Fund. Theorem of Finite Abelian Groups : Algebra

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
30 September, 2022 (at *17:44*)

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

Overview. We work inside a fixed gp $(\mathbb{G}, \cdot, \varepsilon)$. 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 $^{\#}\mathbb{G} = p^N$, for a posint N and prime p, then we call $\mathbb{G}$ a "p-group". The standing notational assumption is that $\mathbb{G} \supset \mathsf{M},\mathsf{F}$ are groups and $\beta \in \mathbb{G}$ is a particular element. I use Greek letters $\beta, \mu, \gamma, \nu \ldots$ 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 p-group, then it is a finite product of cyclic p-groups. ◊

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

Tools. Let "$\mathsf{M} \perp \mathsf{F}$" indicate trivial intersection, $\mathsf{M} \cap \mathsf{F} = \{\varepsilon\}$; we say that M is ***transverse*** to 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 only soln to eqn*

$$\left[\prod_{\theta\in\Theta} b_\theta\right] = \varepsilon\,, \qquad \text{with each } b_\theta \in \mathbf{C}_\theta, \text{ and all but finitely-many equaling } \varepsilon,$$

is every $b_\theta = \varepsilon$; the trivial soln.

If we choose to enumerate $\mathcal{C}$ as $\mathbf{C}_1, \mathbf{C}_2, \ldots,$ then $\mathcal{C}$ is transverse IFF each n satisfies

$$\mathbf{C}_n \quad \perp \quad \left[\mathbf{C}_1 \cdot \mathbf{C}_2 \cdots \mathbf{C}_{n-1}\right]. \qquad \text{◊}$$

Use $\mathrm{Ord}(\beta)$ for the smallest posint d st. $\beta^d = \varepsilon$.

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

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

3*: $$\langle\beta\rangle \cap \mathsf{M} = \langle\mu\rangle\,.$$

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

$$\text{If} \quad \langle\mu\rangle \perp \mathsf{F} \quad \text{then} \quad \langle\beta\rangle \perp \mathsf{F}\,.$$

Furthermore, $\mathrm{Ord}(\beta) = \mathsf{M}\text{-}\mathrm{Ord}(\beta) \cdot \mathrm{Ord}(\mu)$. ◊

Pf. Let P comprize those posints j with $\beta^j \in \mathsf{M}$. Fixing a $j \in P$, Bézout's lemma tells us $D := \mathrm{GCD}(j, d)$ is in P. Thus $D \geq \mathrm{Min}(P) = d$. But $D \bullet\!\!| \; d$, so $D = d$. Hence (3*), since $d = D \bullet\!\!| \; j$. ♦

Remark. Henceforth "5" represents a arbitrary prime p. Use ***PoF*** to mean "power of 5".

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

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

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

where $5^B := \mathrm{Ord}(\beta) \geq \mathsf{M}\text{-}\mathrm{Ord}(\beta) =: 5^J$ 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 $\mathbf{C}$*-generator* $\gamma = \gamma(\nu)$ *and some* $K = K(\nu) \in [0\,..\,L]$. ◊

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 $n \perp 5$. Hence $n \perp |\mathbf{C}|$, so element $\gamma := {\gamma_0}^n$ generates $\mathbf{C}$. ♦

Prelims. 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

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

be the product of the first T many chosen groups. So F_0 is the trivial group $\{\boldsymbol{\varepsilon}\}$. Each F_T is a group, since $\mathbb{G}$ is abelian.

Construction. At stage T, with F_{T-1} chosen:

> *If there exists a cyclic group* $\mathbf{C} \perp \mathsf{F}_{T-1}$, *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 $\mathsf{M} := \mathsf{F}_{26}$ be this maximal product. We thus have

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

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

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

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

Proof of FT of abelian p-groups

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

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

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

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

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

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

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

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

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

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

thanks to Prop'n 3.

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

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

After all, at stage T=18, transverse to F we chose a cyclic subgroup with maximum cardinality. Since $\langle \boldsymbol{\beta} \rangle$ is transverse to 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 $\boldsymbol{\beta}\mathsf{M}$ coset satisfying that

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

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 $\rho \in \mathsf{R}$, and $K \in [1\,..\,96]$. 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 R.

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

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

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

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

Inevitably, then, $K - J \geq 96 - B$. 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

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

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

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

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

8: $$\left\{ \mathbf{W}_p \;\middle|\; p \in \textsc{Primes} \right\}$$

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.

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

†: $$\nu_1^{M_1} \cdot \nu_2^{M_2} \cdot \ldots \cdot \nu_J^{M_J} \quad = \quad \boldsymbol{\beta}\,.$$

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

‡: $$\sum_{j=1}^{J} r_j M_j \quad = \quad 1\,.$$

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: *30Sep2022 at 17:44.*

[♡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 $\boldsymbol{\varepsilon}$.