Fundamental Theorem of Abelian Groups : Algebra

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
23 September, 2017 (at *14:35*)

ABSTRACT: Seat-of-the-pants proof scribbled out one Thursday.

Overview. We work inside a fixed group $(\mathbb{G}, \cdot, \boldsymbol{\varepsilon})$. Henceforth let "***cyclic group***" mean a *non–one-point cyclic group*.

Use ***PoP*** to mean *Power Of a Prime*. A group $\mathbb{G}$ is a ***PoP group*** if $^{\#}\mathbb{G}$ is a PoP. If $^{\#}\mathbb{G} = \boldsymbol{p}^N$, for a posint N and prime $\boldsymbol{p}$, then we call $\mathbb{G}$ a "$\boldsymbol{p}$-group". The standing notational assumption is that $\boxed{\mathbb{G} \supset \mathbf{M}, \mathbf{F} \text{ are groups}}$ and $\boxed{\boldsymbol{\beta} \in \mathbb{G}}$ is a particular element. I use Greek letters $\boldsymbol{\beta}, \mu, \gamma, \nu \ldots$ to name elements of groups.

Our goal is to prove the following classical theorem.

1: Fund. Theorem of Finite Abelian Groups (FToAG). *Each finite abelian group $\mathbb{G}$ is isomorphic to a finite cartesian product of cyclic groups. The multiset of sizes of the factor groups is unique, when counted appropriately.*

Furthermore, if $\mathbb{G}$ is a $\boldsymbol{p}$-group, then it is a finite product of cyclic $\boldsymbol{p}$-groups. ♢

The crux for FToAG is handling the special case when $\mathbb{G}$ is a PoP group.

Tools. Let "$\mathbf{M} \perp \mathbf{F}$" indicate trivial intersection, $\mathbf{M} \cap \mathbf{F} = \{\boldsymbol{\varepsilon}\}$; we say that $\mathbf{M}$ is ***transverse*** to $\mathbf{F}$. A collection $\{\mathbf{C}_\theta\}_{\theta \in \Theta}$ of groups is a ***transverse family***, if *each* member $\mathbf{C}_\theta$ is transverse to the *subgroup generated* by the other members.

2: Fact. *Suppose the gps $\mathcal{C} := \{\mathbf{C}_\theta\}_{\theta \in \Theta}$ are inside an **abelian** gp. Then $\mathcal{C}$ is a transverse family IFF the <u>only</u> soln to eqn*

$$\prod_{\theta \in \Theta} b_\theta \;=\; \boldsymbol{\varepsilon}\,, \qquad \textit{with each } b_\theta \in \mathbf{C}_\theta, \textit{ and all but finitely-many equal } \boldsymbol{\varepsilon}$$

is every $b_\theta = \boldsymbol{\varepsilon}$. If we choose to enumerate $\mathcal{C}$ as $\mathbf{C}_1, \mathbf{C}_2, \ldots,$ then $\mathcal{C}$ is transverse IFF each

$$\mathbf{C}_n \quad \perp \quad \mathbf{C}_1 \cdot \mathbf{C}_2 \cdots \mathbf{C}_{n-1}\,. \qquad \diamondsuit$$

Use $\mathrm{Ord}(\boldsymbol{\beta})$ for the smallest posint d st. $\boldsymbol{\beta}^d = \boldsymbol{\varepsilon}$. Use $\mathbf{M}$-$\mathrm{Ord}(\boldsymbol{\beta})$ for the smallest posint d such that $\boldsymbol{\beta}^d \in \mathbf{M}$. (So $\mathrm{Ord}(\boldsymbol{\beta})$ is $\mathbf{M}$-$\mathrm{Ord}(\boldsymbol{\beta})$ when $\mathbf{M} := \{\boldsymbol{\varepsilon}\}$.)

3: Prop'n. *Imagine that $d := \mathbf{M}\text{-}\mathrm{Ord}(\boldsymbol{\beta})$ is finite and let $\mu := \boldsymbol{\beta}^d \in \mathbf{M}$. Then*

$$3^*\text{:} \qquad \langle \boldsymbol{\beta} \rangle \cap \mathbf{M} \;=\; \langle \mu \rangle\,.$$

Consequently, for each subgroup $\mathbf{F} \subset \mathbf{M}$:

$$\textit{If} \quad \langle \mu \rangle \perp \mathbf{F} \quad \textit{then} \quad \langle \boldsymbol{\beta} \rangle \perp \mathbf{F}\,.$$

Furthermore, $\mathrm{Ord}(\boldsymbol{\beta}) \;=\; \mathbf{M}\text{-}\mathrm{Ord}(\boldsymbol{\beta}) \cdot \mathrm{Ord}(\mu)$. ♢

Pf. Let P be the set of posints j with $\boldsymbol{\beta}^j \in \mathbf{M}$. Fixing a $j \in P$, Bézout's lemma tells us that $D := \mathrm{Gcd}(j, d)$ is in P. Thus $D \geqslant \mathrm{Min}(P) = d$. But $D \bullet\!\!| \; d$, so $D = d$. Hence (3^*), since $d = D \bullet\!\!| \; j$. ♦

Remark. Henceforth "5" represents a arbitrary prime $\boldsymbol{p}$. Use ***PoF*** to mean "power of 5".

In the case where $\mathbb{G}$ is a $\boldsymbol{p}$-group, say $\boldsymbol{p} = 5$, then Lagrange's thm assures that both $\mathrm{Ord}(\boldsymbol{\beta})$ and $\mathrm{Ord}(\mu)$ are PoFs; so $\mathbf{M}$-$\mathrm{Ord}(\boldsymbol{\beta})$ is a PoF. □

4: Corollary. *Suppose that $\mathbb{G}$ is a 5-group and $\mathbf{M}$ a subgp. Then both $\mathrm{Ord}(\boldsymbol{\beta})$ and $\mathbf{M}$-$\mathrm{Ord}(\boldsymbol{\beta})$ are PoFs. Further,*

$$4^*\text{:} \qquad \mathrm{Ord}(\mu) \;=\; 5^{B-J}\,,$$

where $5^B := \mathrm{Ord}(\boldsymbol{\beta}) \geqslant \mathbf{M}\text{-}\mathrm{Ord}\boldsymbol{\beta} =: 5^J$ define natnums. ♢

5: Generator Lemma. *Suppose $\mathbf{C}$ is cyclic of order 5^L. Then each element $\nu \in \mathbf{C}$ can be written*

$$\nu \quad = \quad \gamma^{5^K}$$

for some $\mathbf{C}$-<u>generator</u> $\gamma = \gamma(\nu)$ and $K = K(\nu) \in [0 \,..\, L]$. ♢

Proof. Pick a $\mathbf{C}$-generator γ_0 and take the unique $d \in [1 \,..\, 5^L]$ st. ${\gamma_0}^d = \nu$. Factor d as $d = n \cdot 5^K$ with $K \in [0 \,..\, L]$ and $n \perp 5$. Automatically $n \perp 5^K$, so the element $\gamma := {\gamma_0}^n$ generates $\mathbf{C}$. ♦

Preliminaries. Henceforth $\mathbb{G}$ is an abelian p-group. For specificity, suppose that $p = 5$ and $^{\#}\mathbb{G} = 5^{1293}$.

We will successively pick cyclic subgroups $\mathbf{C}_1, \mathbf{C}_2, \ldots \subset \mathbb{G}$. At stage T, let

$$\mathbf{F}_T \quad := \quad \mathbf{C}_1 \cdot \mathbf{C}_2 \cdot \ldots \cdot \mathbf{C}_T$$

be the product of the first T many chosen groups. So $\mathbf{F}_0$ is the trivial group $\{\varepsilon\}$. Each $\mathbf{F}_T$ is a gp, since $\mathbb{G}$ is abelian.

Construction. At stage T, with $\mathbf{F}_{T-1}$ chosen:

> *If there exists a cyclic group* $\mathbf{C} \perp \mathbf{F}_{T-1}$, *then pick one such* $\mathbf{C}$ *of* ***maximum cardinality*** *and let* $\mathbf{C}_T := \mathbf{C}$.

Continue until no such group can be chosen.

For specificity, say that the process terminates with

$$\mathbf{C}_1\,, \mathbf{C}_2\,, \ldots\,, \mathbf{C}_{26}\,.$$

(By construction, this is a transverse family of cyclic groups.) Let $\mathbf{M} := \mathbf{F}_{26}$ be this maximal product. We thus have

6: $\forall \boldsymbol{\beta} \in \mathbb{G} \smallsetminus \mathbf{M}$: *The cyclic group* $\langle \boldsymbol{\beta} \rangle$ *intersects* $\mathbf{M}$ *non-trivially.*

Let $\mathbf{R}_T := \mathbf{C}_T \cdot \mathbf{C}_{T+1} \cdot \mathbf{C}_{T+2} \cdot \ldots \cdot \mathbf{C}_{26}$ be the product of the rest of the cyclic groups in our list. (In consequence, $\mathbf{R}_{27}$ is the trivial group.) Thus

$$\mathbf{M} \quad = \quad \mathbf{F}_{T-1} \cdot \mathbf{C}_T \cdot \mathbf{R}_{T+1}\,,$$

for each value $T = 1, 2, \ldots, 26$.

Proof of FT of abelian p-groups

FTSOContradiction, suppose that $\mathbf{M} \neq \mathbb{G}$, and consider an element

$$\boldsymbol{\beta} \;\in\; \mathbb{G} \smallsetminus \mathbf{M}\,.$$

Then $B \geqslant J \geqslant 1$ where, thanks to (4),

$$5^B := \mathrm{Ord}(\boldsymbol{\beta}) \quad \text{and} \quad 5^J := \mathbf{M}\text{-}\mathrm{Ord}\boldsymbol{\beta}\,,$$

and $\mu := \boldsymbol{\beta}^{5^J}$ is in $\mathbf{M}$. Now $\mu \neq \varepsilon$, courtesy (6) and (3*). So there is a *unique* stage $T \in [1\,..\,26]$ with

$*$: $$\mu \;\in\; \mathbf{R}_T \smallsetminus \mathbf{R}_{T+1}\,.$$

Maximize the stage. Arrange to have taken a $\boldsymbol{\beta} \in \mathbb{G} \smallsetminus \mathbf{M}$ which *maximizes the corresponding stage* T from $(*)$. WELOGenerality, $\boxed{T = 18}$. So let

$$\mathbf{F} := \mathbf{F}_{17} \quad \text{and} \quad \mathbf{C} := \mathbf{C}_{18} \quad \text{and} \quad \mathbf{R} := \mathbf{R}_{19}\,.$$

I.e, $\mu \in \mathbf{C} \cdot \mathbf{R}$. Hence $\langle \mu \rangle \perp \mathbf{F}$. So

$$\langle \boldsymbol{\beta} \rangle \perp \mathbf{F}\,,$$

thanks to Prop'n 3.

History. For specificity of notation, suppose that $^{\#}\mathbf{C} = 5^{96}$. I claim that

7: $$96 \;\geqslant\; B\,.$$

After all, at stage T=18, transverse to $\mathbf{F}$ we chose a cyclic subgroup with maximum cardinality. Since $\langle \boldsymbol{\beta} \rangle$ is transverse to $\mathbf{F}$, yet we chose $\mathbf{C}$ (=$\mathbf{C}_{18}$), it must be that $^{\#}\mathbf{C}$ dominates $^{\#}\langle \boldsymbol{\beta} \rangle$.

The Contradiction. We now find an element $\boldsymbol{\beta}_0$ in the $\boldsymbol{\beta}\mathbf{M}$ coset satisfying that

$$\boldsymbol{\beta}_0^{5^J} \;\in\; \mathbf{R} \;\overset{\text{note}}{=\!=}\; \mathbf{R}_{19}\,.$$

This will contradict the maximality of stage T.

The Generator Lemma allows us to write

$$\mu \quad = \quad \gamma^{5^K} \cdot \rho\,,$$

where γ generates $\mathbf{C}$ with $\rho \in \mathbf{R}$, and where $K \in [1\,..\,96]$. It suffices to show this.

Goal: $\boxed{\textit{The difference } K - J \textit{ is non-negative.}}$

Why does this suffice? Well, in that circumstance

$$\boldsymbol{\beta}_0 \quad := \quad [\gamma^{-1}]^{5^{K-J}} \cdot \boldsymbol{\beta}$$

is well-defined. Raising $\boldsymbol{\beta}_0$ to power 5^J yields

$$[\gamma^{-1}]^{5^K} \cdot \mu \quad = \quad [\gamma^{-1}]^{5^K} \cdot \gamma^{5^K} \cdot \rho \quad \overset{\text{note}}{=\!=} \quad \rho\,.$$

And ρ is in $\mathbf{R}$.

Establishing the Inequality. Let $X := \text{Ord}(\mu)$. Because $\gamma^{5^K} \in \mathbf{C}$ and $\mathbf{C} \perp \mathbf{R}$, we have that $[\gamma^{5^K}]^X = \boldsymbol{\varepsilon}$. In other words,

$$5^K \cdot X \;\big|\bullet\; {}^{\#}\mathbf{C} \;=\; 5^{96}\,.$$

From (4*), recall that $X = 5^{B-J}$. So

$$K + B - J \quad \geqslant \quad 96\,.$$

Inevitably, then, $K - J \geqslant 96 - B$. This latter difference, thanks to (7), is non-negative. ♦

Uniqueness. Exercise.

The General Theorem

Suppose α and β are *commuting elements* of some group $\mathbb{G}$, and have orders A and B. Then

$$\text{Ord}(\alpha\beta) \textit{ is a divisor of } \text{Lcm}(A, B).$$

An Lcm of PoPs is a PoP, so each divisor is a PoP. In an **abelian** $\mathbb{G}$, then, the set

$$\mathbf{W}_p \quad := \quad \Big\{ \boldsymbol{\beta} \in \mathbb{G} \;\Big|\; \begin{matrix}\text{Ord}(\boldsymbol{\beta}) \text{ is some} \\ \text{power of } p\end{matrix} \Big\}$$

is a sub***group***, for each prime p. Let PRIMES be the set of all primes. Then the collection

$$8\text{:} \qquad \Big\{ \mathbf{W}_p \;\Big|\; p \in \text{PRIMES} \Big\}$$

is a transverse family.[♡1] So to complete the proof of the Fund Thm of Finite Abelian Groups, we need but prove the following.

9: *Suppose that $\mathbb{G}$ has no elements of infinite order. Then family (8) generates <u>all</u> of $\mathbb{G}$.*

In particular, this happens when $\mathbb{G}$ is finite.

[♡1] If $\boldsymbol{\beta}$ is in $\mathbf{W}_5$ and also the subgroup generated by $\{\mathbf{W}_p\}_{p\neq 5}$, then the order of $\boldsymbol{\beta}$ is simultaneously a power of 5, and is co-prime to 5. So $\boldsymbol{\beta}$ is $\boldsymbol{\varepsilon}$.

Proof of (9). . Consider a non-identity element $\boldsymbol{\beta}$, and factor its order as $N = p_1^{E_1} \cdot \ldots \cdot p_J^{E_J}$ into a product of powers of distinct primes. We will produce elements $\nu_j \in \mathbf{W}_{p_j}$ and integers M_j, so that

$$\dagger\text{:} \qquad {\nu_1}^{M_1} \cdot {\nu_2}^{M_2} \cdot \ldots \cdot {\nu_J}^{M_J} \;=\; \boldsymbol{\beta}\,.$$

How? Well, the numbers $r_j := N \big/ [{p_j}^{E_j}]$. are collectively relatively prime. Hence there exist integers M_j with

$$\ddagger\text{:} \qquad \sum_{j=1}^{J} r_j M_j \;=\; 1\,.$$

The element

$$\nu_j \;:=\; \boldsymbol{\beta}^{r_j}$$

has order ${p_j}^{E_j}$, so it is in $\mathbf{W}_{p_j}$. And (†) holds, courtesy (‡). ♦

Filename: `Problems/Algebra/abelian-gps.latex`
As of: *Thursday 23Feb2006.* Typeset: *23Sep2017 at 14:35.*