Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on:
  `https://japorized.github.io/TeX_notes`

20 Lecture 20 Jun 18th 2018

20.1 Finite Abelian Groups (Continued 2)

20.1.1 p-Groups (Continued 2)

Recall that we had the following subgroup of a group G.

$$G^{(m)} = \{g \in G : g^m = 1\}.$$

We discussed about the Primary Decomposition, Theorem 52, and then arrived at Proposition 55. With these, we can have the following theorem:

Theorem 56 (Finite Abelian Groups are Isomorphic to a Direct Product of Cyclic Groups)

Let $G \neq \{1\}$ be a finite abelian p-group. Then G is isomorpic to a direct product of cylic groups.

Proof

By Proposition 55, there is a cyclic group C_1 and a subgroup B_1 of G, such that $G \cong C_1 \times B_1$. Since $B_1 \leq G$, we have that $|B_1| \mid |G|$, and so by Theorem 23, B_1 is also a p-group. If $B_1 \neq \{1\}$, then by Proposition 55, there exists a cyclic group C_2 and a $B_2 \leq B_1$ such that $B_1 \cong C_2 \times B_2$.

By continuing this line of argument, we can get $C_1, C_2, \ldots$ until we get to some C_k with $B_k = \{1\}$, for some $k \in \mathbb{N}$. Then

$$G \cong C_1 \times C_2 \times \ldots \times C_k$$

as required. □

Remark

We can verify that the decomposition of a finite abelian p-group into a direct product of cyclic groups is in fact unique up to their orders.[1]

[1] This is the bonus question on A4. It will be included once the assignment is over.

Combining the above remark, Theorem 52 and Theorem 56, we have the following theorem.

Theorem 57 (Finite Abelian Group Structure)

If G is a finite abelian group, then

$$G \cong C_{p_1^{n_i}} \times \ldots \times C_{p_k^{n_k}}$$

where $C_{p_i^{n_i}}$ is a cyclic group of order $p_i^{n_i}$, where $1 \leq i \leq k$. The numbers $p_i^{n_i}$ are uniquely determined up to their order.[2]

[2] Note that the p_i's do not have to be unique.

Remark

Note that if p_1 and p_2 are distinct primes, then

$$C_{p_1^{n_1}} \times C_{p_2^{n_2}} \cong C_{p_1^{n_1} p_2^{n_2}},$$

the cyclic group of order $p_1^{n_1} p_2^{n_2}$. Thus, by combining suitable prime factors together, for a finite abelian group G, we can also write

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_r},$$

where $m_i \in \mathbb{N}$, $i \leq 1 \leq r$, $m_1 > 1$ and

$$m_1 \,|\, m_2 \,|\, \ldots \,|\, m_r$$

Example 20.1.1

Conder an abelian group G with order 48. Since $48 = 2^4 \cdot 3$, an abelian group of order 48 is isomorphic to $H \times \mathbb{Z}_3$, where H is an abelian group of order 2^4. The options for H are:

$$\mathbb{Z}_{2^4} \qquad \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \qquad \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}$$
$$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Therefore, we have the following possible decompositions of G:

$$G \cong \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \cong \mathbb{Z}_{48}$$
$$G \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_{24}$$
$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 = \mathbb{Z}_4 \times \mathbb{Z}_{12}$$
$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$$
$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$$

20.2 Rings

20.2.1 Rings

Definition 31 (Ring)

A set R is a ring if $\forall a, b, c \in R$,

1. $a + b \in R$
2. $a + b = b + a$
3. $a + (b + c) = (a + b) + c$
4. $\exists 0 \in R \;\; a + 0 = a = 0 + a$
5. $\exists (-a) \in R \;\; a + (-a) = 0 = (-a) + a$
6. $ab \in R$
7. $a(bc) = (ab)c$
8. $\exists 1 \in R \;\; 1 \cdot a = a = a \cdot 1$
9. $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$

We call 1 as the ***Unity*** *of R, 0 as the Zero of R, and $-a$ as the* ***negative*** *of a.*

The ring R is called a ***Commutative Ring*** *if it also satisfies the following:*

10. $ab = ba$.

As daunting as this definition seems, it is much easier to remember if we think of R being an **abelian group under addition**, **"almost" a group under multiplication**, save the fact that the **multiplicative inverse of an element does not necessarily exist**, and with the **distributive law**.

Example 20.2.1

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are commutative rings with the zero being 0, and unity being 1.

Example 20.2.2

For $n \in \mathbb{N}$, $n \geq 2$, $\mathbb{Z}_n$ is a commutative ring with the zero being $[0]$, and unity being $[1]$.

Example 20.2.3

The set $M_n(\mathbb{R})$ is a ring using matrix addition and matrix multiplication, with zero being the zero matrix 0, and unity being the identity matrix I. We also know that $M_n(\mathbb{R})$ is not commutative.

Warning

Note that since $(R, \cdot)$ is not a group, we no longer have the liberty of using Proposition 6, i.e. we do not have left or right cancellation. For example, in $\mathbb{Z}$, $0 \cdot x = 0 \cdot y \implies x = y$.
