Group Notes

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
27 March, 2024 (at *17:36*)

Terms. A general group might be written $\mathbf{(}G, \cdot, \mathbf{e)}$ or $\mathbf{(}\Gamma, \cdot, \boldsymbol{\varepsilon}\mathbf{)}$ or $\mathbf{(}G, \cdot, 1\mathbf{)}$ or $\mathbf{(}G, +, 0\mathbf{)}$. The symbol for the neutral [i.e, identity] element may change, according to whether the group name is a Greek letter, or whether the group is written multiplicatively or additively. A *vectorspace* might be written as $\mathbf{(V, +, 0)}$ or $\mathbf{(U, +, 0)}$. A group of *functions*, under composition, might be written $\mathbf{(}G, \circ, Id\mathbf{)}$.

We *may* use $\mathbb{1}$ (blackboard bold '1') for the *trivial group*, but more often will write $\{\mathbf{e}\}$ or $\{0\}$ or $\{1\}$ as appropriate.

For the N^{th} *cyclic* group, use $\mathbb{Z}_N$ or $\mathbf{(}\mathbb{Z}_N, \mathbf{+)}$ when written additively, but use $\mathbb{Y}_N$ or $\mathbf{(}\mathbb{Y}_N, \mathbf{\cdot)}$ when written multiplicatively. The ***Klein-4*** group $\mathbb{V}_4$, the ***Vierergruppe***, is isomorphic to $\mathbb{Y}_2 \times \mathbb{Y}_2$. [So $\mathbb{V}_4 = \{\mathbf{e}, a, b, c\}$ is a commutative-gp with $a^2 = b^2 = c^2 = \mathbf{e}$ and $abc = \mathbf{e}$.]

Use $\mathbb{S}_N$, $\mathbb{D}_N$ for the N^{th}, *symmetric* and *dihedral* groups. So $|\mathbb{S}_N| = N!$ and $|\mathbb{D}_N| = 2N$ and $|\mathbb{Y}_N| = N$.

The ***alternating group*** $\mathbb{A}_N$ is the subgroup of $\mathbb{S}_N$ comprised of *even permutations*. So $|\mathbb{A}_0| = |\mathbb{A}_1| = 1$; otherwise, $|\mathbb{A}_N|$ is $N!/2$. [An arbitary set Ω engenders its symmetric group $\mathbb{S}_\Omega$ of permutations, but there is no corresponding alternating group unless Ω is *finite*.]

When each element of G has finite order, we call G a ***torsion group***.

To "***conjugate*** g *by element* x" means to form expression $x{\cdot}g{\cdot}x^{-1}$. For an arbitrary exponent $n \in \mathbb{Z}$, note that $[xgx^{-1}]^n = [xg^nx^{-1}]$.

The "***commutator*** *of elements* α *and* β" is

$$[\![\alpha, \beta]\!] \;:=\; \alpha\beta\alpha^{-1}\beta^{-1}$$

(which differs from $[\alpha, \beta]$, the standard notation).

1: Intersection-of-subgroups Lemma. *Suppose $\mathcal{C}$ is a (possibly infinite) collection of subgroups of group G. Then*

$$\bigcap(\mathcal{C}) \stackrel{def}{=} \bigcap_{H \in \mathcal{C}} H$$

is a G-subgroup. *Proof.* Exercise. ◊

ADDENDUM: A union of subgroups is *rarely* a group, since the union is usually not sealed under the gp-operation.

Morphisms

A map $F{:}G{\to}\Gamma$ is a ***homomorphism*** [more precisely, a "***group homomorphism***"] if

¥: $$\forall\, y,x,g \in G:\quad F(y\cdot x) \;=\; F(y)\cdot F(x) \quad \textit{and}$$
$$F(g^{-1}) \;=\; [F(g)]^{-1}\,.$$

The *set* of such homomorphisms is written as $\mathrm{Hom}(G{\to}\Gamma)$ or $\mathrm{Hom}(\Gamma{\leftarrow}G)$ or, more standardly, as $\mathrm{Hom}(G,\Gamma)$.

This F is an ***isomorphism*** if F is a bijection *and* $F^{-1}{:}\Gamma{\to}G$ is a homomorphism. While the following is not necessarily true in other branches of mathematics, for groups [and rings] we have:

2: Fact. *If a homomorphism is a bijection, then it automatically is an isomorphism.* *Proof.* Exercise.♢

When $\Gamma = G$, then a homomorphism is called an ***endomorphism***, and an isomorphism is called an ***automorphism***. My abbreviations are:

$G{\to}\Gamma$	$G{\to}G$
hom = *homomorphism*,	***endo*** = *endomorphism*,
iso = *isomorphism*,	***aut*** = ***auto*** = *automorphism*.

The set $\mathrm{Aut}(G)$ of automorphisms $G{\to}G$ forms a *group* under composition: the group $\big(\mathrm{Aut}(G),\circ,Id_G\big)$.

The endomorphisms $f{:}G\circlearrowright$ form $\big(\mathrm{End}(G),\circ,Id_G\big)$; a *monoid*.

Inner automorphisms. Each $x \in G$ yields an ***inner automorphism*** of G defined by

$$J_x(g) \;:=\; x{\cdot}g{\cdot}x^{-1}\,.$$

To "***conjugate*** g by element x" means to form expression xgx^{-1}. The set $\mathrm{Inn}(G) := \{J_x\}_{x\in G}$ forms a group, $\big(\mathrm{Inn}(G),\circ,Id_G\big)$, which is a subgroup of $\mathrm{Aut}(G)$. [Indeed, a *normal* subgp (defined later) of $\mathrm{Aut}(G)$.]

The map $\mathcal{J}{:}G{\to}\mathrm{Aut}(G)$ by $\mathcal{J}(x) := J_x$, is a group homomorphism.

NB 1: A BEST (Bright Energetic STudent) asked: *In defn* (¥) *of gp-hom, is condition* $\forall g : F(g^{-1}) = F(g)^{-1}$ *necessary?*

Ans: *Good catch; no!* Writing the gps as $(G,\mathbf{e})$ and (Γ,ε), let $\mu := F(\mathbf{e})$. So $\mu{\cdot}\mu = F(\mathbf{e}){\cdot}F(\mathbf{e}) = F(\mathbf{e}{\cdot}\mathbf{e}) = F(\mathbf{e}) = \mu$. So $\mu = \varepsilon$, since Γ has inverses. We've shown: $F(\mathbf{e})$ *must be* ε.

Set $\nu := F(g^{-1})$. Then $F(g^{-1}){\cdot}F(g) = F(g^{-1}\cdot g) = \varepsilon$. Multiply from the right by $[F(g)]^{-1}$ yields $[F(g)]^{-1} = F(g^{-1})$. □

NB 2: In contrast to homomorphism between *groups*, a homomorphism between *monoids* does want an extra condition

Let $\mathcal{P} := \mathcal{P}(\mathbb{R})$, the family of subsets of $\mathbb{R}$. Then $(\mathcal{P},\cup,\mathbb{R})$ is a commutative monoid; the binary operation is union of sets, and the identity element is $\mathbb{R}$ itself.

Fix an arbitrary "target" set $\tau \in \mathcal{P}$. Define $F{:}\mathcal{P}{\to}\mathcal{P}$ by $F(X) := \tau$; a constant-fnc. This F satisfies

∗: $$\forall A,B \in \mathcal{P}:\quad F(A\cup B) \;=\; F(A)\cup F(B)\,,$$

since $\tau{\cup}\tau = \tau$. Yet the *only* identity element in $\mathcal{P}$ is $\mathbb{R} \in \mathcal{P}$; so our F does *not* send the identity-elt to the identity-elt; *ouch!*

Thus our defn of ***monoid homomorphism*** F from monoid $(\mathsf{M},\mathbf{e})$ to monoid $(\mathsf{M}',\mathbf{e}')$ should have $F(\mathbf{e}) = \mathbf{e}'$ as part of the defn; condition $(*)$ is not sufficient by itself. □

Nota Bene 3: In a semigroup $(S,\cdot)$, hence monoid and group,, an element τ is ***idempotent*** (or is "*an idempotent element*") if $\tau{\cdot}\tau = \tau$. The above powerset-monoid is weird in that *every* element is idempotent. □

NB 4: The space of functions from a set Ω to itself, is a monoid under $\circ$, fnc-composition, with identity element Id_Ω, the identity-fnc $\omega \mapsto \omega$. So a *function* f is *idempotent* if $f\circ f = f$.

In contrast, "f is an *involution*" means $f\circ f = Id_\Omega$. □

Centralizer/Normalizer. The ***centralizer*** of an element $\mathbf{b} \in G$ is the subgroup

$$\mathcal{C}(\mathbf{b}) \;=\; \mathcal{C}_G(\mathbf{b}) \;:=\; \{x \in G \mid x\mathbf{b}x^{-1} = \mathbf{b}\}\,.$$

The centralizer of a sub*set* $S \subset G$ is

$$\mathcal{C}(S) \;=\; \mathcal{C}_G(S) \;:=\; \bigcap_{\mathbf{b}\in S} \mathcal{C}_G(\mathbf{b})\,.$$

I.e, each inner-aut J_x fixes S *pointwise*. [Note $\mathcal{C}_G(\{\mathbf{b}\})$ and $\mathcal{C}_G(\mathbf{b})$ are synonyms.] When S is the whole group, rather than $\mathcal{C}_G(G)$, we use notation $\mathcal{Z}(G)$ for the ***center***[♡1] of G; those elts that commute with everyone.

The ***normalizer*** of a subset $S \subset G$ is subgroup

$$\mathcal{N}(S) \;=\; \mathcal{N}_G(S) \;:=\; \{x \in G \mid xSx^{-1} = S\}\,.$$

So $x \in \mathcal{N}_G(S)$ says that inner-aut J_x fixes S *as a set*, but might permute its elements.

For a sub*group* $H \subset G$, automatically $\mathcal{N}_G(H) \supset H$. When its normalizer is everything, $\mathcal{N}_G(H) = G$, then we say "H is ***normal*** in G" and write $H \lhd G$ or $G \rhd H$. By defn, $H \lhd \mathcal{N}_G(H)$.

3: N/C Theorem (#17[P.203]). *Consider G, subgroup H, its normalizer $\mathcal{N} := \mathcal{N}_G(H)$ and centralizer $\mathcal{C} := \mathcal{C}_G(H)$. This leads to a group-homomorphism $F{:}\mathcal{N}\to\mathrm{Aut}(H)$ defined by restricting an $\mathcal{N}$-inner-automorphism to H:*

∗: $$F(x) \;:=\; J_x\!\downarrow_H .$$

Then $\mathrm{Ker}(F)$ is our $\mathcal{C}$, whence quotient $\mathcal{N}/\mathcal{C}$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

If index $|\mathcal{N}{:}\mathcal{C}|$ is finite, then

∗∗: *Index $|\mathcal{N}{:}\mathcal{C}|$ divides $\mathrm{Ord}(\mathrm{Aut}(H))$.* ♢

Proof. The index is the cardinality of quotient group $Q := \frac{\mathcal{N}}{\mathcal{C}}$, which is isomorphic to $F(\mathcal{N})$, a subgp of $\mathrm{Aut}(H)$. Now apply Lagrange. ♦

[♡1] From German *Zentrum*.

Equiv-relation result

The thms here proceed by putting an equivalence relation $\sim$ on a set Λ, then showing that the equiv-classes have a common cardinality $\boldsymbol{\kappa}$. Hence

†: $$\boldsymbol{\kappa} \cdot M \;=\; |\Lambda|$$

where M is the number of equiv-classes.

4a: Lagrange's theorem (#7.1^{P}142). *Consider H, a subgroup of group G. Then*

†: $$|H| \cdot \left[\begin{smallmatrix}\text{Number of } H \text{ in } G\end{smallmatrix}\ \begin{smallmatrix}\text{left-cosets}\end{smallmatrix}\right] \;=\; |G|\,.$$

When G is finite, then, $\mathrm{Ord}(H)$ divides $\mathrm{Ord}(G)$. ♢

Proof. Define binrel $\sim_{\mathsf{L}}$ on G by $\alpha \sim_{\mathsf{L}} \beta$ iff $\alpha^{-1}\beta \in H$. Evidently reflexive and symmetric, we establish transitivity. Suppose $a \sim_{\mathsf{L}} b$ and $b \sim_{\mathsf{L}} c$. Then $H \ni a^{-1}b,\ b^{-1}c$. Thus $H \ni a^{-1}b \cdot b^{-1}c \overset{\text{note}}{=\!=} a^{-1}c$.

ISTShow each $\sim_{\mathsf{L}}$ equiv-class E is bijective with H. Fix an $\boldsymbol{\alpha}\in\mathsf{E}$. For $h \in H$, note $\boldsymbol{\alpha}^{-1}\cdot\boldsymbol{\alpha}h$ lies in H; hence $\boldsymbol{\alpha}h \in \mathsf{E}$. Thus injection $f(h) \coloneqq \boldsymbol{\alpha}h$ indeed maps H into E.

To see that f is surjective, fix a target $\tau \sim_{\mathsf{L}} \boldsymbol{\alpha}$. Then $\widehat{h} \coloneqq \boldsymbol{\alpha}^{-1}\tau$ lies in H. And $f(\widehat{h}) \overset{\text{note}}{=\!=} \tau$. ♦

Remark. The $\sim_{\mathsf{L}}$ equiv-classes are called the "***left-cosets*** of H in G". The *in-same-right-coset* relation, $\alpha \sim_{\mathsf{R}} \beta$, is $\beta\alpha^{-1} \in H$. □

Ques. *Q1.* Suppose G is finite, and posint $D \bullet\!\!\mid \mathrm{Ord}(G)$. Must G have a cyclic subgp of order D? How about just a (non-cyclic) subgp? □

No. The N^{th} dihedral group $\mathbb{D}_N$ is generated by *flip-on-Vertical-axis* $\mathtt{F}$, and an order-N *rotation* $\mathtt{R}$.

Although $\mathrm{Ord}(\mathbb{D}_{15}) = 30$ and $6 \bullet\!\!\mid 30$, nonetheless $\mathbb{D}_{15}$ has *no* elt of order 6: Its 15 "flip elts", $\mathtt{R}^i\mathtt{F}$, each have order 2. And inside the order-15 rotation-subgp there are certainly no order-6 elts, courtesy Monsieur Lagrange.

BTWay, the divisors k of 15 are $15, 5, 3, 1$. The number of elts in $\langle \mathtt{R} \rangle_{\mathbb{D}_{15}}$ of each of these orders is

k	15	5	3	1
$\varphi(k)$	8	4	2	1

And $8+4+2+1 = 15$.[♡2]

[♡2] Indeed, this yields a proof that $\sum_{d \bullet\!\!\mid N} \varphi(d)$ equals N.

Although $\mathbb{D}_{15}$ has no *element* of order-6, it does have a sub*group* of order 6. The 6-element subgroup $\langle \mathtt{F}, \mathtt{R}^5 \rangle$ is isomorphic to $\mathbb{D}_3$. ♦

4b: Really *really* No. *Although $\mathrm{Ord}(\mathbb{A}_4) = 12$ and $6 \bullet\!\!\mid 12$, nonetheless $\mathbb{A}_4$ has no subgroup of order 6:* ♢

Proof. The cycle-structures for even permutations on four tokens are

Cyc-struct	$\lceil 1,1,1,1 \rfloor$	$\lceil 2,2 \rfloor$	$\lceil 3,1 \rfloor$
Order	1	2	3
How many	1	$\frac{1}{2}\cdot\binom{4}{2} = 3$	$2\cdot\binom{4}{1} = 8$

And $1+3+8 = 12 = |\mathbb{A}_4|$.

Let H be the *alleged* order-6 subgp of $\mathbb{A}_4$. Necessarily there is a $\beta \in H$ with cyc-struct $\lceil 3,1 \rfloor$. If H owned a $\lceil 2,2 \rfloor$ elt α, then $\alpha' \coloneqq \beta\alpha\beta^{-1}$ would have to be a *different* $\lceil 2,2 \rfloor$. (Because there are only 4 tokens, there is only one way [upto isomorphism] a $\lceil 2,2 \rfloor$ can interact with a $\lceil 3,1 \rfloor$, and they cannot commute.) But then H includes the Klein-4[♡3] group $\langle \alpha, \alpha' \rangle$. Yet $4 \nmid 6$.

The upshot is that no elt of $H \smallsetminus \{\mathsf{e}\}$ is $\lceil 2,2 \rfloor$, so each is a $\lceil 3,1 \rfloor$. And there are $6 - 1 = \mathbf{5}$ of them.

Applying the below (5b) to H, says that $5 \bullet\!\!\mid \varphi(3)$. But $5 \nmid 2$. ♦

5a: *Defn.* For a (possibly infinite) group G and posint D, define

$$S_{D,G} \;\coloneqq\; \{x \in G \mid \mathrm{Ord}(x) = D\}\,.$$

On $S_{D,G}$ define relation: $x \sim_D y$ IFF $\langle x \rangle_G = \langle y \rangle_G$. □

5b: Phi-divides Lemma (#4.4Coro^{P}84). *With $S_{D,G}$ and $\sim_D$ from above: $x \sim_D y$ IFF $x \in \langle y \rangle$. In particular, each equivalence class has precisely $\varphi(D)$ many elements. So*

†: $$\varphi(D) \;\; \textit{divides} \;\; |S_{D,G}|\,. \;\; \textit{Indeed,}$$
$$\varphi(D) \cdot M \;=\; |S_{D,G}|\,,$$

where M counts the cyclic order-D subgroups of G. ♢

[♡3] Why must α & α' commute? [Hint: Permuting only 4 tokens.]

Pf ($\Leftarrow$). By hypothesis, $\langle x\rangle \subset \langle y\rangle$. But these sets have the same, *finite*, cardinality. So they are equal.

An element $x \in G$ generates an order-D cyclic subgp IFF $x \in S_{D,G}$. So the order-D cyclic subgroups are in 1-to-1 correspondence with the above equivalence classes. ♦

6a: *Subset-product:* For sub*sets* $\mathsf{N}, \Gamma \subset G$, let $\mathsf{N}\Gamma$ mean the set of products $x\alpha$, over all $x \in \mathsf{N}$ and $\alpha \in \Gamma$. Even when N and Γ are sub*groups*, product $\mathsf{N}\Gamma$ need not be a subgroup.

E.g, let $\mathtt{R}, \mathtt{F}$ be the rotation and flip in $G := \mathbb{D}_3$. Subgroups $\mathsf{N} := \{\mathbf{e}, \mathtt{F}\}$ and $\Gamma := \{\mathbf{e}, \mathtt{FR}\}$ make $\mathsf{N}\Gamma$ equal $\{\mathbf{e}, \mathtt{F}, \mathtt{FR}, \mathtt{R}\}$. This is not a group, since it does not own $\mathtt{R}^2$. □

6b: Lemma. *If at least one of the subgroups $\mathsf{N}, \Gamma \subset G$ is normal in G, then $\Gamma\mathsf{N} = \mathsf{N}\Gamma$, and this product is itself a G-subgroup.* ♢

Proof. (Use letters $x, y \in \mathsf{N}$ and $\alpha, \beta \in \Gamma$.) WLOG $\mathsf{N} \lhd G$. Thus $x' := \beta x \beta^{-1}$ is an N-element. Hence $\beta x \in \Gamma\mathsf{N}$ equals $x'\beta$. Consequently, $\Gamma\mathsf{N} \subset \mathsf{N}\Gamma$. By symmetry, then, $\Gamma\mathsf{N} = \mathsf{N}\Gamma$.

Why is $\mathsf{N}\Gamma$ sealed under multiplication? Product $y\beta \cdot x\alpha$ equals $yx'\beta\alpha \overset{\text{note}}{\in} \mathsf{N}\Gamma$. Finally, the inverse element $x\alpha = \alpha^{-1}x^{-1}$ is in $\Gamma\mathsf{N} = \mathsf{N}\Gamma$. ♦

6c: Prop'n ($^{\#}\mathbf{7.2}^{P}144$). *Suppose K,$L \subset G$ are groups. Then*

$$\dagger: \qquad \begin{aligned} |K \cap L| \cdot |KL| &= |K{\times}L|\,. \quad \textit{I.e, product-set} \\ |KL| &= \frac{|K| \cdot |L|}{|K \cap L|}\,; \textit{needs } K \textit{ or } L \textit{ finite.} \end{aligned}$$

[*Note: Product-set KL may or may not be a group.*] ♢

Proof. Let $P := |K \cap L|$. By definition, the map

$$\ddagger: \qquad K{\times}L \to KL : (k, \ell) \mapsto k\ell$$

is onto. We now show that an elt $\kappa\lambda \in KL$ has precisely P many preimages under ($\ddagger$).

Each elt $c \in K \cap L$ yields $\kappa c \in K$ and $c^{-1}\lambda \in L$, with product $\kappa c \cdot c^{-1}\lambda$ equaling $\kappa\lambda$.

Conversely, a product $k\ell = \kappa\lambda$ yields a common element

$$\kappa^{-1}k = \lambda\ell^{-1} =: c \qquad \textit{in } K \cap L.$$

And $\kappa c = k$ and $c^{-1}\lambda = \ell$. So each c gives a preimage. ♦

7: Lemma. *Consider $F{:}G{\to}\Gamma$, a homomorphism. Then $F(G)$ [i.e, Range(F)] is a subgroup of Γ and*

†: $$|F(G)| \text{ divides } |G| \,. \quad \text{Indeed,}$$
$$|K| \cdot |F(G)| \;=\; |G|$$

where $K := \mathrm{Ker}(F)$. ◊

Proof. The F-inverse-image of each $\gamma \in \Gamma$ is a left-coset of K in G. (Using right-cosets also works, since $K \lhd G$.) ♦

8a: *Group actions.* The symbol $G \circlearrowleft \Omega$ means that gp G ***acts on*** set Ω; there is a gp-hom $\boxed{F{:}G{\to}\mathbb{S}_\Omega}$. For $g \in G$ and $\omega \in \Omega$, write the gp-action as

$$F_g(\omega) \text{ or } g(\omega) \text{ or just } g\omega.$$

Define the ***orbit*** and ***stabilizer*** of a point ω, and the ***fixed-pt set*** of a group-element g:

$$\begin{aligned} \mathcal{O}_F(\omega) &:= \{g\omega \mid g \in G\} &&\subset \Omega\,; \\ \mathrm{Stab}_F(\omega) &:= \{g \in G \mid g\omega = \omega\} &&\subset G\,; \\ \mathrm{Fix}_F(g) &:= \{\omega \in \Omega \mid g\omega = \omega\} &&\subset \Omega\,. \end{aligned}$$

This Stab(ω) is a subgp, but is rarely normal in G:

8b: $\forall f \in G$: $\quad f \cdot \mathrm{Stab}(\omega) \cdot f^{-1} \;=\; \mathrm{Stab}(f\omega)\,.$ □

8c: Orbit-Stabilizer Lemma. *For each* ***token*** $\omega \in \Omega$*:*

†: $$\mathrm{Ord}(\mathrm{Stab}_F(\omega)) \cdot |\mathcal{O}_F(\omega)| \;=\; \mathrm{Ord}(G)\,.$$ ◊

Proof. Let $H := \mathrm{Stab}(\omega)$. Say two elements $g, h \in G$ are "equivalent", $g \sim h$, if $g(\omega) = h(\omega)$. [Written out, $F_g(\omega) = F_h(\omega)$.] Evidently, the equiv-class of g is simply the left-coset gH. These equivalence-classes partition G; hence (†). ♦

Normalizer mod Centralizer

Call a posint N is ***Grouply unique*** if the cyclic group is the *only* group of order N. We get a sufficient condition for a product $p \cdot q$ to be grouply-unique. Here is a routine generalization of an elegant proof from Gallian.

9: Thm. *[#17P203] Suppose $p < q$ are prime numbers such that*

†: $\quad p-1 \nmid q-1$ *and*

‡: $\quad p \nmid q-1$.

Then the only group G of order $p \cdot q$ is cyclic. ♢

Setup. FTSOC we'll assume that G is not cyclic. Our goal is to exhibit *commuting* elts $h, k \in G$ of orders p and q, resp.. Necessarily, the product hk will have order pq. *To produce this miracle, ISTProve that*

∗: *G has a unique order-q subgp; call it K. Moreover, its centralizer $C_G(K)$ is all of G.*

The uniqueness implies that each elt $h \in G \smallsetminus K$ [such an h exists, since $pq > q$] necessarily has order p. And h commutes with each chosen $k \in K \smallsetminus \{\mathbf{e}\}$. □

Proof of (∗). We proceed in four steps.

There exists an order-q element in G. FTSOC, suppose no elt $x \in G \smallsetminus \{\mathbf{e}\}$ has order-q; so each x has order-p. Hence the Phi-divides Lemma says $\varphi(p) \overset{\text{note}}{=\!=} p-1$ must divide $\mathrm{Ord}(G) - 1$. Observe

$$pq - 1 \;=\; [p-1]q + [q-1]\,,$$

so this would imply $p-1 \bullet\!\!| \; q-1$. But this ⚡s (9†).

The upshot: There exists an order-q cyclic subgp $K \subset G$.

This order-q subgp is unique. Were there another, call it $\widehat{K}$, then

$$\widehat{K} \cap K \;=\; \{\mathbf{e}\}\,,$$

since q is prime. From (6c†), then,

$$|\widehat{K}K| \;=\; \tfrac{q \cdot q}{1}\,.$$

But inequality $|G| \geq |\widehat{K}K|$ implies $p \geq q$; a contradiction. So there is but one order-q subgp.

The normalizer $\mathcal{N}_G(K) = G$. Conjugating K must give a subgp isomorphic to K; thus is K itself.

The centralizer is all of G. Let $\mathcal{C} := C_G(K)$ denote the centralizer. Since K is cyclic, it is abelian. So $K \subset \mathcal{C} \subset G$. By Lagrange's thm, then,

$$q \;\bullet\!\!|\; \mathrm{Ord}(\mathcal{C}) \;\bullet\!\!|\; pq\,.$$

Since p is prime, *ISTShow that* $\mathrm{Ord}(\mathcal{C}) \neq q$.

Were $\mathrm{Ord}(\mathcal{C}) = q$ [i.e $\mathcal{C} = K$], then the quotient group

$$\frac{\mathcal{N}_G(K)}{\mathcal{C}} \overset{\text{note}}{=\!=} \frac{G}{K}$$

would have order $\frac{pq}{q} = p$. This quotient is group-isomorphic to a subgp of $\mathrm{Aut}(K)$. Consequently

$$p \;\bullet\!\!|\; \mathrm{Ord}(\mathrm{Aut}(K))\,.$$

But K is cyclic so $\mathrm{Aut}(K)$ is isomorphic to $\mathbf{U}(q)$; i.e $|\mathrm{Aut}(K)| = \varphi(q)$. Thus p divides $\varphi(q) \overset{\text{note}}{=\!=} q-1$. But this annoys (9‡). ♦

What are some examples of this thm?

Works: $p < q$	Hypothesis fails: $p < q$	What exactly fails?
	$3 < q$	$2 \bullet\!\!| \; q-1$ (†)
	$3 < 7$	$3 \bullet\!\!| \; 6$ (‡)
$5 < 23$	$5 < 13$	$4 \bullet\!\!| \; 12$ (†)
$5 < 19$	$5 < 11$	$5 \bullet\!\!| \; 10$ (‡)
$7 < 11$	$7 < 13$	$6 \bullet\!\!| \; 12$ (†)
$7 < 17$	$7 < 29$	$7 \bullet\!\!| \; 28$ (‡)
$7 < 53$	$7 < 51$	*Ahem!*
$11 < 13$	$11 < 67$	$11 \bullet\!\!| \; 66$ (‡)

Dull CEX. For p=2, and q an odd prime, dihedral group $|\mathbb{D}_q| = 2q$, yet $\mathbb{D}_q$ is not cyclic. The hyp. that fails is that $2-1$ divides $q-1$. □

Interesting CEX. Here $p{=}3$ and $q{=}7$; let $\equiv$ mean $\equiv_7$.

In mult-gp $\mathbf{U}(7)$ [which has 6 elts] let $\Omega := \{1, 2, 4\}$. This Ω is a subgp of $\mathbf{U}(7)$, as $2{\cdot}2 \equiv 4$ and $2{\cdot}4 \equiv 1$.

Let $\mathcal{G}$ be comprise the 2×2 matrices of form

$$\begin{bmatrix} \alpha & x \\ 0 & 1 \end{bmatrix} \quad \textit{with } \alpha \in \Omega \textit{ and } x \in \mathbb{Z}_7.$$

Multiplying two such matrices gives

$$*: \qquad \begin{bmatrix} \alpha & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \beta & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha\beta & \alpha y + x \\ 0 & 1 \end{bmatrix},$$

(arithmetic mod-7), showing the mult. is well-defined. The inverse of $\begin{bmatrix} \alpha & x \\ 0 & 1 \end{bmatrix}$ is $\begin{bmatrix} \alpha^{-1} & -\alpha^{-1}x \\ 0 & 1 \end{bmatrix}$, so $\mathcal{G}$ *is* a group, whose order is $\mathrm{Ord}(\Omega){\cdot}\mathrm{Ord}(\mathbb{Z}_7) = 3 \cdot 7$.

Finally, $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, whereas in the other order, $\left[\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 & 2 \\ 0 & 1 \end{smallmatrix}\right]$. So $\mathcal{G}$ is non-abelian. □

Still interesting. Let's compute the number of elts of each order in the above $\mathcal{G}$. Consider a non-id element $g := \left[\begin{smallmatrix} \alpha & x \\ 0 & 1 \end{smallmatrix}\right]$. Our $\mathcal{G}$ is not cyclic, so the possible orders of g are $3, 7$.

First take $\alpha = 1$: Computing, $\left[\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right]^N = \left[\begin{smallmatrix} 1 & Nx \\ 0 & 1 \end{smallmatrix}\right]$. Hence $Nx \equiv 0$; so $N \equiv 0$ since $x \not\equiv 0$. Thus

$$\mathrm{Ord}\left(\left[\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right]\right) \;=\; 7\,,$$

and there are 6 such elements. Luckily, 6 is divisible by $\varphi(7)$.

Consider $\alpha{\neq}1$: Cubing, $\left[\begin{smallmatrix} \alpha & x \\ 0 & 1 \end{smallmatrix}\right]^3 = \left[\begin{smallmatrix} \alpha^3 & Z \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & Z \\ 0 & 1 \end{smallmatrix}\right]$, where Z is $[\alpha^2 + \alpha + 1]x$. Now $[\alpha^2 + \alpha + 1][\alpha - 1]$ equals $[\alpha^3 - 1] \equiv 0$. In $\mathbb{Z}_7$ we may divide by $\alpha - 1$ to conclude that $[\alpha^2 + \alpha + 1] \equiv 0$, whence $Z \equiv 0$. So

$$\mathrm{Ord}\left(\left[\begin{smallmatrix} \alpha{\neq}1 & x \\ 0 & 1 \end{smallmatrix}\right]\right) \;=\; 3\,,$$

and there are $21 - 7 = 14$ such elements. Happily, 14 is a multiple of $\varphi(3){=}2$. □

Cyclic groups

I'll use $(\mathbb{Z}_N, +)$ when writing a cyclic group *additively*, but will use $(\mathbb{Y}_N, \cdot)$ when writing *multiplicatively*. The infinite group $\mathbb{Y}_\infty$ is iso to $(\mathbb{Z}, +)$.

Defn. For $x \in G$ we use $\text{Periods}_G(x)$ for the set of integers k with $x^k = \mathbf{e}$.

For a *subgroup* $H \subset G$, let $P_H(x) = P_{H,G}(x)$ be $\{k \in \mathbb{Z} \mid x^k \in H\}$. So $\text{Periods}(x)$ is simply $P_H(x)$, when H is the trivial subgp $\{\mathbf{e}\}$. □

11: Periods Lemma. *Fix G, H, x as above, and let P_H mean $P_H(x)$. If P_H is not just $\{0\}$, then $P_H = N\mathbb{Z}$, where N is the least positive element of P_H.*

For G-subgroups $H \supset K$, then,

$$\text{H-Ord}_G(x) \;\bullet\!\!\!\!\!\!\mid\; \text{K-Ord}_G(x) \;\bullet\!\!\!\!\!\!\mid\; \text{Ord}_G(x)\,. \qquad \Diamond$$

Proof. Suppose $N := \text{Min}(\mathbb{Z}_+ \cap P_H)$ is finite. Fixing a $k \in P_H$, we will show that $k \bullet\!\!\!\!\!\!\mid N$.

Set $D := \text{GCD}(N, k)$. LBolt (well, Bézout's lemma) produces integers such that $D = NS + kT$. Hence $D \in P_H$, since x^D equals $[x^N]^S \cdot [x^k]^T = \mathbf{e}^S \cdot \mathbf{e}^T$. Thus $N = D \bullet\!\!\!\!\!\!\mid k$. ♦

12: *Defn.* Use $\text{H-Ord}(x)$ or $\text{H-Ord}_G(x)$ for the above N; else, if P_H is just $\{0\}$ then $\text{H-Ord}(x) := \infty$. Call this the "***$H$-order*** of x". The ***order*** of x, written $\text{Ord}(x)$ or $\text{Ord}_G(x)$, is simply $\text{H-Ord}_G(x)$ when $H := \{\mathbf{e}\}$. □

Suppose $H \lhd G$. Now $[xH]^k = x^k H$, so $[xH]^k = H$ IFF $x \in H$. In terms of the quotient group,

11′:
$\forall x \in G$: $\text{Ord}_{G/H}(xH) = \text{H-Ord}_G(x) \bullet\!\!\!\!\!\!\mid \text{Ord}_G(x)\,.$

Dihedral groups

The ***Klein-4*** group is isomorphic to $\mathbb{Y}_2 \times \mathbb{Y}_2$. Sometimes called the ***Vierergruppe***, it has presentation

13:
$$V := \left\langle \mathtt{a}, \mathtt{b}, \mathtt{c} \;\middle|\; \begin{array}{l}\text{Each of } \{\mathtt{a},\mathtt{b},\mathtt{c}\} \text{ is an involution,}\\ \text{each pair commutes, and the prod-}\\ \text{uct of each two equals the third.}\end{array} \right\rangle.$$

Using fewer generators, but less symmetric, is this presentation:

13′: $$V = \langle \mathtt{a}, \mathtt{b} \mid \mathtt{a}^2 = \mathbf{e} = \mathtt{b}^2,\ \mathtt{a} \leftrightarrows \mathtt{b} \rangle\,.$$

For each posint N, the N^{th} ***dihedral group*** is

14: $$\begin{aligned} \mathbb{D}_N &:= \langle \mathtt{R}, \mathtt{F} \mid \mathtt{F}^2 = \mathbf{e},\ \mathtt{FRFR} = \mathbf{e},\ \mathtt{R}^N = \mathbf{e} \rangle\,; \\ \mathbb{D}_\infty &:= \langle \mathtt{R}, \mathtt{F} \mid \mathtt{F}^2 = \mathbf{e},\ \mathtt{FRFR} = \mathbf{e} \rangle\,, \text{ for } N = \infty. \end{aligned}$$

Now for some straightforward facts.

15: Fact. *For all $N \in [1\,..\,\infty]$ and integers j:*

$$\mathtt{R}^j \cdot \mathtt{F} = \mathtt{F} \cdot \mathtt{R}^{-j}\,.$$

Lastly, $\text{Ord}(\mathbb{D}_N) = 2N$, *and* $\text{Ord}(\mathbb{D}_\infty) = \aleph_0$. ◊

16: Lemma. *Groups $\mathbb{D}_1 \cong \mathbb{Y}_2$ and $\mathbb{D}_2 \cong \mathbb{Y}_2 \times \mathbb{Y}_2$ (the Vierergruppe), so each has full center and trivial* Inn()*-group.*

For each $N \in [3\,..\,\infty]$:

Both $\mathcal{Z}(\mathbb{D}_\infty)$ and $\mathcal{Z}(\mathbb{D}_{Odd\,N})$ are trivial. Consequently $\text{Inn}(\mathbb{D}_\infty) \cong \mathbb{D}_\infty$ *and* $\text{Inn}(\mathbb{D}_{Odd\,N}) \cong \mathbb{D}_N$.

When $N = 2K$ is even: Center $\mathcal{Z}(\mathbb{D}_{2K}) = \{\mathbf{e}, \mathtt{R}^K\}$. Consequently $\mathbb{D}_K \cong \text{Inn}(\mathbb{D}_{2K})$ via the map

$$*: \qquad \mathtt{R}^j \mapsto J_{\mathtt{R}^j} \quad \text{and} \quad \mathtt{R}^j\mathtt{F} \mapsto J_{\mathtt{R}^j\mathtt{F}}\,. \qquad \Diamond$$

Proof. The commutator $[\![\mathtt{R}^j, \mathtt{F}]\!]$ equals

$$\mathtt{R}^j\mathtt{F}\mathtt{R}^{-j}\mathtt{F}^{-1} = \mathtt{R}^{2j}\mathtt{F}^2 = \mathtt{R}^{2j}\,.$$

Thus $\mathtt{R}^j \leftrightarrows \mathtt{F}$ IFF $2j \bullet\!\!\!\!\!\!\mid N$. So the only possible nt-element in the center is $\mathtt{R}^K$, where $N = 2K < \infty$.

Finally, map $(*)$ *is* a homomorphism, and *is* onto, since $\mathtt{R}^K$ commutes with each element of $\mathbb{D}_{2K}$ and thus each $J_{\mathtt{R}^{K+j}} = J_{\mathtt{R}^j}$ and $J_{\mathtt{R}^{K+j}\mathtt{F}} = J_{\mathtt{R}^j\mathtt{F}}$. ♦

Misc. theorems

Temporarily here.

17: Lemma. *For each $N \geq 2$, the full symmetric group $\mathbb{S}_N$ is generated by an N-cycle $\nu := (b_0, b_1, b_2, \ldots, b_{N-1})$ together with $\tau := (b_0, b_1)$; an "adjacent" 2-cycle.* ♢

Proof. WLOGenerality, $N \geq 3$.

ISTShow subgroup $\langle \nu, \tau \rangle$ owns all transpositions. Hence, by our argument from class, ISTJust show that $\langle \nu, \tau \rangle$ owns all *adjacent* [relative to ν] transpositions.

Finally, note that $\nu^{-1}\tau\nu = (b_1, b_2)$. Etc. ♦

18a: Cauchy's Thm for *abelian* groups (#**9.5**^{P}*182*). *Suppose $N := |G| < \infty$ where G is an abelian group, written multiplicatively. If prime $p \bullet\!\!| N$, then there exists $y \in G$ with $\mathrm{Ord}(y) = p$.* ♢

Proof. [From the web.] Enumerate G as $g_1, g_2, \ldots, g_N$ and let $K_1, \ldots, K_N$ be their orders. ISTProve that

$$p \bullet\!\!| \widetilde{K} := \prod_{n=1}^{N} K_n ,$$

since then, p must divide *some* K_n [since p is prime]; say, $p \bullet\!\!| K_2$. And then, $y := {g_2}^{[K_2/p]}$ has order p.

Additive group $\widetilde{G} := \mathbb{Z}_{K_1} \times \ldots \times \mathbb{Z}_{K_N}$ has order $\widetilde{K}$. The map

$$f{:}\widetilde{G}{\to}G \quad \text{by} \quad f(\mathbf{(}\ell_1, \ldots, \ell_K\mathbf{)}) := {g_1}^{\ell_1} {g_2}^{\ell_2} \cdots {g_N}^{\ell_N}$$

is onto, since $f(\mathbf{(}1, 0, \ldots, 0\mathbf{)}) = g_1$, etc.. And f is a group-homomorphism since G is abelian. Thus $\mathrm{Ord}(G) \bullet\!\!| \mathrm{Ord}(\widetilde{G})$. Hence $p \bullet\!\!| \mathrm{Ord}(G) \bullet\!\!| \widetilde{K}$. ♦

A more standard proof uses induction on quotient groups.

Pf of (18a). WELOG $p := 5$. We may assume that

18b: *If Q is a finite abelian group with $\mathrm{Ord}(Q) \not\bullet 5$, then Q owns an element of order 5.*

holds for each group Q with $|Q| < |G|$.

It suffices to produce a $y \in G$ with $\mathrm{Ord}_G(y) \not\bullet 5$. [*Why? Power ${y}^{\mathrm{Ord}(y)/5}$ has order 5.*]

Since $|G| > 1$ we can pick a nt-element $h \in G$; WLOG $K := \mathrm{Ord}(h) \not\bullet 5$. Thus 5 divides $\frac{N}{K}$, which is the order of $Q := \frac{G}{H}$, where $H := \langle h \rangle$. Automatically $H \lhd G$ since G is abelian. Finally, $h \neq \mathbf{e}$ so $|Q| < |G|$.

Since quotient Q is abelian, our (18b) applies to produce an element $y \in G$ with whose coset yH has order 5 in Q. I.e

$*$: *Power $y^5 \in H$, yet $y \notin H$.*

Thus $\mathrm{Ord}_G(y) \overset{\text{note}}{=\!=} 5 \cdot \mathrm{Ord}_H(y^5)$ is a multiple of 5. ♦

Normality

Consider two gps $H \subset G$. Say that "H is ***normal*** in G" , written $H \lhd G$, if $[\forall x \in G\colon xHx^{-1} = H]$. This is equivalent (see (25), below) to $[\forall x \in G\colon xHx^{-1} \subset H]$. However, an individual element x could give *proper* inclusion, as the following two examples show.

Proper inclusion, $xHx^{-1} \subsetneqq H$, forces that $|H| = \infty$ and $\mathrm{Ord}(x) = \infty$ and that G is not abelian.

19: *E.g.* Let $G := \mathbb{S}_{\mathbb{Z}}$. Let $H \subset G$ comprise those permutations $h\colon \mathbb{Z} \circlearrowleft$ st. $[\forall n < 0\colon h(n) = n\,]$; i.e, $h\restriction_{\mathbb{Z}_-}$ is the identity-fnc.

Define $x \in G$ by $x(n) := n{-}5$. For n negative,

$$\dagger\colon \qquad n \overset{x}{\longmapsto} n{-}5 \overset{h}{\longmapsto} n{-}5 \overset{x^{-1}}{\longmapsto} n\,,$$

for an arbitrary $h \in H$. Consequently, $xHx^{-1} \subset H$.

Note that (†) holds for all $n{<}5$. So no elt $\eta \in H$ which *moves* something in $[0\,..\,5)$, e.g, $\eta(2) = 3$, can possibly be in xHx^{-1}. We have thus $xHx^{-1} \subsetneqq H$, *proper* inclusion. □

20: *E.g.* [See file.] In $G := \mathrm{GL}_2(\mathbb{Q})$, the shear $\mathsf{S} := \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ generates $H := \langle \mathsf{S} \rangle_G$, which is a copy of $(\mathbb{Z}, +)$. Conjugating by $\mathsf{X} := \left[\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ produces $\boxed{\mathsf{XSX}^{-1} = \mathsf{S}^2}$. Consequently,

$$\mathsf{X}H\mathsf{X}^{-1} \;=\; \left\{ \left[\begin{smallmatrix} 1 & 2n \\ 0 & 1 \end{smallmatrix}\right] \,\middle|\, n \in \mathbb{Z} \right\}.$$

This is a *proper* subset of H. □

Strengthening normality

Relation $\mathsf{N}\triangleleft G$ is equivalent to $[\forall x \in G\colon J_x(H) \subset H]$. By enlarging the set of endomorphisms under which this inclusion holds, we get successively stronger versions of normality.

Defn. Two subgroups $\mathsf{N}, \Gamma \subset \widehat{G}$ are ***transverse*** , written $\mathsf{N} \perp \Gamma$, if $\mathsf{N} \cap \Gamma = \{\mathbf{e}\}$. Always, the map

21: $$f\colon \mathsf{N}\times\Gamma \to \mathsf{N}\Gamma\,, \quad \text{by } \mathbf{(}x,\omega\mathbf{)} \mapsto x\omega,$$

is onto. It is injective IFF N and Γ are transverse. The following result characterises direct product. □

22: Direct-product Lemma. *Suppose $\mathsf{N}, \Gamma \subset \widehat{G}$ groups, with $\mathsf{N} \triangleleft \widehat{G}$, and $\mathsf{N} \perp \Gamma$. Let*

$$G \;:=\; \langle \mathsf{N}, \Gamma \rangle_{\widehat{G}} \overset{\text{note}}{=\!=} \mathsf{N}\Gamma\,.$$

Recalling the bijection. $f\colon \mathsf{N}\times\Gamma \to G$ from (21), the following are equivalent:

i: $\mathsf{N} \leftrightarrows \Gamma$, *inside* G.
ii: f *is a homomorphism, hence isomorphism.*
iii: $\Gamma \triangleleft G$. ♢

Pf (i)⇒(ii). Does f respect multiplication? Checking,

$$f(\mathbf{(}x,\alpha\mathbf{)}) \cdot f(\mathbf{(}y,\beta\mathbf{)}) \overset{\text{def}}{=\!=} x\alpha \cdot y\beta \;=\; xy\alpha\beta\,,$$

since $\mathsf{N} \leftrightarrows \Gamma$. And this equals $f(\mathbf{(}xy, \alpha\beta\mathbf{)})$. ♦

Pf (ii)⇒(iii). Always $\{\mathbf{e}\}\times\Gamma \triangleleft \mathsf{N}\times\Gamma$. Now apply f. ♦

Pf (iii) ⇒ (i). With $x \in \mathsf{N}$ and $\alpha \in \Gamma$, we need to show that $\boxed{x\alpha x^{-1}\alpha^{-1} = \mathbf{e}}$.

Note that $\alpha x^{-1}\alpha^{-1} \in \mathsf{N}$, since $\mathsf{N} \triangleleft \widehat{G}$. Hence

$$x \cdot \alpha x^{-1}\alpha^{-1} \;\in\; \mathsf{NN} \;\subset\; \mathsf{N}\,.$$

And $x\alpha x^{-1} \in \Gamma$, since $\Gamma \triangleleft G$. So $x\alpha x^{-1} \cdot \alpha^{-1} \in \Gamma$. Thus $[\![x, \alpha]\!] \in \mathsf{N} \cap \Gamma$, so $[\![x, \alpha]\!] = \mathbf{e}$. ♦

Defn. Let $\mathrm{SurEnd}(G)$ denote the monoid of *surjective endomorphisms* of G. Evidently

23: $$\mathrm{Inn}(G) \;\subset\; \mathrm{Aut}(G) \;\subset\; \mathrm{SurEnd}(G) \;\subset\; \mathrm{End}(G)\,.$$

Any of these inclusions can be strict, depending on the group.

Here are various strengthenings of the notion "*H is a normal subgroup of G*". They are defined by how many homomorphisms $F\colon G\circlearrowright$ send H into itself.

Suppose that $\boxed{F(H) \subset H}$ for *every* ...

24:

Which Homs?	Then written as
$\ldots\ F \in \mathrm{Inn}(G)$	$H \triangleleft G$
$\ldots\ F \in \mathrm{Aut}(G)$	$H \overset{\text{Aut}}{\triangleleft} G$
$\ldots\ F \in \mathrm{SurEnd}(G)$	$H \overset{\text{Sur}}{\triangleleft} G$
$\ldots\ F \in \mathrm{End}(G)$	$H \overset{\text{End}}{\triangleleft} G$

25: *Note.* In the $H \triangleleft G$ and $H \overset{\text{Aut}}{\triangleleft} G$ cases, we may conclude that each (inner-)automorphism α in fact gives *equality* $\boxed{\alpha(H) = H}$. This, because inclusion $F(H) \subset H$ must hold for both $F := \alpha$ *and* $F := \alpha^{-1}$. □

In the examples below, $H, K \subset \mathbf{(}G, \cdot, \mathbf{e}\mathbf{)}$ are groups. Abbrev the normalizer $\mathcal{N} := \mathcal{N}(H) := \mathcal{N}_G(H)$ and centralizer $\mathcal{C} := \mathcal{C}(H) := \mathcal{C}_G(H)$ of subgp H. □

26: *E.g.* Each $x \in G$ engenders a ***conjugation map*** $J_x\colon G\circlearrowright$ by

$$J_x(g) \;:=\; xgx^{-1}\,.$$

Easily $J_y \circ J_x = J_{yx}$. Conjugations are called ***inner automorphisms*** of G; the group of conjugations is written $\mathrm{Inn}(G)$. This map

27: $$\mathcal{J}\colon G \twoheadrightarrow \mathrm{Inn}(G) : x \mapsto J_x$$

is a surjective gp-homomorphism. Its kernel is the center $\mathcal{Z}(G)$. So $\mathcal{Z}(G) \triangleleft G$ and

28: $$\mathrm{Inn}(G) \;\cong\; \tfrac{G}{\mathcal{Z}(G)}\,.$$

A slight generalization, taking a subgp H, is to map

27′: $$\mathcal{J}_H : \mathcal{N}_G(H) \to \mathrm{Aut}(H) \;:\; x \mapsto J_x\restriction_H\,.$$

Its kernel is the centralizer $\mathcal{C}_G(H)$. So $\frac{\mathcal{N}(H)}{\mathcal{C}(H)}$ is group-isomorphic to the subgroup

$$A \;:=\; \mathrm{Range}(\mathcal{J}_H) \;\subset\; \mathrm{Aut}(H)\,. \qquad \square$$

29: Lemma. *Suppose* $\left|{}^{G}\!/_{H}\right| = 2$. *Then* $H \lhd G$. ♢

Pf. Pick $b \in G \smallsetminus H$. Since the index is 2,

$$[bH] \sqcup H \;=\; G \;=\; [Hb] \sqcup H\,.$$

Thus the left and right coset-partitions are equal. So $H \lhd G$. ♦

Remark. Index $\left|{}^{G}\!/_{H}\right| = 2$ need *not* imply the stronger $H \overset{\text{Aut}}{\lhd} G$. In the Vierergruppe, (13′), the $\langle a\rangle_V$ subgroup has index 2 in V. Yet the automorphism that exhanges a and b moves $\langle a\rangle$.

Also, $\left|{}^{G}\!/_{H}\right| = 3$ is not sufficient to imply normality. In $\mathbb{D}_3$, the non-normal subgp $\langle \mathtt{F}\rangle$ has index 3. [Conjugating, $J_{\mathtt{R}}(\mathtt{F}) = \mathtt{RFR}^{-1} = \mathtt{R}^2\mathtt{F} \neq \mathtt{F}$.] [Also: The natural embedding of $\mathbb{D}_4$ has index-3 in $\mathbb{S}_4$, yet is not a normal subgp.]□

30: Lem. *Consider groups* $H \subset G \subset F$. *Then*

31: $$[H \overset{\text{Aut}}{\lhd} G \overset{\text{Aut}}{\lhd} F] \implies H \overset{\text{Aut}}{\lhd} F\,.$$

32: $$[H \overset{\text{Aut}}{\lhd} G \lhd F] \implies H \lhd F\,.$$

And $[H \overset{\text{End}}{\lhd} G \overset{\text{End}}{\lhd} F] \Rightarrow H \overset{\text{End}}{\lhd} F$. *Proof.* Use (25). ♢

Ques. Does $[H \overset{\text{Sur}}{\lhd} G \overset{\text{Sur}}{\lhd} F]$ imply $H \overset{\text{Sur}}{\lhd} F$? A CEX necessarily has G infinite, since there would be a $F \in \text{SurEnd}(F)$ which maps G properly inside G.□

33: Normal Grabbag.

i: *For two subgps* H, K *of* G, *let* $\overset{?}{\lhd}$ *be the strongest normality so that both* $H, K \overset{?}{\lhd} G$. *Then the commutator-subgp* $[\![H, K]\!] \overset{?}{\lhd} G$.

ii: *The center* $\mathcal{Z}(G) \overset{\text{Sur}}{\lhd} G$, *but not necessarily* $\overset{\text{End}}{\lhd}$.

iii: $\text{Inn}(G) \lhd \text{Aut}(G)$, *but not necessarily* $\overset{\text{Aut}}{\lhd}$. ♢

Pf of (i). Take an-endomorphism $x \mapsto \widehat{x}$ of the appropriate type. Fix $h \in H$ and $k \in K$. By hypothesis, $\widehat{h} \in H$ and $\widehat{k} \in K$. Thus

$$[\![H, K]\!] \;\ni\; [\![\widehat{h}, \widehat{k}]\!] \overset{\text{note}}{=\!=} \widehat{[\![h, k]\!]}\,.$$ ♦

Pf of (ii). Take an onto-endomorphism $x \mapsto \widehat{x}$ and a point $z \in \mathcal{Z}(G)$. To show $\widehat{z} \in \mathcal{Z}(G)$, we fix a $g \in G$ and show that $g\widehat{z}g^{-1} = \mathbf{e}$. Since the endo is surjective, there exists an $\gamma \in G$ such that $\widehat{\gamma} = g$.

Now $z \leftrightarrows \gamma$, so $\mathbf{e} = \gamma z \gamma^{-1}$. Thus

$$\mathbf{e} \;=\; \widehat{\gamma z \gamma^{-1}} \;=\; \widehat{\gamma} \cdot \widehat{z} \cdot \widehat{\gamma}^{-1} \;=\; g \cdot \widehat{z} \cdot g^{-1}\,.$$ ♦

Pf of (ii)*bis.* We produce an endomorphism, of a group $G := \Omega{\times}D$, which carries its center $\mathcal{Z}(G)$ *outside* of itself. Here, $\Omega = \{\omega, \boldsymbol{\varepsilon}\}$ is an order-2 group generated by ω. And $D := \mathbb{D}_3$ is a dihedral group; use $\mathbf{e}$ for its neutral elt. So the center of G is

$$\mathcal{Z}(G) \;=\; \mathcal{Z}(\Omega) \times \mathcal{Z}(D) \;=\; \Omega \times \{\mathbf{e}\}\,.$$

Let $\mathtt{F}$ be a flip in $\mathbb{D}_3$; it generates an order-2 subgp $\{\mathtt{F}, \mathbf{e}\} =: F \subset D$. The Klein-4 group $\Omega{\times}F$ has an "exchange the generators" automorphism, $\mathcal{A}$, with

$$\begin{aligned} \mathcal{A}(\mathbf{(}\omega, \mathbf{e}\mathbf{)}) &:= \mathbf{(}\boldsymbol{\varepsilon}, \mathtt{F}\mathbf{)} \quad \text{and} \\ \mathcal{A}(\mathbf{(}\boldsymbol{\varepsilon}, \mathtt{F}\mathbf{)}) &:= \mathbf{(}\omega, \mathbf{e}\mathbf{)}\,. \end{aligned}$$

defined by exhanging the generators of subgps Ω and F. Finally, consider the endomorphism $\mathcal{E}{:}G{\to}G$ which collapses the D side:

$$\text{For all } \alpha \in \Omega \text{ and } x \in D\text{:} \quad \mathcal{E}(\mathbf{(}\alpha, x\mathbf{)}) := \mathbf{(}\alpha, \mathbf{e}\mathbf{)}\,.$$

Finally, the composition $\mathcal{E} \triangleright \mathcal{A}$ is a G-endo which carries $\Omega{\times}\{\mathbf{e}\}$ to $\{\boldsymbol{\varepsilon}\}{\times}F$. ♦

Pf of (iii). [See file.] Note that $\mathbb{D}_4$ has exactly two subgroups isomorphic to the Vierergruppe,

$$\begin{aligned} V &:= \langle \mathtt{R}^2, \mathtt{F}\rangle \;=\; \{\mathbf{e}, \mathtt{R}^2, \mathtt{F}, \mathtt{FR}^2\} \quad \text{and} \\ V' &:= \langle \mathtt{R}^2, \mathtt{FR}\rangle \;=\; \{\mathbf{e}, \mathtt{R}^2, \mathtt{FR}, \mathtt{FR}^3\}\,. \end{aligned}$$

And $\alpha(V) = V'$, where $\alpha \in \text{Aut}(\mathbb{D}_4)$ is the automorphism which sends $\mathtt{R} \mapsto \mathtt{R}$ and $\mathtt{F} \mapsto \mathtt{FR}$.

Now for the example. Let $G := \mathbb{D}_4$. Check that $A := \text{Aut}(\mathbb{D}_4) \cong \mathbb{D}_4$. Its subgp $S := \text{Inn}(\mathbb{D}_4) \cong \mathbb{D}_2$ is isomorphic to a Vierergruppe. One can interpret the above α as in $\text{Aut}(A)$, and as carrying S to the *other* copy of the Vierergruppe. ♦

Examples of normal subgps. On $\mathfrak{D}$-dim'al Euclidean space $\mathbb{R}^{\mathfrak{D}}$, let G_{Trans} be the group of translations. Then G_{Trans} is normal inside the gp of all isometries. Indeed, G_{Trans} is normal in the gp of invertible *affine maps* $\mathbb{R}^{\mathfrak{D}}\circlearrowleft$.

Proof. On $\mathbf{V} := \mathbb{R}^{\mathfrak{D}}$, each vector $\boldsymbol{\kappa} \in \mathbf{V}$ yields a translation $\mathsf{T}_{\boldsymbol{\kappa}}{:}\mathbf{V}\circlearrowleft$ by $\mathsf{T}_{\boldsymbol{\kappa}}(\mathbf{v}) := \mathbf{v} + \boldsymbol{\kappa}$. Evidently a linear $\mathsf{L}{:}\mathbf{V}\circlearrowleft$ has commutation

$$\mathsf{L} \circ \mathsf{T}_{\boldsymbol{\kappa}} \;=\; \mathsf{T}_{\mathsf{L}(\boldsymbol{\kappa})} \circ \mathsf{L}\,.$$

Consequently, a general (we want "invertible") affine map can be written $\mathsf{A} := \mathsf{L} \circ \mathsf{T}$, for some linear L and translation T;

So to show G_{Trans} normal in the affines, it is enough to conjugate by an invertible linear map, L. Our goal is to show that $\mathsf{L} \circ \mathsf{T}_{\boldsymbol{\kappa}} \circ \mathsf{L}^{-1}$ is some translation. But

$$\mathsf{L}\mathsf{T}_{\boldsymbol{\kappa}}\mathsf{L}^{-1} \;=\; \mathsf{L}\mathsf{L}^{-1}\mathsf{T}_{\mathsf{L}(\boldsymbol{\kappa})} \;=\; \mathsf{T}_{\mathsf{L}(\boldsymbol{\kappa})}\,. \qquad \blacklozenge$$

34: Observation. *There exist groups G with $\mathrm{Inn}(G) \cong G$, yet with center $\mathcal{Z}(G)$ non-trivial.* $\lozenge$

Proof. Let $G := \mathbb{D}_2 \times \mathbb{D}_4 \times \mathbb{D}_8 \times \mathbb{D}_{16} \times \ldots$. By (16), group $\mathrm{Inn}(G)$ equals

$$\begin{aligned} &\mathrm{Inn}(\mathbb{D}_2) \times \mathrm{Inn}(\mathbb{D}_4) \times \mathrm{Inn}(\mathbb{D}_8) \times \mathrm{Inn}(\mathbb{D}_{16}) \times \ldots \\ \cong\; &\mathbb{1} \quad \times \quad \mathbb{D}_2 \quad \times \quad \mathbb{D}_4 \quad \times \quad \mathbb{D}_8 \quad \times \ldots, \end{aligned}$$

which is isomorphic to G. $\blacklozenge$

Examples of homomorphisms. For posints K,L and cyclic gps $(\mathbb{Z}_K, +)$ and $(\mathbb{Z}_L, +)$, what is the set $H := \mathrm{Hom}(\mathbb{Z}_K \to \mathbb{Z}_L)$?

Let $D := \mathrm{GCD}(K, L)$ and write

$$K = D \cdot A \quad \text{and} \quad L = D \cdot B\,, \quad \text{where } A \perp B.$$

A homomorphism $f \in H$ is determined by where it sends 1; $f(y) = y \cdot f(1)$. This f is well-defined as long as it sends 0 and K to the same place. So we need that

$$0 \;\equiv_L\; f(K) \overset{\text{note}}{=\!=} DA \cdot f(1)\,.$$

I.e, $DA \cdot f(1) \;\vdots\; DB$. Hence we need $A \cdot f(1) \;\vdots\; B$. Since $A \perp B$, this latter is equiv to $f(1) \;\vdots\; B$. Writing $f(1) := jB$, we get D many homomorphisms

$$\mathrm{Hom}(\mathbb{Z}_K \to \mathbb{Z}_L) \;=\; \left\{ f_M \;\middle|\; \begin{array}{l} M = jB, \text{ where} \\ j \in [0\,..\,D) \end{array} \right\},$$

defined by $f_M(y) := [M \cdot y] \mod L$.

When $L = K$. Let E be the set of endomorphisms of $(\mathbb{Z}_K, +)$. So $(E, \circ)$ is a monoid; indeed, a commutative monoid It is semigp-isomorphic to $(\mathbb{Z}_K, \cdot)$. Its automorphism subgp is, of course, gp-isomorphic with $(\Phi(K), \cdot)$.

Ways to count in groups

35: Burnside's Lemma (#**29.1**[P]474). *Counting cardinalities,*

$$\dagger: \quad \sum_{\omega\in\Omega}|\mathrm{Stab}(\omega)| \overset{\#}{=} \big\{(g,\omega)\ \big|\ g\omega=\omega\big\} \overset{\#}{=} \sum_{g\in G}|\mathrm{Fix}(g)|\,.$$

Counting the number of G-orbits, then,

$$\ddagger: \quad {}^{\#}Orbits = \frac{1}{|G|}\cdot\sum_{g\in G}|\mathrm{Fix}(g)| = \left[\begin{matrix}\#\text{ of points fixed by an av-}\\ \text{erage element of } G\end{matrix}\right]. \qquad \Diamond$$

Proof. The number of G-orbits equals

$$\sum_{\omega\in\Omega}\frac{1}{|\mathcal{O}(\omega)|} \overset{\text{Orb-Stab, (8c*)}}{=\!=\!=} \frac{1}{|G|}\cdot\sum_{\omega\in\Omega}|\mathrm{Stab}(\omega)|\,.$$

Now apply (35†) to earn (35‡). ♦

Application: *Coloring a cube's faces.* Color the six faces of a cube red, white and blue; let Ω be the set of color-cubes; so $|\Omega| = 3^6$.

How many distinct colorings are there, up to orientation-preserving isometry? We will use Burnside's Lemma. The group, G, of orientation-preserving rotations of the cube has $6\cdot 4 = 24$ elts, and is group-isomorphic to $\mathbb{S}_4$.

In the 2nd column, below, remark that $1+6+3+8+6 = 24 = |G|$.

What isometry g?	How many such g?	${}^{\#}\mathrm{Fix}(g) = 3^F$.	$F :=$ #[Face-orbits under $\langle g\rangle$].
Id	1	3^6	1+1+1+1+1+1
FaceRot 90°	$\frac{6}{2}\cdot 2 = 6$	3^3	1+4+1
FaceRot 180°	$\frac{6}{2}\cdot 1 = 3$	3^4	1+2+2+1
VertexRot 120°	$\frac{8}{2}\cdot 2 = 8$	3^2	3+3
EdgeRot 180°	$\frac{12}{2}\cdot 1 = 6$	3^3	2+2+2

The sum $\frac{1}{24}\cdot[1\cdot 3^6 + 6\cdot 3^3 + 3\cdot 3^4 + 8\cdot 3^2 + 6\cdot 3^3]$ equals 57. Using K many colors, the number of K-colorings is $\frac{1}{24}\cdot[K^6 + 3K^4 + 12K^3 + 8K^2]$, i.e., is

$$36a: \quad K^2\cdot[K^4+3K^2+12K+8]\big/24. \quad \left[\begin{matrix}\text{Coloring}\\ \text{faces}\end{matrix}\right]$$

Coloring a cube's vertices. K-color the eight vertices of a cube. How many OP-isometry distinct colorings are there?

What isometry g?	${}^{\#}\{\text{such } g\}$	${}^{\#}\mathrm{Fix}(g) = K^V$.	$V :=$ #[Vertex-orbits under $\langle g\rangle$].
Id	1	K^8	$\lceil 1^8\rfloor$
FaceRot 90°	6	K^2	$\lceil 4^2\rfloor$
FaceRot 180°	3	K^4	$\lceil 2^4\rfloor$
VertexRot 120°	8	K^4	$\lceil 1^2, 3^2\rfloor$
EdgeRot 180°	6	K^4	$\lceil 2^4\rfloor$

The coeff of K^4 is $3+8+6 = 17$. So the number of vertex K-colorings is $\frac{1}{24}\cdot[K^8 + 17K^4 + 6K^2]$ i.e, is

$$36b: \quad K^2\cdot[K^6+17K^2+6]\big/24. \quad \left[\begin{matrix}\text{Coloring}\\ \text{vertices}\end{matrix}\right]$$

Coloring a cube's edges. K-color the twelve edges of a cube. How many OP-isometry distinct colorings are there?

What isometry g?	${}^{\#}\{\text{such } g\}$	${}^{\#}\mathrm{Fix}(g) = K^E$.	Cyc-sig, #[Edge-orbits under g].
Id	1	K^{12}	$\lceil 1^{12}\rfloor$, **12**
FaceRot 90°	6	K^3	$\lceil 4^3\rfloor$, **3**
FaceRot 180°	3	K^6	$\lceil 2^6\rfloor$, **6**
VertexRot 120°	8	K^4	$\lceil 3^4\rfloor$, **4**
EdgeRot 180°	6	K^7	$\lceil 1^2, 2^5\rfloor$, **7**

Collecting terms, the number of "*really different*" edge K-colorings is

$$\tfrac{1}{24}\cdot\left[K^{12}+6K^7+3K^6+8K^4+6K^3\right].$$

Plausible? Let $h(K) := K^{12}+6K^7+3K^6+8K^4+6K^3$. To verify $h(K) \vdots 24$, ISTCheck mod 3 and 8. Firstly,

$$h(K) \equiv_3 K^{12}-K^4 \equiv_3 \left\{\begin{matrix}0-0 = 0, & \text{when } K\equiv_3 0;\\ 1-1 = 0, & \text{when } K\equiv_3 \pm 1.\end{matrix}\right\}$$

We now work mod 8. WLOG K is odd [since K even has $8 \nmid K^3 \nmid h(K)$]. Now, $K^{\text{Even}}\equiv_8 1$ and $K^{\text{Odd}}\equiv_8 K$. So

$$\begin{aligned} h(K) &\equiv_8 K^{12}-2K^7+3K^6-2K^3\\ &\equiv_8 1-2K+3-2K \equiv_8 4\cdot[1-K] \equiv_8 0,\end{aligned}$$

since $[1-K]$ is even. □

Application: *Coloring a necklace.* Consider an necklace of N pearls, each of one of K colors.

Two necklaces are ***equivalent***, if we can rotate one to be the other. Let $\mathcal{L}_N(K)$ be the number of "really different" neck$\mathcal{L}$ace colorings. And let $\mathcal{B}_N(K)$ be the number of "really different" $\mathcal{B}$racelets colorings; we can turn a bracelet over; so $\mathbb{D}_N$ is the acting group.

Unfinished: as of 27Mar2024 [The formulas are correct, but there is not much explanation.]

$$\mathcal{L}_N(K) \;=\; \frac{1}{N}\sum_{\substack{(d,\ell)\text{ st.}\\ d\cdot\ell=N}} \varphi(d)\cdot K^{\ell}\,.$$

For bracelets, which one may turn over, dihedral group $\mathbb{D}_N$ acts.

$$\mathcal{B}_N(K) = \frac{1}{2N}\left[\mathsf{Flips}_N + \sum_{\substack{(d,\ell)\text{ st.}\\ d\cdot\ell=N}} \varphi(d)\cdot K^{\ell}\right] = \frac{\mathsf{Flips}_N}{2N} + \tfrac{1}{2}\mathcal{L}_N(K).$$

CASE: $N = 2H+1$ odd Each flip has $H{+}1$ orbits, and there are N many flips. So

$$\begin{aligned}\mathsf{Flips}_N \;&=\; N\cdot K^{H+1}\,. \quad \textit{Thus}\\ \mathcal{B}_N(K) \;&=\; \tfrac{1}{2}\mathcal{L}_N(K) \;+\; \tfrac{1}{2}K^{H+1}.\end{aligned}$$

CASE: $N = 2H$ even A flip through two edge-midpoints has H orbits, whereas a flip through two vertices has $H{+}1$ orbits, since each vertex [pearl] is fixed. There are H flips of each type, so

$$\begin{aligned}\mathsf{Flips}_N \;&=\; H\cdot\left[K^H + K^{H+1}\right] \;=\; H\cdot K^H[1+K].\ \textit{Thus}\\ \mathcal{B}_N(K) \;&=\; \tfrac{1}{2}\mathcal{L}_N(K) \;+\; \tfrac{1}{4}K^H[1+K].\end{aligned}$$

Class equation

Consider a finite group acting on a finite set, $G \circlearrowright \Omega$, and let S be its set of orbits. The trivial assertion $\boxed{|\Omega| = \sum_{\mathcal{O}\in S} |\mathcal{O}|}$ leads to a useful formula, when we consider G acting on itself via conjugation.

Universally fixed. The Orbit-Stabilizer thm restates the circled as

$$|\Omega| \;=\; \sum_{\omega\in \textit{All-Reps}} \frac{|G|}{|\mathrm{Stab}(\omega)|}\,,$$

where "*All-Reps*" stands for "all orbit representatives"; this is one token ω per G-orbit. Now let

$$\mathrm{UnivFix}(G) \;:=\; \textstyle\bigcap_{h\in G} \mathrm{Fix}(h)\,.$$

This is the set of ω in 1-point orbits, i.e, $\mathcal{O}(\omega) = \{\omega\}$.

Ex: 3×3 TTT. The TTT-aut group of $\Omega := [1\,..\,3]\times[1\,..\,3]$ is $\mathbb{D}_4$. And $\mathrm{UnivFix}(\mathbb{D}_4)$ is singleton $\{(2,2)\}$, since only the center-cell $(2,2)$ of the 3×3 board is unmoved by each automorphism. □

Let's pull out these ***trivial orbits*** and define

$$\textit{NT-Reps} \;:=\; \textit{All-Reps} \smallsetminus \mathrm{UnivFix}(G)\,;$$

this has one representative in each *non-trivial* orbit. We have a primordial ***class equation***,

$$\textbf{37:}\quad |\Omega| \;=\; |\mathrm{UnivFix}(G)| + \sum_{\omega\in \textit{NT-Reps}} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}\,.$$

Specializing to conjugation. We now let $\Omega := G$, and have G act on Ω by conjugation. So we have a homomorphism $\jmath{:}G\to\mathbb{S}_\Omega$ by $h \mapsto J_h$, where $J_h(\omega)$ equals $h\omega h^{-1}$.

Acting by conjugation, the stabilizer $\mathrm{Stab}_G(\omega)$ is the *centralizer* $\mathcal{C}_G(\omega)$. The orbit of ω is called its ***conjugacy class***, written

$$\mathfrak{CC}(\omega) \;:=\; \{h\omega h^{-1} \mid h\in G\}\,.$$

A conjugacy class is "non-trivial" if it has more than one point. So $\mathfrak{CC}(h)$ is trivial IFF $\mathcal{C}(h) = G$ IFF $h \in \mathcal{Z}(G)$, where $\mathcal{Z}(G) := \bigcap_{h\in G}\mathcal{C}(h)$ is the ***center*** of G. Below, let "$h \in$ All-$\mathfrak{CC}$" mean to take one representative h per $\mathfrak{CC}$. Let NT-$\mathfrak{CC}$ comprise one representative per **Non-Trivial** $\mathfrak{CC}$.

38: Class-Equation Thm (After#**24.1**P388). *For a finite group G,*

$$\textbf{38}'\textbf{:}\qquad |G| \;=\; |\mathcal{Z}(G)| + \sum_{h\in \text{NT-}\mathfrak{CC}} \frac{|G|}{|\mathcal{C}(h)|}\,.$$

Each summand $|G|/|\mathcal{C}(h)|$ is in $[2\,..\,|G|]$, and is a proper divisor of $|G|$. When G is abelian, the $\sum$-sum is empty, hence zero. ♢

Remark. A less useful form of the class-eqn does not separate out the size-1 conjugacy classes. It says

$$|G| \;=\; \sum_{h\in \text{All-}\mathfrak{CC}} \frac{|G|}{|\mathcal{C}(h)|}\,.$$ □

Proof. Everything has been shown, except for the observation that when the action is conjugation, then $\mathrm{UnivFix}(G)$ is the center $\mathcal{Z}(G)$. ♦

We get a nice corollary when G is a "p-group".

39: p-group non-trivial center (#**24.2**P389). *Suppose $|G| = p^L$, where p is prime and $L \in \mathbb{Z}_+$. Then $\mathcal{Z}(G)$ is non-trivial. (So $|\mathcal{Z}(G)| = p^K$ for some $K \in [1\,..\,L]$.)* ♢

Proof. The centralizer of each $h \in$ NT-$\mathfrak{CC}(G)$ is a *proper* subgroup, so p divides $|G|/|\mathcal{C}(h)|$. Hence p divides the sum on RhS(**??'**). So p divides $|\mathcal{Z}(G)|$. ♦

40: Cauchy's Thm for finite groups (After#**24.3**P391). *Suppose $N := |G| < \infty$. If prime $p \bullet\!\!|\, N$, then there exists $y \in G$ with $\mathrm{Ord}(y) = p$.* ♢

Proof. This holds when $G = \mathbb{1}$, so we may assume

$$\boxed{\textit{If } p \bullet\!\!|\, \mathrm{Ord}(Q) \textit{ then } Q \textit{ has an order-}p\textit{ element.}}$$

holds for each group Q with $|Q| < |G|$. So WLOG we may assume that each centralizer $\mathcal{C}(h)$, for h in NT-$\mathfrak{CC}(G)$, has order not a multiple of p. Thus p divides the RhS(**??'**) sum. So $p \bullet\!\!|\, \mathrm{Ord}(\mathcal{Z}(G))$.

We may now apply (18a), Cauchy's thm for *abelian* groups, to $\mathcal{Z}(G)$, to get a order-p element. ♦

Remark. We get a nice progression of proofs. Note that (18b) uses induction on quotient groups, but does not use the Class-Eqn, whereas p-group non-trivial center (39) uses the class equation but no induction. The above Cauchy's thm (40), used quotient-induction to put the class equation in play.

A jazzed-up (40) argument will give Sylow's first theorem. □

Defn. Fix a prime p. For each natnum k and finite group Q, define this proposition.

P(k,Q): *If* $p^k \bullet\!\!\!\mid \mathrm{Ord}(Q)$ *then* Q *has a subgroup of order* p^k.

We now show that this holds universally. □

41: Sylow's First Thm. *For each prime* p*, for each natural number* k *and finite group* G*, proposition* P(k,G) *holds.* ♢

Pf. Always P$(0,*)$ holds, so fixing a $K{\geq}1$ and finite group G, we show that P(K,G). We may assume that $\mathrm{Ord}(G) \not\bullet\!\!\!\mid p^K$ and

42: P$(K{-}1,*)$ *holds. Also* P(K,Q) *obtains, for each group* Q *with* $|Q|<|G|$.

So WLOG $p^K \not\downarrow \mathcal{C}_G(h)$, for each h in NT-$\mathcal{CC}(G)$. Thus p divides the $\sum$-sum in (**??'**). So $p \bullet\!\!\!\mid \mathrm{Ord}(\mathcal{Z}(G))$.

Cauchy's thm for abelian groups now gives us a subgroup $H \subset \mathcal{Z}(G)$ of order-p. Every subgp of the center is G-normal, so we have a quotient group $Q := \frac{G}{H}$, and p^{K-1} divides its order. By (42), this Q has a subgroup Q' of order p^{K-1}.

Lastly, $H' := \bigcup_{U\in Q'} U$ is a subgroup; it is a union of H-cosets U. And $|H'| = |H|\cdot|Q'| = p\cdot p^{K-1} = p^K$. ♦

Misc. counting results. We first state a theorem just for pedagogical purposes.

43: Lemma. *We have a subgroup* $H \subset \mathcal{Z}(G)$*. Suppose that each two left* H*-cosets,* H_1 *and* H_2*, have representatives* $y_i \in H_i$ *such that* $y_1 \leftrightarrows y_2$*. Then* G *is abelian.* ♢

Proof. Pick two arbitrary $x_i \in G$. By hyp., there are $y_i \in Hx_i$ which commute. Write x_i as $h_i y_i$. So x_1x_2 equals

$$\begin{aligned} y_1h_1[y_2h_2] &= y_1y_2h_2h_1\,, && \text{since } h_1 \in \mathcal{Z}(G),\\ &= y_2y_1h_2h_1\,, && \text{since } y_2 \leftrightarrows y_1,\\ &= y_2h_2y_1h_1\,, && \text{since } h_2 \in \mathcal{Z}(G). \end{aligned}$$

And this equals x_2x_1. ♦

An immediate corollary is this "G mod $\mathcal{Z}$" lemma.

44: G/Z Lemma. *We have a subgroup* $H \subset \mathcal{Z}(G)$*; necessarily* $H \lhd G$*. If* G/H *is cyclic, then* G *is abelian.* ♢

Remark. In the lemma, any of G, H or G/H may be infinite.

Hypothesis "G/H is cyclic" cannot be weakened to "G/H is abelian". For example, the 8 elt dihedral group $G := \mathbb{D}_4$ is non-abelian. It has presentation

$$G \;=\; \langle \mathtt{R},\mathtt{F} \mid \mathtt{F}^2 = \mathbf{e},\ \mathtt{FRFR} = \mathbf{e},\ \mathtt{R}^4 = \mathbf{e}\rangle\,.$$

Its center is $H := \{\mathbf{e}, \mathtt{R}^2\}$ and the quotient group G/H is isomorphic to $\mathbb{D}_2$, which *is* abelian ($\cong \mathbb{Z}_2{\times}\mathbb{Z}_2$). What goes wrong with the proof, below? Well, the two H-cosets $\{\mathtt{R},\mathtt{R}^3\}$ and $\{\mathtt{F},\mathtt{FR}^2\}$ have *no* representatives which commute. □

Proof. Pick an elt $z \in G$ so that coset zH generates the cyclic group $Q := G/H$. Each element of Q has form $[zH]^n$. Since H is G-normal, $[zH]^n = z^nH$. So we let z^n be our representative of coset $[zH]^n$. ♦

45: Lemma. *In group* G*, suppose commuting elements* a, c *have* ***different prime*** *orders* p *and* q*. Then*

$$\mathrm{Ord}(ac) \;=\; p\cdot q\,. \qquad ♢$$

Proof. Let $y := ac$. Were $y = \mathbf{e}$ then $p = \mathrm{Ord}(a) = \mathrm{Ord}(c^{-1}) = \mathrm{Ord}(c) = q$; ⋙. So $\mathrm{Ord}(y) \neq 1$.

Since $a \leftrightarrows c$,

$$\mathrm{Ord}(y) \bullet\!\!\!\mid \mathrm{LCM}(p,q) \overset{\text{note}}{=\!=} p\cdot q\,.$$

Were $\mathrm{Ord}(y) \bullet\!\!\!\mid p$, then $\mathbf{e} = [ac]^p = c^p$, so $p \not\bullet\!\!\!\mid \mathrm{Ord}(c)$. I.e $p \not\bullet\!\!\!\mid q$. Contradiction.

So $\mathrm{Ord}(y) \not\downarrow p$. Ditto $\mathrm{Ord}(y) \not\downarrow q$. But $\mathrm{Ord}(y) \bullet\!\!\!\mid pq$. Thus $\mathrm{Ord}(y) = pq$, ♦

Sylow Theorems

For a prime p, a **"*p-group*"** is a (finite) group whose order is a power of p. E.g, a p-group for p=5 has order in $\{1, 5, 25, 125, \ldots\}$.

Normal subgroups

For this section N is a natnum. Here is the theorem we are shooting for:

46: Thm. *For each $N \in \mathbb{N} \smallsetminus \{4\}$, the alternating group $\mathbb{A}_N$ is simple.* ♢

Remark. The alternating groups $\mathbb{A}_0, \mathbb{A}_1, \mathbb{A}_2$ (i.e, comprising all the even permutations) are each the triv-gp, hence simple. Since Ord($\mathbb{A}_3$)=3 is prime, group $\mathbb{A}_3$ is simple. So the first case we need consider is $N \geq 5$. Some of the lemmas below hold for lower N.

Let a ***solo* 3-*cycle*** mean a perm whose cycle lengths are $3, 1, 1, \overset{N-3}{\ldots} 1$. □

47: 3-cycle Lemma. *The solo 3-cycles generate $\mathbb{A}_N$.* ♢

Proof.

48: Lemma. *Suppose $\pi \in \mathbb{A}_N$ has a 3-cycle. Let K be the smallest normal subgp of $\mathbb{A}_N$ owning π. Then K has a solo 3-cycle.* ♢

Proof.

§A Appendix: (Semi)group Axioms

Semigroups & Monoids. A ***semigroup*** is a pair $(S, \bullet)$, where $\bullet$ is an associative *binary operation* [***binop***] on set S. A special case is a ***monoid***. It is a triple $(S, \bullet, \mathbf{e})$, where $\bullet$ is an associative binop on S, and $\mathbf{e} \in S$ is a two-sided identity elt.

Axiomatically:

G1: Binop $\bullet$ is ***associative***, i.e $\forall \alpha,\beta,\gamma \in S$, necessarily $[\alpha \bullet \beta] \bullet \gamma = \alpha \bullet [\beta \bullet \gamma]$.

G2: Elt $\mathbf{e}$ is a ***two-sided identity element***, i.e $\forall \alpha \in S$: $\alpha \bullet \mathbf{e} = \alpha$ and $\mathbf{e} \bullet \alpha = \alpha$.

Moreover, we call S a ***Group*** if t.fol also holds.

G3: Each elt admits a ***two-sided inverse element***: $\forall \alpha$, $\exists \beta$ such that $\alpha \bullet \beta = \mathbf{e}$ and $\beta \bullet \alpha = \mathbf{e}$.

When the binop is '+', *addition*, then write the inverse of α as $-\alpha$ and call it "***negative*** α". We then use 0 for the id-elt.

When the binop is '*multiplication*', write the inverse of α as α^{-1} and call it the "***reciprocal*** of α" We use 1 for the id-elt. Usually, one omits the binop-symbol and writes $\alpha\beta$ for $\alpha \bullet \beta$.

For an *abstract* binop '$\bullet$', we often write α^{-1} for the inverse of α ["α inverse"], and omit the binop-symbol. If $\bullet$ is ***commutative*** [$\forall \alpha,\beta$, necessarily $\alpha \bullet \beta = \beta \bullet \alpha$] then we call S a ***commutative group***.

Rings/Fields. A ***ring*** is a five-tuple $(\Gamma, +, 0, \cdot, 1)$ with these axioms.

R1: Elements 0 and 1 are distinct; $0 \neq 1$.

R2: Triple $\big(\Gamma, +, 0\big)$ is a commutative group.

R3: Triple $\big(\Gamma, \cdot, 1\big)$ is monoid.

R4: Mult. ***distributes-over*** addition from the *left*, $\alpha[x + y] = [\alpha x] + [\alpha y]$, and from the *right*, $[x + y]\alpha = [x\alpha] + [y\alpha]$; this, for all $\alpha,x,y \in \Gamma$.

Our Γ is a ***commutative ring*** (abbrev.: ***commRing***) if the multiplication is commutative.

When Γ is commutative: Say that $\alpha \bullet\!\!| \ \beta$ [α ***divides*** β] if *there exists* $\mu \in \Gamma$ s.t $\alpha\mu = \beta$. This is the same relation as $\beta \ |\!\!\bullet \ \alpha$ [β is a multiple of α].

Zero-divisors. Fix $\alpha \in \Gamma$. Elt $\beta \in \Gamma$ is a "***(two-sided) annihilator*** of α" if $\alpha\beta = 0 = \beta\alpha$. An α is a ***(two-sided) zero-divisor*** if it admits a *non-zero* annihilator. So 0 is a ZD, since $0 \cdot 1 = 0 = 1 \cdot 0$, and $1 \neq 0$. We write the *set* of Γ–zero-divisors as

$$\mathrm{ZD}_\Gamma \quad \text{or} \quad \mathrm{ZD}(\Gamma)\,.$$

[E.g: In the $\mathbb{Z}_{15}$ ring, note $9 \not\equiv 0$ and $10 \not\equiv 0$, yet $9{\cdot}10$ *is* $\equiv 0$. So each of 9 and 10 is a "*non-trivial zero-divisor* in $\mathbb{Z}_{15}$".]

An $\alpha \in \Gamma$ is a Γ-***unit*** if $\exists \beta \in \Gamma$ st. $\alpha\beta = 1 = \beta\alpha$. Use

$$\mathbf{U}_\Gamma \quad \text{or} \quad \mathbf{U}(\Gamma)$$

for the units group. In the special case when Γ is $\mathbb{Z}_N$, I will write Φ_N for its units group, to emphasize the relation with the Euler-phi fnc, since $\varphi(N) := |\Phi_N|$. [Some texts use $\mathbf{U}(N)$ for the $\mathbb{Z}_N$ units group.]

Integral domains, Fields. A ***commutative ring*** is a ring in which the multiplication is commutative. A commRing with no (non-zero) zero-divisors [that is, $\mathrm{ZD}_\Gamma = \{0\}$] is called an ***integral domain*** (***intDomain***), or sometimes just a ***domain***.

An intDomain F in which every non-zero element is a unit [i.e $\mathbf{U}(F) = F \setminus \{0\}$] is a ***field***. That is to say, F is a commRing where triple $\big(F \setminus \{0\}, \cdot, 1\big)$ is a group.

Examples. The fields we know are: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and, for p prime, $\mathbb{Z}_p$.

Every ring has the "trivial zero-divisor" —zero itself. The ring of integers doesn't have others. In contrast, the non-trivial zero-divisors of $\mathbb{Z}_{12}$ comprise $\{\pm 2, \pm 3, \pm 4, 6\}$.

In $\mathbb{Z}$ the units are ± 1. But in $\mathbb{Z}_{12}$, the ring of integers mod-12, the set of units, $\Phi(12)$, is $\{\pm 1, \pm 5\}$. In the ring $\mathbb{Q}$ of rationals, *each* non-zero element is a unit. In the ring $\mathbb{G} := \mathbb{Z} + \mathbf{i}\mathbb{Z}$ of ***Gaussian integers***, the units group is $\{\pm 1, \pm \mathbf{i}\}$. [Aside: Units($\mathbb{G}$) is cyclic, generated by $\mathbf{i}$. And Units($\mathbb{Z}_{12}$) is not cyclic. For which N is $\Phi(N)$ cyclic?] □

Irreducibles, Primes. Consider $(\Gamma, +, 0, \cdot, 1)$, a commutative ring[♡4]. An elt $\alpha \in \Gamma$ is a ***zero-divisor*** [abbrev **ZD**] if there exists a *non-zero* $\beta \in \Gamma$ st. $\alpha\beta = 0$.

In contrast, an element $u \in \Gamma$ is a ***unit*** if $\exists w \in \Gamma$ st. $u{\cdot}w = 1$. This w, written as u^{-1}, is called the ***reciprocal*** [or ***multiplicative-inverse***] of u. [When an element *has* a mult-inverse, this mult-inverse is unique.]

Exer 1a: If α divides a unit, $\alpha \bullet\!\!| \, u$, then α is a unit.

Exer 1b: If $\gamma \not\bullet\!\!| \, z$ with $z \in$ ZD, then γ is a zero-divisor.

Exer 2: In an arbitrary ring Γ, the set ZD(Γ) is *disjoint* from Units(Γ).

An element $p \in \Gamma$ is:

i: Γ-***irreducible*** if p is a non-unit, non-ZD, such that for each Γ-factorization $p = x{\cdot}y$, either x or y is a Γ-unit. [Restating, using the definition below: Either $x{\approx}1, y{\approx}p$, or $x{\approx}p, y{\approx}1$.]

ii: Γ-***prime*** if p is a non-unit, non-ZD, such that for each pair $c,d \in \Gamma$: If $p \bullet\!\!| \, [c \cdot d]$ then *either* $p \bullet\!\!| \, c$ or $p \bullet\!\!| \, d$.

Associates. In a *commutative* ring, elts α and β are ***associates***, written $\alpha \approx \beta$, if *there exists* a unit u st. $\beta = u\alpha$. [For emphasis, we might say ***strong associates***.] They are ***weak-associates***, written $\alpha \sim \beta$, if $\alpha \bullet\!\!| \, \beta$ *and* $\alpha \not\bullet\!\!| \, \beta$ [i.e, $\alpha \in \beta\Gamma$ and $\beta \in \alpha\Gamma$].

Ex 3: Prove *Assoc* ⇒ *weak-Assoc*.

Ex 4: If $\alpha \sim \beta$ and $\alpha \notin$ ZD, then α, β are (strong) associates.

Ex 5: In $\mathbb{Z}_{10}$, zero-divisors $2, 4$ *are* weak-associates. [This, since $2{\cdot}2 \equiv 4$ and $4{\cdot}3 = 12 \equiv 2$.] Are $2, 4$ (strong) associates?

Ex 6: With $d \bullet\!\!| \, \alpha$, prove: *If α is a non-ZD, then d is a non-ZD.* And: *If α is a unit, then d is a unit.*

49: Lemma. *In a commRing*[♡4] Γ, *each prime* $\boldsymbol{\alpha}$ *is irreducible.* ♢

Proof. Consider factorization $\boldsymbol{\alpha} = xy$. Since $\boldsymbol{\alpha} \bullet\!\!| \, xy$, WLOG $\boldsymbol{\alpha} \bullet\!\!| \, x$, i.e $\exists c$ with $\boldsymbol{\alpha}c = x$. Hence

$$*: \qquad \boldsymbol{\alpha} \;=\; xy = \boldsymbol{\alpha}cy\,.$$

By defn, $\boldsymbol{\alpha} \notin$ ZD. We may thus cancel in $(*)$, yielding $1 = cy$. So y is a unit. ♦

[♡4] More generally, a commutative monoid.

There are rings[♡5] with irreducible elements p which are nonetheless not prime. However...

50: Lemma. *Suppose commRing* Γ *satisfies the Bézout condition, that each GCD is a linear-combination. Then each irreducible* $\boldsymbol{\alpha}$ *is prime.* ♢

Pf. Suppose $\boldsymbol{\alpha} \bullet\!\!| \, c{\cdot}d$. WLOG $\boldsymbol{\alpha} \not\bullet\!\!| \, c$. Let $g := \text{GCD}(\boldsymbol{\alpha}, c)$. Were $g \approx \boldsymbol{\alpha}$, then $\boldsymbol{\alpha} \bullet\!\!| \, g \bullet\!\!| \, c$, a contradiction. Thus, since $\boldsymbol{\alpha}$ is irreducible, our $g \approx 1$.

Bézout produces $S,T \in \Gamma$ with

$$1 \;=\; S\boldsymbol{\alpha} + Tc\,. \quad \textit{Hence}$$
$$*: \qquad d \;=\; S\boldsymbol{\alpha}d + Tcd \;=\; Sd\boldsymbol{\alpha} + Tcd\,.$$

By hyp, $\boldsymbol{\alpha} \bullet\!\!| \, cd$, hence $\boldsymbol{\alpha}$ divides RhS$(*)$. So $\boldsymbol{\alpha} \bullet\!\!| \, d$. ♦

51: Lemma. *In commRing* Γ, *if prime* p *divides product* $\alpha_1 \cdots \alpha_K$ *then* $p \bullet\!\!| \, \alpha_j$ *for some* j. [*Exer. 7*] ♢

52: Prime-uniqueness thm. *In commRing* Γ, *suppose*

$$p_1{\cdot}p_2{\cdot}p_3 \cdots p_K \;=\; q_1{\cdot}q_2{\cdot}q_3 \cdots q_L$$

are equal products-of-primes. Then $L = K$ *and, after permuting the* p *primes, each* $p_k \approx q_k$. ♢

Pf. [From Ex.4, previously, for non-ZD, relations $\sim$ and $\approx$ are the same.] For notational simplicity, we do this in $\mathbb{Z}_+$, in which case $p_k \approx q_k$ will be replaced by $p_k = q_k$.

FTSOC, consider a CEX which minimizes sum $K{+}L$; necessarily positive. WLOG $L{\geq}1$. Thus $K{\geq}1$. [Otherwise, q_L divides a unit, forcing q_L to be a unit; see Ex.1a.] By the preceding lemma, q_L divides *some* p_k; WLOG $q_L \bullet\!\!| \, p_K$. Thus $q_L = p_K$ [since p_K is prime and q_L is not a unit]. Cancelling now gives $p_1{\cdot}p_2 \cdots p_{K-1} = q_1{\cdot}q_2 \cdots q_{L-1}$, giving a CEX with a *smaller* $[K{-}1] + [L{-}1]$ sum. ♦

[♡5] Consider the ring, Γ, of polys with coefficients in $\mathbb{Z}_{12}$. There, $x^2 - 1$ factors as $[x-5][x+5]$ *and* as $[x-1][x+1]$. Thus none of the four linear terms is prime. Yet each is Γ-irreducible. (Why?) This ring Γ has zero-divisors (yuck!), but there are natural subrings of $\mathbb{C}$ where Irred$\not\Rightarrow$Prime.

Example where $\sim \neq \approx$. Here a modification of an example due to Irving ("Kap") Kaplansky.

Let Ω be the ring of real-valued *continuous* fncs on $[-2,2]$. Define $\mathcal{E},\mathcal{D} \in \Omega$ by: *For* $t \geq 0$:

$$\mathcal{E}(t) \;=\; \mathcal{D}(t) \;:=\; \begin{Bmatrix} t-1 & \text{if } t \in [1,2] \\ 0 & \text{if } t \in [0,1] \end{Bmatrix} .$$

And for $t \leq 0$ define

$$\mathcal{E}(t) \;:=\; \mathcal{E}(-t) \quad \textit{and} \quad \mathcal{D}(t) \;:=\; -\mathcal{D}(-t) .$$

[So $\mathcal{E}$ is an Even fnc; $\mathcal{D}$ is odD.] Note $\mathcal{E} = f\mathcal{D}$ and $\mathcal{D} = f\mathcal{E}$, where

$$f(t) \;:=\; \begin{Bmatrix} 1 & \text{if } t \in [\,1,\,2] \\ t & \text{if } t \in [\text{-}1,\,1] \\ \text{-}1 & \text{if } t \in [\text{-}2,\text{-}1] \end{Bmatrix} .$$

Hence $\mathcal{E} \sim \mathcal{D}$. [This f is not a unit, since $f(0) = 0$ has no reciprocal. However, f is a *non*-ZD: For if $fg = \mathbf{0}$, then g must be zero on $[-2,2] \smallsetminus \{0\}$. Cty of g then forces $g \equiv \mathbf{0}$.]

Could there be a unit $u \in \Omega$ with $u\mathcal{D} = \mathcal{E}$? Well

$$u(2) = \tfrac{\mathcal{E}(2)}{\mathcal{D}(2)} \overset{\text{note}}{=\!=} +1 , \quad \textit{and} \quad u(-2) = \tfrac{\mathcal{E}(-2)}{\mathcal{D}(-2)} \overset{\text{note}}{=\!=} -1 .$$

Cty of $u()$ forces u to be zero somewhere on interval $(-2,2)$, hence u is *not* a unit. □

Addendum. By Ex.4, both $\mathcal{E}$ and $\mathcal{D}$ must be zero-divisors. [Exer.8: Exhibit a function $g \in \Omega$, *not* the zero-fnc, such that $\mathcal{E} \cdot g \equiv \mathbf{0}$.] □

Inverses

Consider a not-nec-commutative monoid $(S, \bullet, \mathbf{e})$ and an $x \in S$. An elt $\lambda \in S$ is a "***left inverse*** of x" if $\lambda \bullet x = \mathbf{e}$. Of course, then x is a ***right inverse*** of λ. Use ***LInv***/***RInv*** for "left/right inverse".

We will often suppress the binop-symbol and write xy for $x \bullet y$.

53: Prop'n. *In a monoid* $(S, \bullet, \mathbf{e})$*:*

i: *For each* $x \in S$*: If* x *has at least one LInv and one RInv, then* x *has a unique LInv and RInv, and they are equal.*

ii: *Suppose every elt of* S *has a right-inverse. Then* S *is a group.* ◊

Proof of (i). Suppose λ is a LInv of x, and ρ a RInv. Then

$$\lambda \;=\; \lambda[x\rho] \;=\; [\lambda x]\rho \;=\; \rho .$$

And if two LInvs, then $\lambda_1 = \rho = \lambda_2$. ♦

Proof of (ii). Given $x \in S$, pick a *RInv* r and a *RInv* to r, call it y. Now

$$x \;=\; x \bullet [ry] \;=\; [xr] \bullet y \;=\; y .$$

Hence x is both a left and right inverse to r. So r is a right/left inverse to x. [Now apply part (i).] ♦

In the next lemma, we **neither** assume *existence* of left-identity/left-inverses, **nor** do we assume *uniqueness* of right-identity/right-inverses.

54: Lemma. *Suppose* $\ltimes$ *is an associative binop on* S*, and* $\mathbf{e} \in S$ *is a righthand-identity elt. Suppose that each* $y \in S$ *has a* [*wrt* $\mathbf{e}$] *righthand inverse,* y'*. Then:*

54a: *If* $y \ltimes y = y$*, then* $y = \mathbf{e}$.

Moreover:

54b: *Each* y' *is also a left inverse to* y*, and* $\mathbf{e}$ *is also a lefthand-identity.*

Thus $(S, \ltimes, \mathbf{e})$ *is a group,* ◊

Pf (54a). Note $y = y \ltimes \mathbf{e} = y \ltimes [y \ltimes y'] = [y \ltimes y] \ltimes y'$. By hypothesis $y \ltimes y = y$, so the above asserts that $y = y \ltimes y' \overset{\text{note}}{=\!=} \mathbf{e}$. ♦

Pf of (54b). First let's show that every RInv, y', of y, is also a LInv of y. Let $b := [y' \ltimes y]$. Courtesy (54a), it is enough to show that $b \ltimes b = b$. And

$$\begin{aligned} b \ltimes b &= [y' \ltimes [y \ltimes y']] \ltimes y \,, \quad \text{by assoc.,} \\ &= [y' \ltimes \mathbf{e}] \qquad \ltimes y \\ &= y' \ltimes y \overset{\text{note}}{=\!=} b \,. \end{aligned}$$

We can now show that $\mathbf{e}$ is also a *left*hand identity. After all, $\mathbf{e} \ltimes y = [y \ltimes y'] \ltimes y = y \ltimes [y' \ltimes y] = y \ltimes \mathbf{e}$, since y' is a LHInverse. I.e, $\mathbf{e} \ltimes y = y$. ♦

Notes to me. Bertrand Postulate.
Burnside's Normal p-complement Theorem.

§B Appendix: Miscellaneous results

Here are uncategorized theorems & and examples. My Algebra notes are spread out over many files; I need to organize them.

55: Min-prime normality lemma. *Consider finite groups $G \supset H$ with index $p := |G : H|$ prime. Moreover, p is the smallest prime dividing $|G|$. Then $H \lhd G$.* ♢

Proof. Group G acts on the H-left-cosets by mult-on-the-left, engendering a group-hom $\psi: G \to \mathbb{S}_p$ into the symmetric group. Evidently, $g \notin H$ forces $gH \neq H$. Hence $K := \text{Ker}(\psi) \subset H$. [Were $|G : K|$ prime, then H is either K or G, each of which is normal in G.] ISTShow $n := |G : K| \stackrel{?}{=} p$.

Lagrange's thm says: n *divides* $|G|$. Hence, the *smallest* prime that could divide n is p.

Quotient group $\frac{G}{K}$ is isomorphic (via ψ) to $\mathbb{S}_p$-subgp $\text{Range}(\psi)$. Hence: n *divides* $p! \stackrel{\text{note}}{=\!=} |\mathbb{S}_p|$. So the *largest* prime that could divide n is p. Moreover, p^2 does not divide $p!$, hence $\boxed{n = p}$. ♦

§Index for Group Notes