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`

19 Lecture 19 Jun 15th 2018

19.1 Finite Abelian Groups (Continued)

19.1.1 p-Groups (Continued)

Note (Recall)

Recall the definition of a p-group:

G is a p-group if the order of all of its elements is a non-negative power of $p \iff |G| = p^k$ for some $k \in \mathbb{N} \cup \{0\}$.

We shall now proceed to prove the proposition mentioned by the end of last class.

Proposition 54 (Finite Abelian p-Groups of Order p are Cyclic)

If G is a finite abelian p-group that contains only 1 subgroup of order p, then G is cyclic. In other words, if a finite abelian p-group is not cyclic, then G has at least 2 subgroups of order p.

Proof

Since G is finite, let $y \in G$ have maximal order.

Claim: $G = \langle y \rangle$

***Proof of Claim:** Suppose not. Since $\langle y \rangle \lhd G$* [1]*, consider the quotient group $G/\langle y \rangle$, which is, therefore, a nontrivial p-group, since $|\langle y \rangle| = p$. By Cauchy's Theorem, we know that $\exists z \in G/\langle y \rangle$ such that $o(z) = p$* [2]*. In particular, we have that $z \neq 1$* [3]*. Consider the coset map*

[1] We have $\langle y \rangle \leq G$ and G is abelian.

[2] Note that we have $G/\langle y \rangle$ is a p-group $\iff \left| G/\langle y \rangle \right| = p^k$ for some $k \in \mathbb{N} \cup \{0\}$. The existence of our chosen z follows from there by Cauchy's Theorem.

[3] If $z = 1$, then its order would not be p.

$$\pi : G \to G/\langle\, y \,\rangle.$$

Let $x \in G$ such that $\pi(x) = z$[4]*. Since*

$$\pi(x^p) = \pi(x)^p = z^p = 1,$$

we have that x^p gets mapped to 1 by π, i.e. $x^p \in \langle\, y \,\rangle$.

$\implies \exists m \in \mathbb{Z}$ *such that $x^p = y^m$. We shall consider two cases:*

Case 1: *$p \nmid m$.*

$\because$ *$p \nmid m$, we have that $\gcd(m, |\langle\, y \,\rangle|) = 1$, and hence by Proposition 18*[5]*, we have that $o\left(y^m\right) = o(y)$. Because y has maximal order, we have*

$$o(x^p) \overset{(1)}{<} o(x) \leq o(y) = o(y^m) = o(x^p)$$

where note that (1) is true because x would need to take more powers of p than x^p to get back to 1. We observe that we have arrived at a contradiction.

Case 2: *$p \mid m$.*

$p \mid m \implies \exists k \in \mathbb{Z} \;\; m = pk \implies x^p = y^m = y^{pk}$

$\because$ *G is abelian, we have that $(xy^-k)^p = 1$.*

By assumption, there is only one subgroup of G of order p, call it H. Thus $xy^k \in H$. On the other hand, by the Fundamental Theorem of Finite Cyclic Groups[6]*, $\langle\, y \,\rangle$ has only one subgroup of of order p, which must be H. Therefore, in particular, we have $xy^{-k} \in \langle\, y \,\rangle$ which implies $x \in \langle\, y \,\rangle$. It follows that $z = \pi(x) = 1$ since $\langle\, y \,\rangle$ is the identity in the quotient group $G/\langle\, y \,\rangle$, which contradicts our choice of $z \neq 1$.*

Therefore, by combining the two cases, we have that $G = \langle\, y \,\rangle$. □

[4] Recall that π is surjective by Proposition 35.

[5] **Proposition (Proposition 18)** *Let $G = \langle\, g \,\rangle$ with $o(g) = n \in \mathbb{N}$. We have*

$$G = \langle\, g^k \,\rangle \iff \gcd(k, n) = 1$$

[6] **Theorem (Theorem 19)** *Let $G = \langle\, g \,\rangle$ with $o(g) = n \in \mathbb{N}$.*

1. *H is a subgroup of $G \implies \exists d \in \mathbb{N} \;\; d \mid n \quad H = \langle\, g^d \,\rangle \implies |H| \mid n$.*
2. *$k \mid n \implies \langle\, g^{\frac{k}{n}} \,\rangle$ is the unique subgroup of G of order k.*

Proposition 55

Let $G \neq \{1\}$ be a finite abelian p-group that contains one subgroup of order p. Let C be the cyclic subgroup of G of maximal order. Then $\exists B \leq G$ such that $G = CB$ and $C \cap B = \{1\}$. By Corollary 33, we have $G \cong C \times B$.

Proof

We shall prove this result by induction. If $|G| = p$, then $C = G$ by definition and we can choose $B = \{1\}$. The result follows from there.

Suppose that the result holds for all groups of order p^{n-1} with $n \in \mathbb{N}$ and $n \geq 2$. Consider the case for $|G| = p^n$. There are two cases to consider from here.

***Case 1**: If $C = G$, then we can pick $B = \{1\}$ so that the result follows.*

***Case 2**: If $C \neq G$, then G is not cyclic. By Proposition 54, there exists at least 2 subgroups of G that are of order p. Since C is cyclic, by the Fundamental Theorem for Finite Cyclic Groups, we have that C contains exactly one subgroup of order p. Then $\exists D \leq G$ such that $|D| = p$ and $D \nsubseteq C$, and consequently $C \cap D = \{1\}$. Now since G is abelian, $D \lhd G$ and hence we may consider its coset map:*

$$\pi : G \to G/D.$$

*If we consider $\pi \restriction_C$, called the **restriction** of π on C [7], then $\ker \pi \restriction_C = C \cap D = \{1\}$. Then by the First Isomorphism Theorem, we have*

$$C = C/\ker \pi \restriction_C \cong \operatorname{im} \pi \restriction_C = \pi(C).$$

Now let y be the generator of the cyclic group C. Then since $\pi(C) \cong C$, we have $\pi(C) = \langle \pi(y) \rangle$. By assumption on C, $\pi(C)$ is the cyclic subgroup of G/D of maximal order [8]. Since $\left| G/D \right| = p^{n-1}$ by Lagrange's Theorem, by the induction hypothesis, G/D has a subgroup E such that $\pi(C)E = G/D$ and $\pi(C) \cap E = \{1\}$.

Therefore, choose $B = \pi^{-1}(E)$, i.e. $\pi(B) = E$.

<u>Claim 1</u>: $G = CB$

Note that $D \subseteq B$ [9]. If $x \in G$, $\because \pi(C)\pi(B) = \pi(C)E = G/D$, we have that $\exists u \in C$, $\exists v \in B$ such that

$$\pi(x) = \pi(u)\pi(v).$$

By homomorphicity, we have $\pi(xu^{-1}v^{-1}) = 1$ which implies $xu^{-1}v^{-1} \in D \subseteq B$. Then because $v \in B$, we have that $xu^{-1} \in B$ since B is a group. Then since G is abelian, we have

$$x = uxu^{-1} \in CB.$$

<u>Claim 2</u>: $C \cap B = \{1\}$.

Let $x \in C \cap B$. Then $\pi(x) \in \pi(C) \cap \pi(B) = \pi(C) \cap E = \{1\}$. Then, $\because \pi(x) = 1 \in C/D$ [10], we have that $x \in D$. Therefore, $x \in C \cap D = \{1\}$ which then $x = 1$.

[7] The restriction of π on C simply means that we restrict the domain of π to work solely for the subset C. In plain words, we are only considering the case where π is applied onto elements of C.

[8] **I need to get some clarification from the professor on this.**

[9] **This needs clarification as well.**

[10] **I need to double check this to make sure that it is indeed C and not G, because it does not make sense with C being the one that D is onto.**

Since ***Claims 1 & 2*** *hold, the result follows by induction.* □