z}_n, +)$, $(R[x], +)$

ii) Units of R : $R^* = \{r \in R \mid r^{-1} \text{ exists}\}$ is a group wrt multiplication.

$$\mathbb{Z}^* = \{\pm 1\}, F^* = F - \{0\}.$$

iii) (R, \cdot) is not a group $0 \in R$ has no multiplicative inverse.

iv) $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is a group wrt multiplication

• Multiplication is associative

• $1 \in S$

• z^{-1} has abs $|z| = 1$

Subgroup $G = \left\{ e^{2\pi i \frac{k}{n}}; k=0, \dots, n-1 \right\} \cong \mathbb{Z}_n$

[[$1 \in G, e^{2\pi i \frac{k}{n}} \cdot e^{2\pi i \frac{l}{n}} = e^{\frac{2\pi i}{n}(k+l)}$: n^{th} roots of unity.

Consider rotations in \mathbb{R}^2 which map the n -gon to itself. These form a group.

All the elements are of the form rotation by $\frac{2\pi}{n}, k=0, \dots, n-1 \cong \mathbb{Z}_n$

$C_n = \text{rotations of } n\text{-gon} \cong \mathbb{Z}_n$]]

v) $r = \text{rotation by } \frac{2\pi}{n} : r^n = e$ (identity element)

In addition, consider all reflections through an axis which preserve the n -gon: n reflections.

Together, these form a symmetry group D_n : dihedral group. $\#D_n = 2n$

s is reflection in y axis: $s^2 = e$

What if we apply srs ? $srs = r^{-1} = r^{n-1}$

All elements in D_n can be written as $r^k, k=0, \dots, n-1$

$$sr^k, k=0, \dots, n-1$$

D_n is the group generated by r and s (everything is a word in r, s), with relations

$$r^n = e, s^2 = e, srs = r^{n-1} = r^{-1}$$

RTP

sr^k is a reflection need $(sr^k)^2 = (sr^k)(sr^k) = e$

Indeed, $sr^k sr^k = srssr^{k-1} sr^k = r^{-1} sr^{k-1} r^k$

$$= r^{-1} srssr^{k-2} sr^k = r^{-2} sr^{k-2} sr^k = \dots = r^{-k} sr^k = r^{-k} r^k = e$$

Not abelian.

vi) Matrix Groups

• $GL_n(\mathbb{R}) = (n \cdot n \text{ invertible matrices with entries in } F) \text{ (with multiplication)}$

$$= \{ g \in M_n(F) \mid \det(g) \neq 0 \}$$

• $SL_n(F) = \{ g \in M_{n \times n}(F) \mid \det(g) = 1 \}$

• $SO(2) = \{ \text{rotations in the plane} \}$

$$\left\{ g \in M_2(\mathbb{R}) \mid g \cdot g^t = I_2, \det(g) = 1 \right\} = \left\{ \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} \mid \theta \in [0, 2\pi] \right\}$$

• $O(2) = \{ g \in M_2(\mathbb{R}) \mid g \cdot g^t = I_2 \}$ (also reflections)

vii) $S_n = \text{group of permutations on } n \text{ letters.}$

Notation

+ is reserved for abelian groups

* in general

Cartesian Products

G, H groups $G \times H$ is also a group

Lemma 5.3 Subgroup Criterion

Let G be a group, H a subset. H is in fact a subgroup if

- i) $h_1, h_2 \in H, h_1 h_2 \in H$
- ii) for $h \in H, h^{-1} \in H$

Definition 5.4 Group Homomorphism

A map $\Phi : G \rightarrow H$ of 2 groups is called a group homomorphism if $\Phi(gg') = \Phi(g)\Phi(g')$

Φ is called an isomorphism, if Φ is a bijection.

Examples 5.5

i) $\mathbb{Z}^* = \{ \pm 1 \} \cong \mathbb{Z}_2 = \{0, 1\}$

ii) Any ring homomorphism $\Phi : R \rightarrow S$ is in particular a group homomorphism $(R, +) \rightarrow (S, +)$

iii) CRT $\mathbb{Z}_n \cong \mathbb{Z}_n \times \mathbb{Z}_m$ if $\gcd(m, n) = 1$

iv) If $\gcd(m, n) > 1$, then $\mathbb{Z}_{mn} \not\cong \mathbb{Z}_n \times \mathbb{Z}_m$

Lemma 5.6

Let $\Phi : G \rightarrow G'$ be a group homomorphism. then:

- i) $\text{Ker}(\Phi) = \{g \in G \mid \Phi(g) = e\}$
- ii) $\Im(\Phi)$ is a subgroup of G'

Lemma 5.7

A group homomorphism Φ is injective $\Leftrightarrow \text{Ker}(\Phi) = e$

Proof 5.6

i) Let $g, g' \in \text{Ker}(\Phi)$

Then $\Phi(gg') = \Phi(g)\Phi(g') = e \cdot e = e \Rightarrow gg' \in \text{Ker}(\Phi)$

ii) Let $h, h' \in \Im(\Phi)$

ie. $h = \Phi(g), h' = \Phi(g')$

Then $hh' = \Phi(g)\Phi(g') = \Phi(gg')$ Inverse the same

Proof 5.7

Same proof as before

Remarks 5.8

• G is a group

• $(gh)^{-1} = h^{-1}g^{-1} \quad [(gh)(h^{-1}g^{-1}) = e]$

• Cancellation: $gh_1 = gh_2 \Rightarrow h_1 = h_2$
 $h_1g = h_2g \Rightarrow h_1 = h_2$

• Multiplying from the left/right permutes the elements of G , ie is a multiplication of a group, each element occurs exactly once in each row/column.

• If $gH = H$ for all $g \in G$ (H subgroup) then actually, $gHg^{-1} = H$

Proof

Need $h \in gHg^{-1} \forall g \in G$; know that $g^{-1}hg \in H$, replacing g by g^{-1} then

$g(g^{-1}hg)g^{-1} \in gHg^{-1} = H$

Definition 5.9

Let $g \in G$. The order of g " $ord(g)$ " is the smallest positive integer n such that $g^n = e$

If g is written additively: $ng = 0$

If no such n exists, $ord(g) = \infty$

The group generated by g is $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$

A group generated by one element is called cyclic.

Eg. $\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}_n = \langle 1^- \rangle$

$\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

Lemma 5.10

$\# \langle g \rangle = ord(g)$

Proof

Let $ord(g) = n$. Then $g^n = e$, but g, g^2, \dots, g^{n-1} are all different from e , and all different from each other. So $\# \langle g \rangle = n$

For $m > n$, write $m = kn + l$, $l < n$. Then

$g^m = g^{kn+l} = (g^n)^k \cdot g^l = e^k \cdot g^l = g^l$. Already part of the list.

Theorem 5.11 (Lagrange)

Let G be a finite group, H be a subgroup

Then $\# H \mid \# G$ (so groups with prime orders have no subgroups)

In particular, by 5.10, $ord(g) \mid \# G \forall g \in G$

Corollary 5.12 (Fermat's Little Theorem)

Let $a \in \mathbb{Z} : gcd(a, p) = 1$ for some prime p .

Then $a^{p-1} \equiv 1 \pmod{p}$

or, for all $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$

Proof

$a^- \in \mathbb{Z}_p^*$, $ord(a^-) = n$ with $n \mid \#\mathbb{Z}_p^* = p-1$

So $p-1 = n \cdot l$

Then $(a^-)^{p-1} = (a^-)^{n \cdot l} = ((a^-)^n)^l = (1^-)^l = 1^-$

Corollary 5.13

Let G be a group of order p a prime. Then G is cyclic and $G \cong \mathbb{Z}_p$

Proof

Take $g \in G$ not the neutral element. So $ord(g) = p$ and $\langle g \rangle = G$

Furthermore, the map $G \rightarrow \mathbb{Z}_p : g^n \rightarrow n^-$ is an isomorphism.

List of groups with small order:

#1 $\{e\}$

#2 $\mathbb{Z}_2 \cong \mathbb{Z}^*$

... list of groups...

Definition 5.14

Cosets: Let $H \subseteq G$ be a subgroup $g \in G$

Left coset: $gH = \{gh : h \in H\}$

Right coset: $Hg = \{hg : h \in H\}$

For G abelian, written additively this is $g + H = H + g$

Lemma 5.15

If H is normal in G . ie $gH^{-1}g = H \forall g$, then $gH = Hg$. So left coset=right coset

Examples

$G = D_3$

$$r^3 = e = s^3, srs = r^2 = r^{-1}$$

elements: e, r, r^2, sr, sr^2

a) $H = \langle s \rangle = \{e, s\}$

$$eH = H$$

$$sH = \{s, s^2\} = \{s, e\} = H$$

$$rH = \{r, rs\} = \{r, sr^2\}$$

$$r^2H = \{r^2, r^2s\} = \{r^2, sr\}$$

$$srH = \{sr, srs\} = \{sr, r^2\} = r^2H$$

$$sr^2H = \{sr^2, sr^2s\} = \{sr^2, r\} = rH$$

$$He = H$$

$$Hs = H$$

$$Hr = \{r, sr\} \neq rH \Rightarrow H \text{ is not normal}$$

b) $H = \langle r \rangle = \{e, r, r^2\}$

$$eH = H = rH = r^2H$$

$$sH = \{s, sr, sr^2\} = srH = sr^2H$$

Lemma 5.16

i) $gH = Hg = H \Leftrightarrow g \in H$

ii) $g_1H = g_2H \Leftrightarrow g_2^{-1}g_1 \in H$

$$Hg_1 = Hg_2 \Leftrightarrow g_2g_1^{-1} \in H$$

iii) $ghH = gH$

$$Hhg = Hg$$

iv) Cosets either coincide or are disjoint.

Proof

i) If $g \in H$, then $gH = Hg = H$ is clear, by closedness.

If $gH = H$, in particular $\exists h \in H$ s.t. $gh = e \in H$. Then $h = g^{-1} \in H$, so $g \in H$.

ii) $g_1H = g_2H \Leftrightarrow g_2^{-1}g_1 \in H$ (by (i))

$$\Leftrightarrow g_2^{-1}g_1H$$

$$\text{Same } Hg_1 = Hg_2$$

iii) Clear $hH = Hh = H$

iv) Assume $g_1H \cap g_2H \neq \emptyset$ need to show $g_1H = g_2H$

So can find $g \in H$ s.t. $g_1h_1 \in g_1H$, $g_1h_1 = g = g_2h_2 \in g_2H$

i.e. $g_1h_1 = g_2h_2$; $g_2^{-1}g_1 = h_2h_1^{-1} \in H$

By (ii) $g_1H = g_2H$ Same for right cosets.

Lemma 5.17

If $\#H < \infty$, then $\#gH = \#H = \#Hg$

Proof

$gH = \{gh; h \in H\}$

So $\#gH \leq \#H$

And the order would be smaller if $gh_1 = gh_2$ for some $h_1, h_2 \in H$

But by cancellation, $h_1 = h_2$, so the element $gh, h \in H$ are all different.

Proof of Lagrange's Theorem

We can decompose G into left (or right) cosets. $G = H \cup g_1H \cup g_2H \cup \dots \cup g_nH$ with all these cosets disjoint. (Proceed inductively to find new cosets, process must end once $(\# \text{ cosets}) \times \#H \geq \#G$)

So $\#G = \#H + \#g_1H + \#g_2H + \dots + \#g_nH$

(by Lemma 5.17) $= \#H + \#H + \dots + \#H$ [$n + 1$ times] $= (n + 1)\#H$

So the order of H divides the order of G .

Corollary 5.18

$\#$ of left/right cosets of H in $G = \frac{\#G}{\#H}$