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`

18 Lecture 18 Jun 13th 2018

18.1 Finite Abelian Groups

18.1.1 Primary Decomposition

Note (Notation)

Let G be an abelian group and $m \in \mathbb{Z}$. We define

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

Proposition 50 (Group of Elements of the Same Order is a Subgroup)

Let G be an abelian group. Then $G^{(m)} \leq G$.

Proof

Note that $1^m = 1 \in G^{(m)}$. $\forall g, h \in G^{(m)}$, since G is abelian, we have that[1]

$$(gh)^m = g^m h^m = 1 \cdot 1 = 1.$$

Therefore $gh \in G^{(m)}$. Also, for $g \in G^{(m)}$, we have

$$\left(g^{-1}\right)^m = (g^m)^{-1} = 1.$$

Thus $g^{-1} \in G^{(m)}$. By the **Subgroup Test**, *we have that $G^{(m)} \leq G$.* □

[1] Pay attention that this is only true if G is abelian.

Proposition 51 (Decomposition of a Finite Abelian Group)

Let G be a finite abelian group with $|G| = mk$ such that $\gcd(m,k) = 1$. Then

1. $G \cong G^{(m)} \times G^{(k)}$*; and*
2. $\left|G^{(m)}\right| = m$ *and* $\left|G^{(k)}\right| = k$.

Proof

1. *Since G is abelian, $G^{(m)} \triangleleft G$ and $G^{(k)} \triangleleft G$.*

   Claim 1: $G^{(m)} \cap G^{(k)} = \{1\}$
   Proof of Claim 1: $\forall g \in G^{(m)} \cap G^{(k)}$, $g^m = 1 = g^k$
   $\because \gcd(m,k) = 1$, *by Bezout's Lemma*, $\exists x, y \in \mathbb{Z} \quad 1 = mx + ky$
   $\implies g = g^1 = g^{mx+ky} = (g^m)^x (g^k)^y = 1 \cdot 1 = 1$
   $\implies G^{(m)} \cap G^{(k)} = \{1\}$ *as claimed.*

   Claim 2: $G = G^{(m)} G^{(k)}$ [2]
   $\forall g \in G \quad \because o(g) = mk \quad 1 = g^{mk} = (g^k)^m = (g^m)^k$
   *It follows that $g^k \in G^{(m)}$ and $g^m \in G^{(k)}$. From **Claim 1** and by abelianness, we have that*

   $$g = g^{mx+ky} = (g^k)^y (g^m)^x \in G^{(m)} G^{(k)}$$

   Thus $G \subseteq G^{(m)} G^{(k)}$. On the other hand, since $G^{(m)} \triangleleft G$ and $G^{(k)} \triangleleft G$, by Lemma 29, we have that $G^{(m)} G^{(k)} \leq G$ and hence $G^{(m)} G^{(k)} \subseteq G$. Thus $G = G^{(m)} G^{(k)}$ as claimed.

   *From **Claims 1 and 2**, we can conclude by Corollary 33*[3]*, that $G \cong G^{(m)} \times G^{(k)}$ as required.*

2. *Write $\left|G^(m)\right| = m'$ and $\left|G^{(k)}\right| = k'$. By part (1), we have that $mk = |G| = m'k'$.*

   Claim 3: $\gcd(m, k') = 1$
   Suppose not
   $\implies \exists p$ *prime* $\quad p \mid m$ *and* $p \mid k'$
   $\implies \exists g \in G^{(k)} \quad o(g) = p \qquad \because$ *Cauchy's Theorem*
   Now $p \mid m \implies \exists q \in \mathbb{Z} \quad m = pq$
   $\implies g^m = g^{pq} = 1 \quad \because o(g) = p$
   $\implies g \in G^{(m)}$.
   By part (1), we have that $g \in G^{(m)} \cap G^{(k)} = \{1\} \implies g = 1$, which

[2] Recall that this is the Product

[3] Should this not be Theorem 32?

contradicts the fact that $o(g) = p$*. Thus* $\gcd(m, k') = 1$ *as claimed. Similarly, we can get that* $\gcd(m', k) = 1$*.*

Notice that $mk = m'k' \implies m \mid m'k'$
$\implies m \mid m' \quad \because \gcd(m, k') = 1$ *and similarly* $k \mid k'$*. But then* $mk = m'k'$ *would imply that* $m' = m$ *and* $k' = k$*.*

$\square$

As a direct consequence of Proposition 51, we have the following:

Theorem 52 (Primary Decomposition)

Let G *be a finite abelian group with* $|G| = p_1^{n_1} \dots p_k^{n_k}$*, where* $p_1, \dots, p_k$ *are distinct primes, and* $n_1, \dots, n_k \in \mathbb{N}$*. Then*

1. $G \cong G^{\left(p_1^{n_1}\right)} \times \dots \times G^{\left(p_k^{n_k}\right)}$*; and*
2. $\forall i \;\; 1 \leq i \leq k \quad \left| G^{\left(p_i^{n_i}\right)} \right| = p_i^{n_i}$*.*

18.1.2 *p-Groups*

On a related note of the groups $G^{\left(p_i^{n_i}\right)}$, we define the following:

Definition 30 (p-Group)

Let p *be a prime. A* ***p-group*** *is a group in which every element has an order that is a non-negative power of* p*.*

Proposition 53 (p-Groups are Finite)

A finite group G *is a p-group* $\iff$ $|G|$ *is a power of* p *(including* p^0*).*

Proof

$(\impliedby)$ *If* $|G| = p^\alpha$ *for some* $\alpha \in \mathbb{N} \cup \{0\}$ *and* $g \in G$*, by Corollary 24,* $o(g) \mid p^\alpha$

$\implies$ *G is a p-group.*

($\implies$ *) Consider the contrapositive and let* $|G| = p^n p_2^{n_2} \dots p_k^{n_k}$ *where* $p, p_2, ..., p_k$ *are distinct primes,* $n \in \mathbb{N} \cup \{0\}$*, and* $n_2, ..., n_k \in \mathbb{N}$*. For* $k \geq 2$*, by Cauchy's Theorem,* $p_2 \mid |G|$

$\implies \exists g_1 \in G \quad o(g_1) = p_2$

$\implies$ *G is not a p-group.*

Therefore, our desired result follows. $\square$

Our end goal here is to prove to ourselves that all finite abelian groups can be written as cross products of cyclic groups, i.e. if G is an abelian group, then

$$G \cong C_1 \times C_2 \times \ldots \times C_n.$$

With Theorem 52, we have that

$$G \cong G_1 \times G_2 \times \ldots \times G_n.$$

The following proposition will enable us to get to our goal from our current position:

Proposition (Finite Abelian p-Groups of order p are Cyclic)

If G is a finite abelian p-group that contains only one subgroup of order p*, where* p *is prime, then G is cyclic. In other words, if a finite abelian p-group is not cyclic, then it must have at least* 2 *subgroups of order* p*.*
