Name: Tuan Pham
ID : 4652218

General Algebra
Homework #1

~~27/30~~
60/60

10 (8) Let G be a finite abelian group which is not cyclic. Prove that there is a prime number p and a subgroup H of G with $H \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Proof We start the proof by proving the following lemma

(*) [If G is an abelian group of order n and p is a prime divisor of n, then G has an element of order p.]

Proof of the lemma. Let $G = \{x_1, \dots, x_n\}$ and let h_i be the order of x_i. We know that each $\langle x_i \rangle$ is a cyclic group. Thus if p divides some h_i, we will find a subgroup in $\langle x_i \rangle$ of order p, whose generators are of order p. Now consider the case in which p divides none of h_i. ~~Now~~ Define the map

$$\phi : \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle \longrightarrow G$$
$$(x_1^{\alpha_1}, x_2^{\alpha_2}, \dots, x_n^{\alpha_n}) \longmapsto x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

Then ϕ is well-defined and surjective. We have

$$\phi\left((x_1^{\alpha_1}, x_2^{\alpha_2}, \dots, x_n^{\alpha_n})(x_1^{\beta_1}, x_2^{\beta_2}, \dots, x_n^{\beta_n})\right) = \phi\left(x_1^{\alpha_1+\beta_1}, \dots, x_n^{\alpha_n+\beta_n}\right)$$
$$= x_1^{\alpha_1+\beta_1} x_2^{\alpha_2+\beta_2} \cdots x_n^{\alpha_n+\beta_n}$$
$$= \left(x_1^{\alpha_1} x_1^{\beta_1}\right)\left(x_2^{\alpha_2} x_2^{\beta_2}\right) \cdots \left(x_n^{\alpha_n} x_n^{\beta_n}\right)$$
$$\underline{\underline{G \text{ abelian}}} \quad \left(x_1^{\alpha_1} \cdots x_n^{\alpha_n}\right)\left(x_1^{\beta_1} \cdots x_n^{\beta_n}\right)$$
$$= \phi\left(x_1^{\alpha_1}, \dots, x_n^{\alpha_n}\right)\phi\left(x_1^{\beta_1}, \dots, x_n^{\beta_n}\right)$$

Thus ϕ is a group homomorphism. Thus

$$G = \mathrm{Im}\phi \cong \langle x_1 \rangle \times \cdots \times \langle x_n \rangle / \ker\phi$$

and consequently $|G|$ divides $|\langle x_1 \rangle \times \cdots \times \langle x_n \rangle|$, or n divides $h_1 \cdots h_n$. Since p divides n, p also divides $h_1 \cdots h_n$. Since p is prime, p must divide one of the h_i's, which is a contradiction. ▨

The next step is to prove that ~~G contains a subgroup H of order p^2~~ $n = |G|$ has a divisor of the form p^2 where p is a prime number.

Proof of the claim. Suppose by contradiction that n has no square divisor. Then $n = p_1 \cdots p_k$ where $p_1 < \cdots < p_k$ and each p_i's is prime. Then by Lemma (*), G has an element a_1 of order p_1, an element a_2 of order p_2, ..., and an element of order p_k. Consider the following map

$$\psi : \langle a_1 \rangle \times \cdots \times \langle a_k \rangle \longrightarrow G$$
$$(a_1^{\alpha_1}, \ldots, a_k^{\alpha_k}) \longmapsto a_1^{\alpha_1} \cdots a_k^{\alpha_k}$$

for every $0 \le \alpha_i \le p_i - 1$. Again, ψ is well-define and is a group homomorphism. We will show that ψ is injective by showing $\ker\psi = \{e\}$. Suppose that $\psi(a_1^{\alpha_1}, \ldots, a_k^{\alpha_k}) = a_1^{\alpha_1} \cdots a_k^{\alpha_k} = e$. Then we put $h = p_2 \cdots p_k$ and we have $e = (a_1^{\alpha_1} \cdots a_k^{\alpha_k})^h = a_1^{\alpha_1 h} a_2^{\alpha_2 h} \cdots a_k^{\alpha_k h}$. For each $i \ge 2$, p_i divide h. Thus $a_i^{\alpha_i h} = e$. Thus $e = a_1^{\alpha_1 h}$, which means p_1 divides $\alpha_1 h$. However, since p_1 does not divide h, it divides α_1. Thus

$$(a_1^{\alpha_1}, \dots, a_k^{\alpha_k}) = (e, e \dots, e)$$

And so ψ is injective. By the first isomorphism theorem, we have

$$\operatorname{Im}\psi \cong (\langle a_1\rangle \times \cdots \times \langle a_k\rangle)/\ker\psi \cong \langle a_1\rangle \times \cdots \times \langle a_k\rangle,$$ which has $p_1 \cdots p_k = n$ elements. Thus $\operatorname{Im}\psi = G$ and ψ is therefore an isomorphism. ~~Since the group $\langle a_1\rangle \times \cdots \times \langle a_k\rangle$ is abelian, G must also be abelia~~ $G \cong \langle a_1\rangle \times \cdots \times \langle a_k\rangle$

~~and $G = \{a_1^{\alpha_1} \cdots a_k^{\alpha_k} : 0 \le \alpha_i \le p_i - 1\}$~~. Since $p_1, \dots, p_k$ are pairwise prime to each other, the group $\langle a_1\rangle \times \cdots \times \langle a_k\rangle$ is cyclic, and so is G. This is a contradiction!

The next step is to show that G has a subgroup H of order p^2, which is not cyclic.

Proof of the claim. From the preceding claim, n must have a square divisor. Thus we can write $n = p^2 r$ where p is a prime number and $r \ge 1$. By the lemma (*), G has an element of order p, say a. We put $N = \langle a\rangle$. Since G is abelian, G/N is also a group of and

$$|G/N| = \frac{|G|}{|N|} = \frac{p^2 r}{p} = pr$$

Thus the order of G/N divides p. By ~~Lemma~~ Lemma (*) again, G/N must have an element of order p, called bN.

4

Put $K = \{N, bN, \dots, b^{p-1}N\}$. Then K is a subgroup of G/N. Consider the canonical homomorphism $\pi : G \to G/N$. Put $H = \pi^{-1}(K)$.

Then $H = \{x \in G : \pi(x) \in K\}$

$= \{x \in G : xN \in K\}$

$= \{x \in G : xN = b^j N \text{ for some } 0 \le j \le p-1\}$

$= \{x \in G : x \in b^j N \text{ for some } 0 \le j \le p-1\}$

$= \{x \in G : x = b^j a^i \text{ for some } 0 \le i, j \le p-1\}$

$= \{b^j a^i : 0 \le i, j \le p-1\}$

$= \langle b \rangle \langle a \rangle = \langle a \rangle \langle b \rangle$ because G is abelian.

Consider the map

$$\tilde{\phi} : \langle a \rangle \times \langle b \rangle \longrightarrow H$$
$$(a^i, b^j) \longmapsto a^i b^j$$

Again $\tilde{\phi}$ is well-defined and is a homomorphism (since H is abelian). Moreover $\tilde{\phi}$ is surjective. Let $(a^i, b^j) \in \ker \tilde{\phi}$, then $a^i b^j = e$. Thus $a^i = b^{-j}$. Thus $b^{-j} \in \langle a \rangle N$. Thus $j = 0$ and therefore $a^i = e$. Thus $i = 0$. Hence $\ker \tilde{\phi} = \{e\}$ and $\tilde{\phi}$ is injective. Thus, $H \cong \langle a \rangle \times \langle b \rangle$, which has p^2 element. Note that H is not cyclic because it has no element of order p^2. Instead, every element of H, except e, is of order p.

The last step is to show that $H \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. This is straightforward since $\langle a \rangle, \langle b \rangle \cong \mathbb{Z}/p\mathbb{Z}$.

(3) Let G be a group, H a subgroup in G and let N_H be the normalizer of H.

(a) Show that if $K < G$ is a subgroup such that H is normal in K the $K \subset N_H$, i.e. N_H is the largest subgroup of G in which H is normal.

(b) If K is a subgroup contained in N_H, then KH is a group and H is a normal subgroup in KH.

(c) If G is finite and $K \subset N_H$ then

$$|KH| = \frac{|H||K|}{|H \cap K|}$$

Proof

(a) By definition, $N_H = \{x \in G : xHx^{-1} = H\}$. Let $K < G$ be such that H is normal in K. Then $xyx^{-1} \in H \ \forall y \in H, x \in K$. Thus $xHx^{-1} \subset H$ for every $x \in K$. We see that if x is replaced by x^{-1}, then $x^{-1}Hx \subset H$ or equivalently $H \subset xHx^{-1}$. Therefore $xHx^{-1} = H \ \forall x \in K$, and hence $K \subset N_H$. By the definition of N_H, H is normal in N_H if we can show that N_H itself is a subgroup. Now we'll show that N_H is a subgroup:

* $x, y \in N_H \overset{?}{\Rightarrow} xy \in N_H$:

We have $xHx^{-1} = H$ and $yHy^{-1} = H$. Then

6

$$H = xHx^{-1} = x(yHy^{-1})x^{-1} = xyH(xy)^{-1}$$

Thus $xy \in N_H$.

* $x \in N_H \overset{?}{\Longrightarrow} x^{-1} \in N_H$

Since $H = xHx^{-1}$, we can multiply both sides by x to the right and obtain $Hx = xH$. Next, multiply both sides by x to the left, we get

$$x^{-1}Hx = H$$

or equivalently $(x^{-1})H(x^{-1})^{-1} = H$. Thus $x^{-1} \in N_H$.

(b) Suppose that $K < N_H$. First, we'll show that KH is a group:

• let $x, y \in KH$. Show that $xy \in KH$?

Since $x \in KH$, there exist $k_1 \in K$ and $h_1 \in H$ such that $x = k_1 h_1$. Similarly there exist $k_2 \in K$ and $h_2 \in H$ such that $y = k_2 h_2$. Then

$$xy = k_1 h_1 k_2 h_2 = k_1 k_2 \underbrace{(k_2^{-1} h_1 k_2)}_{\in H} h_2 \in KKHH = KH$$

• Let $x \in KH$. Show that $x^{-1} \in KH$?

Since $x \in KH$, there exists $h \in H$, $k \in K$ such that $x = hk$. We have

$$x^{-1} = k^{-1}h^{-1} = \underbrace{k^{-1}}_{\in K}\underbrace{kh^{-1}k^{-1}}_{\in H} \in KH$$

(c) Next, we'll show that H is normal in KH. Take $h \in H$ and $x \in KH$, we'll show that $xhx^{-1} \in H$. There exists $a \in K$ and $b \in H$ such that $x = ab$. We have

$$xhx^{-1} = a\underbrace{bhb^{-1}}_{h'}a^{-1} = a\underbrace{h'}_{\in H}a^{-1} \in H \text{ because } a \in K \subset N_H.$$

(c) The identity which we have to prove

$$|KH| = \frac{|H||K|}{|H \cap K|}$$

is equivalent to $$\frac{|KH|}{|H|} = \frac{|K|}{|H \cap K|}$$

we'll achieve it if we ~~can prove~~ have the isomorphism $KH/H \approx K/(H \cap K)$.

From (b), we know that H is normal in KH/H. Thus KH/H is a group.

We have two more things to prove:

1) $H \cap K$ is normal in K

2) $KH/H \approx K/(H \cap K)$

Prove 1) For every $x \in K, y \in H \cap K$, we have $xyx^{-1} \in K$ and

$xyx^{-1} \in xHx^{-1} = H$. Thus $xyx^{-1} \in H \cap K$.

Prove 2) Consider the following map $f: K \to KH/H$
$x \mapsto xH$

Then f is well-define since $xH = (xe)H \in KH/H$. Then

$$f(x)f(y) = (xH)(yH) = (xy)H = f(xy)$$

Thus f is a group homomorphism. Moreover, for each $y \in KH$, there exists

$k \in K$ and $h \in H$ such that $y = kh$. Thus $yH = khH = kH = f(k)$.

Therefore f is a surjection. By the first isomorphism theorem, we have $K/\ker f \simeq (KH/H)$. We'll find $\ker f$. Let $x \in \ker f$. Then $f(x) = H$, or $xH = H$. Thus $x \in H$. Moreover, $x \in \ker f \subset K$. Then $x \in K \cap H$. Conversely, take $x \in K \cap H$. Then $f(x) = xH = H$. Thus $\ker f = K \cap H$. Therefore,

$$K/(K \cap H) \simeq (KH)/H$$

Now that we have this isomorphism between 2 finite groups, their cardinality must be the same, i.e. $|K/(K \cap H)| = |(KH)/H|$. By Lagrange's theorem,

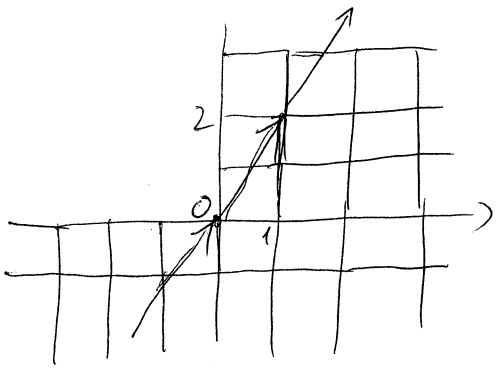
$$|K/(K \cap H)| = \frac{|K|}{|K \cap H|} \quad \text{and} \quad |KH/H| = \frac{|KH|}{|H|}$$

and we get the result.

① Find all subgroups of the additive group $\mathbb{Z} \times \mathbb{Z}$. (2 sgor pg. 23)

Proof We will use picture to have some ideas. But first, we should exclude the trivial cases where $H = \{0\}$ or $H = \mathbb{Z} \times \mathbb{Z}$.

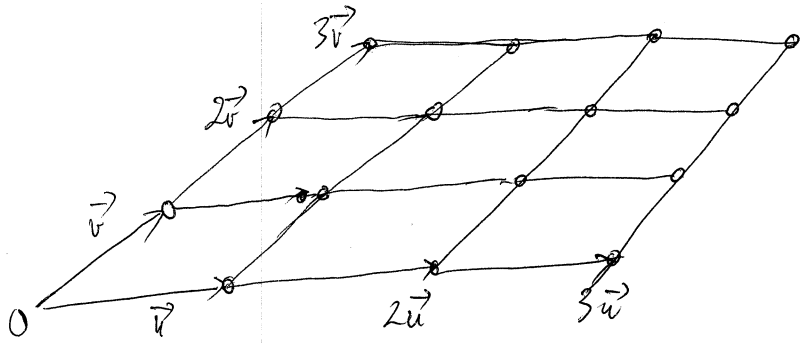
If H is just one line, that is the line generated by one element $\vec{u} = (a, b)$



Then $H = \langle \vec{u} \rangle = \{n(a,b) : n \in \mathbb{Z}\}$

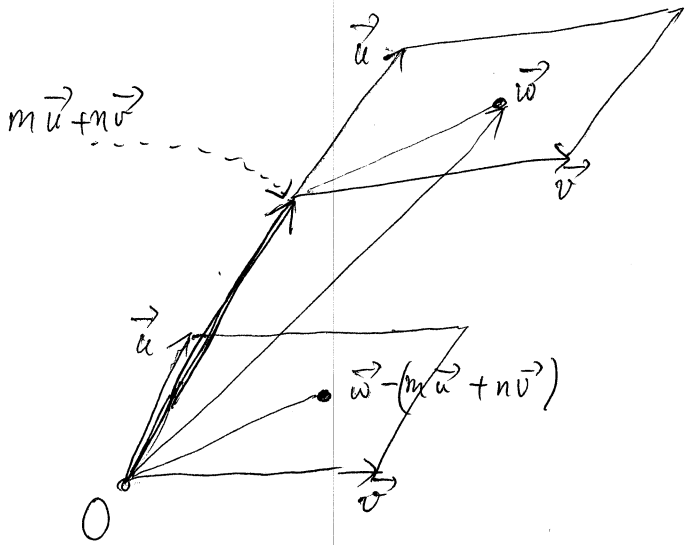
We say H is generated by only one element (cyclic, or "1-dimensional")

If H has more than one line (2-dimensional) then there are two vector $\vec{u}$ and $\vec{v}$ in H which are in general position.



What we are drawing is the subgroup of $\mathbb{Z}\times\mathbb{Z}$ generated by $\{\vec{u},\vec{v}\}$. It looks like a roof with parallelogram tiles. And we want H to be exactly this group. There are two problems with this claim:

1) What if there exists some element of H that lies outside of the parallelogram grids?



Suppose that $\vec{w}$ lies inside a parallelogram "aligned" at $m\vec{u}+n\vec{v}$. Then $\vec{w}-(m\vec{u}+n\vec{v})$ must lie in the parallelogram made by $\vec{u}$ and $\vec{v}$ at the origin 0. Then if we can choose in advance $\vec{u}$ and $\vec{v}$ such that this parallelogram

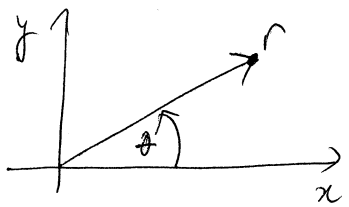
contains no point of H inside, then everything will be OK, i.e. $H = \Gamma(\{\vec{u}, \vec{v}\})$.

2) How to choose $\vec{u}$ and $\vec{v}$ satisfying such a condition?

We will trace backward to make everything rigorous. We will follow the following steps:

Step 1 (introduce an order on $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$ to facilitate the choice of $\vec{u}$ and $\vec{v}$)

We know that on $(\mathbb{Z}\times\mathbb{Z})\setminus\{0\}$, every point corresponds uniquely and injectively to a pair (r,θ) where $r\in\mathbb{R}, r>0, 0\le\theta<2\pi$ called the polar coordinate of that point.



Since two pairs (r_1,θ_1) and (r_2,θ_2) can be compared by using the lexicographical order, we can define an order on $(\mathbb{Z}\times\mathbb{Z})\setminus\{0\}$ as follow

$$\vec{u} \le \vec{v} \iff (r_{\vec{u}}, \theta_{\vec{u}}) \le (r_{\vec{v}}, \theta_{\vec{v}})$$

$$\iff \left(r_{\vec{u}} < r_{\vec{v}}\right) \text{ or } \begin{cases} r_{\vec{u}} = r_{\vec{v}} \\ \theta_{\vec{u}} \le \theta_{\vec{v}} \end{cases}$$

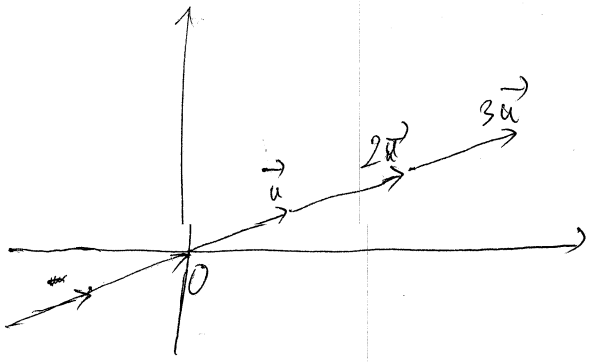
Then $(\mathbb{Z}\times\mathbb{Z}\setminus\{0\}, \le)$ is a totally-ordered set. Then we claim

Claim: $(\mathbb{Z}\times\mathbb{Z}\setminus\{0\}, \le)$ is a well-ordered set, i.e. every nonempty subset has a least element.

Step 2 Now we are ready ~~to~~ to trace the problem forward. Here are the substeps:

(i) $\{0\}$ is obviously a subgroup of $\mathbb{Z}\times\mathbb{Z}$

(ii) If $H\neq\{0\}$, then $H\setminus\{0\}$ is a nonempty subset of $(\mathbb{Z}\times\mathbb{Z})\setminus\{0\}$. Thus it has a least element $\vec{u}=(a,b)$.



Then $H\supset\langle\vec{u}\rangle=\mathbb{Z}\vec{u}=\{n(a,b):n\in\mathbb{Z}\}$

Incase $H\setminus\langle\vec{u}\rangle=\phi$ then $H=\langle\vec{u}\rangle$.

In this case $H\simeq\mathbb{Z}$. However, we won't stop here because we still don't know how to generate a group H of this form. Let $\mathcal{E}_1$ be the family of all subgroups of $\mathbb{Z}\times\mathbb{Z}$ that all gerenerated by one element (cyclic group). Then we claim the map

$$\phi_1:\mathcal{E}_1\longrightarrow X_1=\{\vec{u}\in(\mathbb{Z}\times\mathbb{Z})\setminus\{0\}:0\le\theta_{\vec{u}}<\pi\}$$
$$H\longmapsto\vec{u}=\min(H\setminus\{0\})$$

to be a bijection.

(iii) In this case, $H\setminus\langle\vec{u}\rangle\neq\phi$. Then $H\setminus\langle\vec{u}\rangle$ is a nonempty subset of $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}$. Thus there exists $\vec{v}=\min(H\setminus\mathbb{Z}\vec{u})$. We denote $\vec{v}=(c,d)$.

Since $\vec{u}$ and $\vec{v}$ are independent,

$$D = \det(\vec{u}, \vec{v}) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \neq 0$$

We have 2 claims:

1) $H = \langle \vec{u}, \vec{v} \rangle$, which means two elements are enough to generate H.

2) If we denote $\mathcal{E}_2$ to be the family of all subgroup of $\mathbb{Z}\times\mathbb{Z}$ that are generated by two elements, then the following map

$$\phi_2 : \mathcal{E}_2 \to X_2 = \{(\vec{u}, \vec{v}) : \vec{u}, \vec{v} \in (\mathbb{Z}\times\mathbb{Z}) \setminus \{0\}, \overbrace{0 \le \theta_{\vec{u}}, \theta_{\vec{v}} < \pi}, \det(\vec{u}, \vec{v}) \neq 0, \vec{u} \overbrace{< \vec{v}}^{\angle \vec{u} \pm \vec{v}}\}$$

~~is a b~~ $H \mapsto (\vec{u}, \vec{v})$ such that $\vec{u} = \min H \setminus \{0\}$ and $\vec{v} = \min(H \setminus \langle u \rangle)$, is a bijection.

~~Furthermore, we see that X is just bijective to the set by natural correspondence~~

~~$$Y = \{\{\vec{u}, \vec{v}\} : \vec{u}, \vec{v} \in (\mathbb{Z}\times\mathbb{Z}) \setminus \{0\}, \det(\vec{u}, \vec{v}) \neq 0, 0 \le \theta_{\vec{u}}, \theta_{\vec{v}} < \pi\}$$~~

~~Thus we can view ϕ_2 as a map from $\mathcal{E}_2$ onto Y, which is bijective.~~

Conclusion A subgroup H of $\mathbb{Z}\times\mathbb{Z}$ will fall into one of the following types:

1) $H = \{0\}$

2) $H = \langle \vec{u} \rangle \simeq \mathbb{Z}$, where $\vec{u}$ is characterized by $\vec{u} = \min(H \setminus \{0\})$

3) $H = \langle \vec{u}, \vec{v} \rangle \simeq \mathbb{Z}\times\mathbb{Z}$, where $\vec{u}$ and $\vec{v}$ are characterized by $\vec{u} = \min(H \setminus \{0\})$, $\vec{v} = \min(H \setminus \langle u \rangle)$.

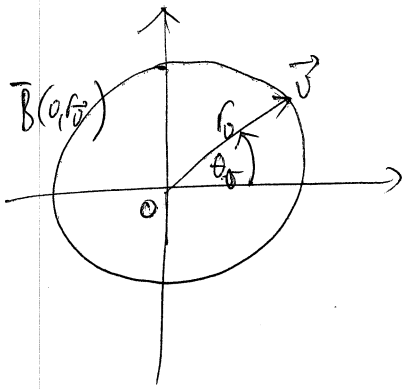
Details of proofs

Step 1: Prove the claim that $(\mathbb{Z}\times\mathbb{Z})\setminus\{0\}$ is well-ordered.

Let A be a nonempty subset of $(\mathbb{Z}\times\mathbb{Z})\setminus\{0\}$. We'll show that A has a least element. Take $\vec{v}\in A$. Then the set $\overline{B}(0,r_{\vec{v}})\cap A$ is finite,

~~$B=\{\vec{u}\in(\mathbb{Z}\times\mathbb{Z})\setminus\{0\} : r_{\vec{u}}\leq r_{\vec{v}}$~~

where $\overline{B}(0,r_{\vec{v}})$ is the closed ball center at 0, radius $r_{\vec{v}}$ in $\mathbb{R}^2$. Moreover, the ~~min~~ $\min A$ exists if and only if $\min(\overline{B}(0,r_{\vec{v}})\cap A)$ exists. We know that every totally-ordered finite set has a least element, whence the proof completes.



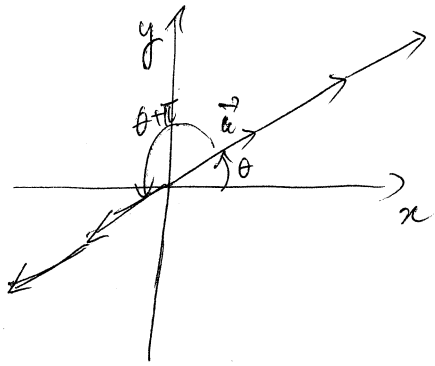
$0\leq\theta_{\vec{u}}<\pi$ because otherwise we have $-\vec{u}<\vec{u}$

Step 2: (ii) We show that the map $\phi_1: \mathcal{E}_1 \longrightarrow$ ~~$\mathbb{Z}\setminus\{0\}$~~ $X_1=\{\vec{u}\in(\mathbb{Z}\times\mathbb{Z})\setminus\{0\} : 0\leq\theta_{\vec{u}}<\pi\}$

$$H \longmapsto \vec{u}=\min(H\setminus\{0\})$$

is a bijection. If $\phi_1(H_1)=\vec{u}=\phi(H_2)$ then $H_1=H_2=\langle\vec{u}\rangle$. Thus ϕ_1 is injective. For each $\vec{u}\in\mathbb{Z}\setminus\{0\}$, we put $H=\langle\vec{u}\rangle=\{n\vec{u} : n\in\mathbb{Z}\}$. Then we show that $\vec{u}=\min(H\setminus\{0\})$.

14



For $n \geq 2$, the length of vector $n\vec{u}$ is greater than that of $\vec{u}$, i.e. $r_{n\vec{u}} > r_{\vec{u}}$. Thus $\vec{u} < n\vec{u}$. The same reason is for $n \leq -2$.

We only need to show that $\vec{u} < -\vec{u}$.

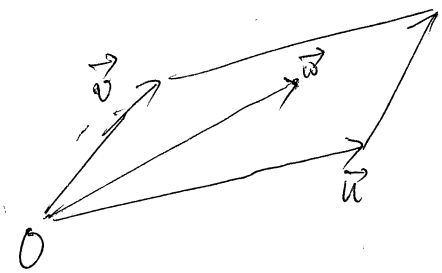
Since $r_{\vec{u}} = r_{-\vec{u}}$, we have to compare the θ's. Since $0 \leq \theta_{\vec{u}} < \pi$, we have $\theta_{-\vec{u}} = \theta_{\vec{u}} + \pi > \theta_{\vec{u}}$. Thus $\vec{u} < -\vec{u}$. Therefore $\vec{u} = \min(H \setminus \{0\})$ and ϕ_1 is a bijection.

(iii). Proof of claim 1)

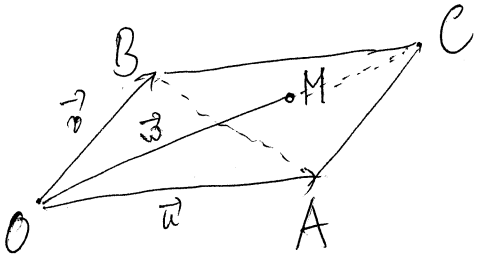
We need to prove that there's no element of H inside (or on edges) of the parallelogram made by $\vec{u}$ and $\vec{v}$ ~~conte~~ originated at O, where

$$\vec{u} = \min(H \setminus \{0\})$$

$$\vec{v} = \min(H \setminus \langle \vec{u} \rangle)$$



Suppose that there exists $\vec{w} \in H$ that lies in the parallelogram. Then the point M (corresponding to $\vec{w}$) is either in $\triangle OAB$ or $\triangle ABC$.



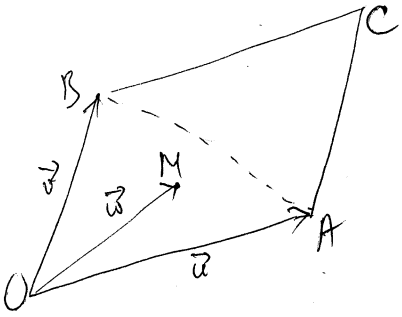
we have $\overrightarrow{OM} = \vec{w} \in H$

$$\overrightarrow{CM} = \overrightarrow{OM} - \overrightarrow{OC} = \vec{w} - (\vec{u} + \vec{v}) \in H$$

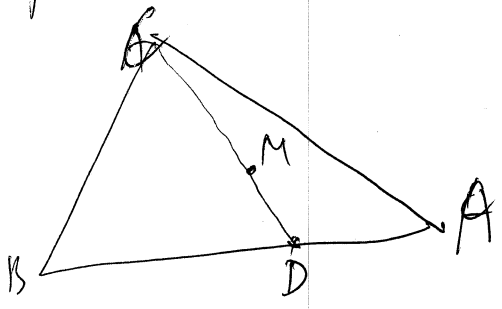
In case that $M \in \triangle ABC$, if we can show that

$CM \le \max\{BC, AC\}$ (which is equal $AC = \vec{v}$)

then we'll have a contradiction to the definition of $\vec{u}$ and $\vec{v}$ (i.e. we can choose $\vec{CM} = \vec{w} - (\vec{u}+\vec{v}) = \min H\setminus\langle\vec{u}\rangle$ instead of $\vec{v}$). The case $M \in \Delta OAB$ is completely the same since we have $OM \le \max\{OA, OB\}$.



Now we'll show that $CM \le \max\{BC, AC\}$ for arbitrary triangle ABC and a point M inside it.



Let D be the intersection of the lines CM and the segment AB. Then $CM \le CD$. Since $\widehat{CDB} + \widehat{CDA} = 180°$, one of them is not less than $90°$, say $\widehat{CDA}$. The triangle CDA has an obtuse angle at D. Thus $AC \ge CD$, which completes the proof.

Proof of claim 2

$\phi_2 : \mathcal{E}_2 \longrightarrow X_2 = \{(\vec{u},\vec{v}) : \vec{u},\vec{v} \in (\mathbb{Z}\times\mathbb{Z})\setminus\{0\},\ 0 \le \theta_{\vec{u}}, \theta_{\vec{v}} < \pi,\ \det(\vec{u},\vec{v}) \ne 0,\ \vec{u} < \vec{v} < \vec{u}+\vec{v}\}$

$H \mapsto (\vec{u},\vec{v})$ where $\vec{u} = \min(H\setminus\{0\})$, $\vec{v} = \min(H\setminus\langle\vec{u}\rangle)$

$\vec{v} < \vec{u}+\vec{v}$ since otherwise we can choose $\vec{u}+\vec{v} = \min(H\setminus\langle\vec{u}\rangle)$ instead of $\vec{v}$

If $H_1, H_2 \in \mathcal{E}_2$ satisfy $\phi_2(H_1) = \phi_2(H_2) = (\vec{u}, \vec{v}) \in X_2$, then $\vec{u}, \vec{v} \in H_1, H_2$ which are "linearly independent". Since H_1 and H_2 are generated by only two elements, we have $H_1 = H_2 = \langle \vec{u}, \vec{v} \rangle$. Thus ϕ_2 is injective.

Let $(\vec{u}, \vec{v}) \in X_2$, i.e. $0 \le \theta_u, \theta_v < \pi$, $\det(\vec{u}, \vec{v}) \neq 0$, $\vec{u} < \vec{v} < \vec{u} \pm \vec{v}$. Put $H = \langle \vec{u}, \vec{v} \rangle$.

Then $H \in \mathcal{E}_2$ since H is generated by two ~~elements~~ ("independent") elements.

$H = \{ m\vec{u} + n\vec{v} \; ; \; m, n \in \mathbb{Z} \}$. We'll show that $\vec{u} = \min(H \setminus \{0\})$.

We have $|m\vec{u} + n\vec{v}| \gtrless |\vec{u}|$

$$\Leftrightarrow (m\vec{u} + n\vec{v})(m\vec{u} + n\vec{v}) \gtrless \vec{u} \cdot \vec{u}$$

$$\Leftrightarrow m^2 r_u^2 + n^2 r_v^2 + 2mn\, r_u r_v \cos(\vec{u}, \vec{v}) \gtrless r_u^2 \qquad (1)$$

From the condition $\vec{v} < \vec{u} \pm \vec{v}$, we have

$$|\vec{v}|^2 \le |\vec{u} \pm \vec{v}|^2$$

$$\Leftrightarrow r_v^2 \le r_u^2 + r_v^2 \pm 2 r_u r_v \cos(\vec{u}, \vec{v})$$

$$\Leftrightarrow \pm 2 r_u r_v \cos(\vec{u}, \vec{v}) \gtrless -r_u^2 \qquad (2)$$

By (2), $LHS(1) \gtrless m^2 r_u^2 + n^2 r_v^2 - |mn| r_u^2 \ge (m^2 + n^2 - |mn|) r_u^2 \gtrless r_u^2$. Then if the ~~idea~~ equalities do not happen at once, we have $m\vec{u} + n\vec{v} > \vec{u}$. The equalities happen at once when

$$\begin{cases} |\vec{v}| = |\vec{u} + \vec{v}| \\ \cos(\vec{u}, \vec{v}) = -1/2 \\ m^2 + n^2 - mn = 1, \; r_u = r_v \end{cases}$$

$$\begin{cases} 2mn r_u r_v \cos(\vec{u},\vec{v}) = -|m||n| r_u^2 \\ m^2 + n^2 - |m||n| = 1 \\ n^2 r_v^2 = n^2 r_u^2 \end{cases}$$

$$\Leftrightarrow \begin{cases} mn\left(2 r_u r_v \cos(\vec{u},\vec{v}) \pm r_u^2\right) = 0 \\ (|m|=1, n=0) \text{ or } (m=0, |n|=1) \\ n^2 r_v^2 = n^2 r_u^2 \end{cases}$$

$$\Leftrightarrow \begin{cases} m = \pm 1 \\ n = 0 \end{cases} \quad \text{or} \quad \begin{cases} m = 0 \\ n = \pm 1 \\ r_v = r_u \end{cases}$$

The first case says $m\vec{u} + n\vec{v} = \pm\vec{u}$. The second says $m\vec{u} + n\vec{v} = \pm\vec{v}$ and we already know that $\pm\vec{v} > \vec{u}$. Thus we always have $\vec{u} = \min(H \setminus \{0\})$.

Now we'll show that $\vec{v} = \min(H \setminus \langle\vec{u}\rangle)$. Let $m \in \mathbb{Z}$ arbitrary, $n \in \mathbb{Z} \setminus \{0\}$.

We have $|m\vec{u} + n\vec{v}| \geq |\vec{v}|$

$$\Leftrightarrow |m\vec{u} + n\vec{v}|^2 \geq |\vec{v}|^2$$

$$\Leftrightarrow m^2 r_u^2 + n^2 r_v^2 + 2mn r_u r_v \cos(\vec{u},\vec{v}) \geq r_v^2$$

We have $m^2 r_u^2 + n^2 r_v^2 + 2mn r_u r_v \cos(\vec{u},\vec{v}) \geq m^2 r_u^2 + n^2 r_v^2 - |m||n| r_u^2$

$$= \left(m^2 - |m||n|\right) r_u^2 + \left(n^2 - 1\right) r_u^2 + r_v^2$$

$$= \underbrace{\left(m^2 - |m||n| + n^2 - 1\right)}_{\geq 0} r_u^2 + r_v^2 \geq r_v^2$$

Then if the equalities do not happen at once, $m\vec{u}+n\vec{v} > \vec{v}$.

The equalities happen at once if and only if

$$\begin{cases} \pm 2mn r_u r_v \cos(\vec{u},\vec{v}) = |m||n| r_u^2 \\ (m^2-1) r_v^2 = (n^2-1) r_u^2 \\ m^2 - |m||n| + n^2 - 1 = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} m=0 \\ n^2=1 \end{cases} \quad \text{or} \quad \begin{cases} m^2=1 \\ n=0 \\ r_u = r_v \end{cases}$$

$$\Leftrightarrow \begin{cases} m=0 \\ n=\pm 1 \end{cases} \quad \text{or} \quad \begin{cases} m=\pm 1 \\ n=0 \\ r_u = r_v \end{cases}$$

The first case says $m\vec{u}+n\vec{v} = \pm\vec{v}$. the second case is unacceptable because $n \in \mathbb{Z}\setminus\{0\}$.

(7) (Divisible groups) An abelian group $(G, +)$ is said to be divisible if for any $y \in G$ and $n \in \mathbb{Z}$, $n \neq 0$, there is an x in G with $nx = y$ (The simplest example is $(\mathbb{Q}, +)$).

(a) Show that any divisible group G is infinite, and that G has no subgroups of finite index other than G itself.

(b) Let $U = \mathbb{Q}/\mathbb{Z}$. Show that every element of U is a torsion element, that is, every element has finite order (or finite period, in the terminology in Lang's book). For each $n \geq 1$ show that U has a unique subgroup of order n, and that this subgroup is cyclic.

(c) For a prime p, let U_p be the subgroup of U consisting of all p-torsion elements, that is, all elements whose order is a power of p. Show that U_p is a divisible group, and describe all its subgroups.

Proof (a) Let $(G,+)$ be an abelian and divisible group. First, we'll show that G is finite. Let $x \in G \setminus \{0\}$. To ensure the existence of x, we realize that there is one missed hypothesis: $G \neq 0$. Now assume that $G \neq 0$ and $x \in G \setminus \{0\}$ exists. We will prove the following lemma:

[Let $v \in G \setminus \{0\}$ and d be a divisor of $\operatorname{ord}(v)$. If $u \in G$ satisfies $du = v$, then $d \cdot \operatorname{ord}(v) \mid \operatorname{ord}(u)$.]

Proof of the lemma. Put $n = \operatorname{ord}(v)$ and $m = \operatorname{ord}(u)$. We'll show that $dn \mid m$. We have $du = v$. Multiplying both sides by m, we have

$$mv = m(du) = (dm)u = d(mu) = 0$$

Thus $n \mid m$. Since $d \mid n$, $d \mid m$. Then we have

20

$$\frac{m}{d}v = \frac{m}{d}(du) = mu = 0$$

Thus $n \mid \frac{m}{d}$, or equivalently $dn \mid m$.

Return to the problem: if x is of infinite order, then $\langle x \rangle$ is an infinite subgroup in G. Thus G is infinite. Now suppose that x is of finite order $ord(x) > 1$. Let d be a divisor of $ord(x)$ (the easiest d to take is $ord(x)$ itself). Since G is divisible, we can divide x into d pieces, that is, there exists $y_1 \in G$ such that $x = dy_1$. By the lemma above, $d \cdot ord(x) \mid ord(y_1)$. Again, there exists $y_2 \in G$ such that $y_1 = dy_2$ and, since $d \mid ord(y_1)$, by the lemma $d \cdot ord(y_1) \mid ord(y_2)$. We can make a induction that given y_n such that $d \mid ord(y_n)$ then there exists $y_{n+1} \in G$ such that $y_n = dy_{n+1}$ and $d \cdot ord(y_n) \mid ord(y_{n+1})$.

Thus we have a strictly increasing sequence in $\mathbb{N}$

$$ord(x) < ord(y_1) < ord(y_2) < \dots < ord(y_n) < \dots$$

Since the order of the subgroup $\langle y_n \rangle$ in G is arbitrarily large by the choice of n, G is infinite.

Secondly, we'll show that G has no subgroup of finite index other than G itself. Let $H < G$ and $H \neq G$. Then G/H is a subgroup of G which

is not trivial. We'll show that G/H is also divisible. If we achieve this, then G/H will be infinte and thus H has infinite index in G. Let $\tilde{y} \in G/H$ and $n \in \mathbb{N}, n \neq 0$. We'll find $\tilde{x} \in G/H$ such that $n\tilde{x} = \tilde{y}$. There exists $y \in G$ such that $\tilde{y} = yH$. Since G is divisible, there exists $x \in G$ such that $y = nx$. Thus

$$\tilde{y} = yH = (nx)H = n\underbrace{(xH)}_{\tilde{x}} = n\tilde{x}.$$

Therefore G/H is also divisible.

(b) $U = (\mathbb{Q}/\mathbb{Z}, +)$. First, we'll show that every element of U is a torsion element. Let $x \in U$. Then there exists $r = \frac{p}{q} \in \mathbb{Q}$ such that $x = r + \mathbb{Z}$. Then

$$qx = q(r+\mathbb{Z}) = qr + q\mathbb{Z}$$
$$= p + q\mathbb{Z}$$
$$= \mathbb{Z}$$

thus x is of finite order and its order divides q.

Next, we'll show that for each $n \geq 1$, U has a unique subgroup of order n. Let ~~$x \in \mathbb{Q}/\mathbb{Z}$ which has order n~~

$$H = \{\tilde{x} \in \mathbb{Q}/\mathbb{Z} : n\tilde{x} = 0\}$$

Then all possible subgroup of $\mathbb{Q}/\mathbb{Z}$ of order n must be contained in H. Thus

if we could show that

- H is a group.
- H is of order n

then H is the unique subgroup of G which has order n.

Show that H is a group:

Let $\tilde{x}, \tilde{y} \in H$. Then $n\tilde{x} = n\tilde{y} = 0$. We have

$$n(\tilde{x}\tilde{y}) = n\{xy : x \in \tilde{x}, y \in \tilde{y}\} = \{(nx)y : x \in \tilde{x}, y \in \tilde{y}\} = (n\tilde{x})\tilde{y} = 0$$

Let $\tilde{x} \in H$. Then $n(-\tilde{x}) = -(n\tilde{x}) = 0$. Thus H is a group.

Show that H is of order n

Take $\tilde{x} \in H$. Then $n\tilde{x} = 0$. Let x be one representative of $\tilde{x}$. We have $n\tilde{x} = n(x+\mathbb{Z}) = nx + \mathbb{Z}$. Thus $n\tilde{x} = 0$ implies $nx \in \mathbb{Z}$.

Therefore $x \in \left\{\frac{0}{n}, \frac{\pm 1}{n}, \frac{\pm 2}{n}, \frac{\pm 3}{n}, \dots\right\}$. ~~However~~ Moreover,

$$\frac{0}{n} \sim \frac{0+kn}{n}$$

$$\frac{1}{n} \sim \frac{1+kn}{n} \qquad \forall k \in \mathbb{Z}$$

$$\frac{2}{n} \sim \frac{2+kn}{n}$$

$$\vdots$$

$$\frac{n-1}{n} \sim \frac{(n-1)+kn}{n}$$

Therefore $\tilde{x} = x + \mathbb{Z} \in \left\{ \frac{0}{n} + \mathbb{Z}, \frac{1}{n} + \mathbb{Z}, \dots, \frac{n-1}{n} + \mathbb{Z} \right\}$

and $H \subset \left\{ \frac{x}{n} + \mathbb{Z}, \frac{1}{n} + \mathbb{Z}, \dots, \frac{n-1}{n} + \mathbb{Z} \right\}$, which also has n elements. Thus

$$H = \left\{ \frac{0}{n} + \mathbb{Z}, \frac{1}{n} + \mathbb{Z}, \dots, \frac{n-1}{n} + \mathbb{Z} \right\}$$

We see that

$$H = \left\{ k\left(\frac{1}{n} + \mathbb{Z}\right) : k = 0, \dots, n-1 \right\} = \left\langle \frac{1}{n} + \mathbb{Z} \right\rangle$$

Thus H is cyclic.

(2) $U_p = \{ \tilde{x} \in \mathbb{Q}/\mathbb{Z} : \operatorname{ord}(\tilde{x}) = p^m \text{ for some } m = 0, 1, 2, \dots \}$

First we'll show that U_p is actually a group.

For $\tilde{x}, \tilde{y} \in U_p$, we have $p^m \tilde{x} = p^n \tilde{y} = 0$. ~~Thus Suppose that this~~

$$p^m(\tilde{x}\tilde{y}) = (p^m \tilde{x})\tilde{y} = 0$$

Thus $\operatorname{ord}(\tilde{x}\tilde{y}) \mid p^m$ and therefore $\operatorname{ord}(\tilde{x}\tilde{y})$ is a power of p. Thus $\tilde{x}\tilde{y} \in U_p$

For $\tilde{x} \in U_p$, we have $p^m \tilde{x} = 0$. Then $p^m(-\tilde{x}) = -(p^m \tilde{x}) = 0$.

Next we'll show that U_p is a divisible group. For each $\tilde{y} \in U_p$ and $n \in \mathbb{N}$, $n \neq 0$, we'll find $\tilde{x} \in U_p$ such that ~~$n\tilde{y} = n\tilde{x}$~~ $n\tilde{x} = \tilde{y}$. Taking an element $y = \frac{u}{v} \in \tilde{y}$. Here we suppose that u and v are relatively prime. We have $\tilde{y} = y + \mathbb{Z} = \frac{u}{v} + \mathbb{Z} = \left\{ \frac{u + kv}{v} : k \in \mathbb{Z} \right\}$

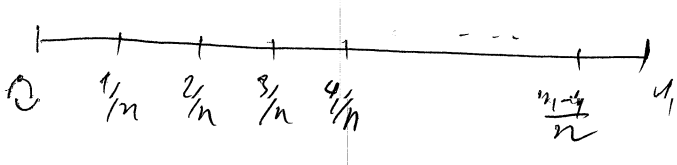
P4

Since $p^m \tilde{y} = 0$, we have $\frac{p^m u}{v} \in \mathbb{Z}$. Since $(u,v)=1$, v must divide p^m. Thus v is also a power of p, and we can write $v = p^\alpha$ where $\alpha \geq 0$. If $n = 1$ or -1, then we can choose $\tilde{x} = \tilde{y}$ or $\tilde{x} = -\tilde{y}$ respectively. If $|n| \geq 2$, we can express n as $n = p^\beta s$ where $\beta \geq 0$ and $(s,p) = 1$. we have $n\tilde{x} = \tilde{y}$ if and only if

$$p^\beta s\, \tilde{x} = y + \mathbb{Z} = \frac{u}{p^\alpha} + \mathbb{Z} = \left\{ \frac{u + kp^\alpha}{p^\alpha} : k \in \mathbb{Z} \right\}$$

If we could find $k_0 \in \mathbb{Z}$ such that $\frac{u + k_0 p^\alpha}{p^\alpha (p^\beta s)} \in \mathbb{Z}$ then $\tilde{x}$ is the one which has a representative $x = \frac{u + k_0 p^\alpha}{p^{\alpha+\beta} s}$, and we can realize that $p^{\alpha+\beta}\tilde{x} = \frac{u + k_0 p^\alpha}{s} + \mathbb{Z} = \mathbb{Z}$ and thus $\tilde{x} \in U_p$. Thus the problem is only to show that there exists $k_0 \in \mathbb{Z}$ such that $s \mid (u + k_0 p^\alpha)$. This is always satisfied since $(s,p) = 1$. A more general statement for this is that

> Given $a, m \in \mathbb{N}$ such that $(a,m) = 1$. Then for every $r \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that $ax \equiv r \pmod m$

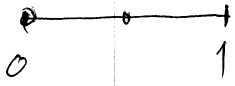


← Picture for the subgroup of U of order n.

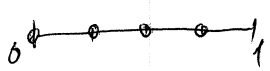
Now we'll find all subgroup of U_p. Since U_p is a subgroup of U and we know that U has only one subgroup of order n which is $\left\langle \frac{1}{n}+\mathbb{Z} \right\rangle$, U_p also has that property. In other words, for every power p^n where $n \geq 0$, there exists only one subgroup of U_p of order p^n. That is $H_{p^n} = \left\langle \frac{1}{p^n}+\mathbb{Z} \right\rangle$.

$$H_{p^n} = \left\{ \frac{1}{p^n}, \frac{2}{p^n}, \dots, \frac{p^n}{p^n} \right\} + \mathbb{Z}$$

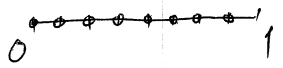
For example : $p=2$

$n=1$ 

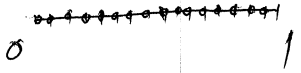
$H_2 = \{0, \frac{2}{2}\} + \mathbb{Z}$

$n=2$ 

$H_4 = \{0, \frac{1}{2^2}, \frac{2}{2^2}, \frac{3}{2^2}\} + \mathbb{Z}$

$n=3$ 

$H_8 = \{0, \frac{1}{2^3}, \frac{2}{2^3}, \frac{3}{2^3}, \frac{4}{2^3}, \frac{5}{2^3}, \frac{6}{2^3}, \frac{7}{2^3}\} + \mathbb{Z}$

$n=4$ 

$H_{16} = \{0, \frac{1}{2^4}, \dots, \frac{15}{2^4}\} + \mathbb{Z}$

We have $0 \leq H_{p^1} < H_{p^2} < H_{p^3} < \dots$ and $\bigcup_{n=0}^{\infty} H_{p^n} = U_p$. Let H be an infinite subgroup of G. Then for each $N \in \mathbb{N}$, there exists $n_N > N$ such that $H \cap H_{p^{n_N}} \neq \{0\}$. Since $H_{p^{n_N}}$ is cyclic, $H_{p^{n_N}} \subset H$. Thus

$$H \supset \bigcup_{N=0}^{\infty} H_{p^{n_N}} = \bigcup_{n=0}^{\infty} H_n = U_p$$

Thus $H = U_p$. In conclusion, there is only one infinite subgroup of U_p that is U_p itself. For any power p^n, there exists a unique subgroup of U_p which is of order p^n. That is $H_{p^n} = \left\{\frac{0}{p^n}, \frac{1}{p^n}, \cdots, \frac{p^n-1}{p^n}\right\} + \mathbb{Z} = \left\langle \frac{1}{p^n} + \mathbb{Z} \right\rangle$. And there is no other subgroups.

2 (5) Problem 7, Lang p. 75

Let G be a group such that $\mathrm{Aut}(G)$ is cyclic. Prove that G is abelian.

Proof Here we are given the structure of $\mathrm{Aut}(G)$, and asked to find the structure of G. There are at least 2 ways to cope with this, but the common principle is to find some homomorphism between them. One way to think is to find a homomorphism from $\mathrm{Aut}(G)$ to G, say $f: \mathrm{Aut}(G) \to G$. Moreover, we hope that f will be surjective, which would be easy to obtain since $\mathrm{Aut}(G)$ is kind of bigger than G. Then we use the first isomorphism theorem to say $G \simeq \mathrm{Aut}(G)/\ker f$. Given the structure of $\mathrm{Aut}(G)$, in this problem is the cyclicity, we will have the corresponding properties for G. This is, however, very difficult to find such an f.

The other way is to find a homomorphism from G to $\mathrm{Aut}(G)$. And we know that there is a handy map between them:

$c_{\phi}: G \to Aut(G)$

$x \mapsto c_x$ such that $c_x(y) = xyx^{-1}$

Each c_x is called an inner isomorphism of G. We verify that c is indeed a homomorphism. Let $x, y, z \in G$, we have

$$c_{xy}(z) = xyz(xy)^{-1} = xyzy^{-1}x^{-1} = x\,c_y(z)x^{-1} = c_x c_y(z)$$

Thus $c_{xy} = c_x c_y$ and hence c is a homomorphism. Then we have

$$G/\ker c \approx \operatorname{Im} c$$

By definition $\ker c = \{x \in G : c_x = id\}$

$= \{x \in G : c_x(y) = y \ \forall y \in G\}$

$= \{x \in G : xyx^{-1} = y \ \forall y \in G\}$

$= Z(G)$ - the center of G.

Since we are to prove that G is abelian, we need to show that $Z(G) = G$, or $\ker c = G$, or equivalently $\operatorname{Im} c = \{id\}$. Since $\operatorname{Im} c$ is a subgroup of $Aut(G)$, which is cyclic, $\operatorname{Im} c$ is also cyclic. Let $f \in \operatorname{Im} c$ be a generator of $\operatorname{Im} c$. We'll show that $f = id$. ~~For each $x \in G$, there exists $n \in \mathbb{Z}$ such that $c_x = f^n$~~ Since $f \in \operatorname{Im} c$, there exist $a \in G$ such that $f = c_a$. For every $x \in G$, there exists $n \in \mathbb{Z}$ such that $c_x = f^n = (c_a)^n = c_{a^n}$. Thus $xax^{-1} = c_x(a) = c_{a^n}(a) = a^n a a^{-n} = a$. Thus $xa = ax$. Hence $axa^{-1} = x$.

which mean $axa^{-1}=x \ \forall x\in G$, or $c_a(x)=x \ \forall x\in G$. Thus $f=c_a$ is the identity map.

(6) Problem 8, Lang p. 75

(a) Let G be a group and H a subgroup of finite index. Show that there exists a normal subgroup N of G contained in H and also of finite index.

(b) Let G be a group and let H_1, H_2 be subgroups of finite index. Prove that $H_1 \cap H_2$ has finite index.

Proof

(a) We are given a group G, and asked to find a normal subgroup N of G such that $|G/N|$ is finite. We won't be able to do so if we are not given H and the correlation between H and G. There are 2 correlations

$$\begin{cases} H<G \\ |G/H| \text{ is finite.} \end{cases}$$

In some sense, we use H to understand G. How could we do so? we need a homomorphism between them, say $f: H\to G$ or $g: G\to H$. what type of structure in G do we want to know? That is the existence of a normal subgroup. A homomorphism $f: H\to G$ won't give us any normal subgroup in G (it only gives a subgroup of G). Thus we should concentrate on $g: G\to H$. Actually, we

know about H less than we know about G/H. Thus, it is reasonable to look for a homomorphism $g: G \to G/H$. However, G/H is not a group since H is not normal in G. We'll never have such a homomorphism. With a general set G/H like this, we only have action. Thus, g looks somehow like $g: G \to \text{Perm}(G/H) \simeq S_n$, where $n = |G/H|$. A group action $G \times (G/H) \to (G/H)$ that is most natural may be the translation

$$g(g'H) := (gg')H$$

However, just keep in mind that there are a bunch of other actions from G to G/H, for example before acting on S, elements of G undergo an

$$G \xrightarrow[\text{endomorphism}]{\text{automorphism}} G \xrightarrow{\pi} \text{Perm}(S)$$

automorphism or endomorphism. Then the composite map with π remains a homomorphism. Now let's prove that the translation is actually an action of G on G/H.

$g(g'H) \overset{T}{=} (gg')H$ is automatically satisfied by definition of translation

we have $g(eH) = gH$ is also automatically satisfied. Thus T is an action $T: G \to \text{Perm}(G/H)$.

30

Since T is a homomorphism, $\ker T$ is a normal subgroup of G and

$G/\ker T \simeq \mathrm{Im}(T)$, which is a subgroup of S_n

Thus $|G/\ker T| = |\mathrm{Im}(G)| \leq n!$, which is finite. Thus it would be perfect to choose $N = \ker T$ if we could prove $N \subset H$. Take $g \in N$, then $T(g) = Id$. Thus $T_g(g'H) = g'H \ \forall g' \in G$, or $(gg')H = g'H \ \forall g' \in G$. We choose $g' = e$ and see that $gH = H$. Thus $g \in H$ and therefore $N \subset H$.

(b) we have G/H_1 and G/H_2 finite. There are finitely many left cosets of H_1 and H_2 in G, and we denote

$$G/H_1 = \{x_1H_1, x_2H_1, \dots, x_nH_1\}$$

$$G/H_2 = \{y_1H_2, y_2H_2, \dots, y_mH_2\}$$

and $\bigcup x_iH_1 = \bigcup y_jH_2 = G$. For each $j = 1, 2 \dots, m$, if y_jH_2 has nonempty intersection of with H_1 then we rechoose y_j (replacing y_j by another representative) such that $y_j \in H_1$. Let $J \subset \{1, 2 \dots, m\}$ be the set of all indices j such that $y_j \in H_1$. Then

$$H_1 = H_1 \cap G = H_1 \cap \left(\bigcup y_jH_2\right) = \bigcup (H_1 \cap y_jH_2) = \bigcup_{j \in J} (H_1 \cap y_jH_2)$$

For each $j \in J$, $H_1 \cap y_jH_2 = y_j(H_1 \cap H_2)$ since $y_j \in H_1$. Thus,

$$H_1 = \bigcup_{j \in J} y_j(H_1 \cap H_2)$$

Thus $\{y_j\}_{j\in J}$ is a set of ~~rep~~ coset representatives of $H_1 \cap H_2$ in H_1. We know that $\{x_i\}_{1\le i\le n}$ is a set of coset representatives of H_1 in G. Thus the set $\{x_i y_j : 1\le i\le n, j\in J\}$ is a set of coset representatives of $H_1 \cap H_2$ in G. Thus $H_1 \cap H_2$ has finite index in G.