Basic Algebra definitions

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
3 October, 2018 (at *08:54*)

Semigroups. For us, a ***semigroup*** is a triple $(S, \bullet, \mathbf{e})$, where $\bullet$ is an associative binary operation on set S, and $\mathbf{e} \in S$ is a two-sided identity elt.[♡1]

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 '+', then we write the inverse of α as $-\alpha$ and call it "***negative*** α".

If we refer to the binop as 'multiplication' then write the inverse of α as α^{-1} and call it "the ***reciprocal*** of α". Also, we usually omit the binop-symbol and write $\alpha\beta$ for $\alpha{\cdot}\beta$.

For an abstract binop '$\bullet$', we usually write α^{-1} for the inverse of α, and we call it "α inverse". If $\bullet$ is ***commutative*** [$\forall\alpha,\beta$, necessarily $\alpha \bullet \beta = \beta \bullet \alpha$] then we call S a ***commutative (semi)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 semigroup.

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 $\alpha,x,y \in \Gamma$.

[♡1] What I'm calling a semigroup is usually called a ***monoid***. The std defn of ***semigroup*** does not require an identity-elt.

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

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

An $\alpha \in \Gamma$ is a Γ-***unit*** if $\exists\beta \neq 0$ st. $\alpha\beta = 1 = \beta\alpha$. Use

$$\mathrm{Units}_\Gamma \quad \text{or} \quad \mathrm{Units}(\Gamma)$$

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

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

An intDomain F in which every non-zero element is a unit, $\mathrm{Units}(F) = F \smallsetminus \{0\}$, is a ***field***. I.e, F is a commRing such that triple $\big(F \smallsetminus \{0\}, \cdot, 1\big)$ is a group.

Examples. 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 $\mathbb{G} := \mathbb{Z} + \boldsymbol{i}\mathbb{Z}$ of ***Gaussian integers***, the units group is $\{\pm 1, \pm \boldsymbol{i}\}$. [Aside: $\mathrm{Units}(\mathbb{G})$ is cyclic, generated by $\boldsymbol{i}$. And $\mathrm{Units}(\mathbb{Z}_{12})$ is not cyclic. For which N is $\Phi(N)$ cyclic?] □

Irreducibles, Primes. Consider a commutative ring $(\Gamma, +, 0, \cdot, 1)$. 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 is the "multiplicative inverse" of u, is unique, and is often written u^{-1}.) Exer 1: In an arbitrary ring Γ, the set $\mathrm{ZD}(\Gamma)$ is *disjoint* from $\mathrm{Units}(\Gamma)$.

An element α is:

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

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

Associates. In a *commutative* ring, elts α and β are ***associates***, written $\alpha \sim \beta$, if $\alpha \bullet\!| \; \beta$ *and* $\alpha \;|\!\bullet \beta$ [i.e, $\alpha \in \beta\Gamma$ and $\beta \in \alpha\Gamma$]. They are ***strong associates***, written $\alpha \approx \beta$, if there exists a unit u st. $\beta = u\alpha$.

Ex 2: Prove *Strong-Assoc* $\Rightarrow$ *Assoc.*

Ex 3: If $\alpha \sim \beta$ <u>and</u> $\alpha \notin \mathrm{ZD}$, then α, β are **strong** associates.

Ex 4: In $\mathbb{Z}_{10}$, zero-divisors $2, 4$ *are* associates. Are they strong associates?

Ex 5: 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.*

1: Lemma. *In a commRing Γ, each prime α is irreducible.* ♢

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

$$*: \qquad \alpha \;=\; xy = \alpha c y\,.$$

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

There are rings[♡2] with irreducible elements p which are nonetheless <u>not</u> prime. However...

[♡2]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.

2: Lemma. *Suppose commRing Γ satifies the Bézout condition, that each GCD is a linear-combination. Then each irreducible α is prime.* ♢

Proof. Suppose $\alpha \bullet\!| \; xy$ and WLOG $\alpha \nmid x$. Let $g := \mathrm{GCD}(\alpha, x)$. Were $g \approx \alpha$, then $\alpha \bullet\!| \; g \bullet\!| \; x$, a contradiction. Thus, since α is irreducible, our $g \approx 1$.

Bézout produces $S,T \in \Gamma$ with

$$\begin{aligned} 1 &= S\alpha + Tx\,. \quad \textit{Hence} \\ *: \qquad y &= S\alpha y + Txy \;=\; Sy\alpha + Txy\,. \end{aligned}$$

By hyp, $\alpha \bullet\!| \; xy$, hence α divides $\mathrm{RhS}(*)$. So $\alpha \bullet\!| \; y$. ♦

Example where $\sim \neq \approx$. Here a modification of an example due to Kaplansky.

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

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

And for $t \leqslant 0$ 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

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

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 $g = \mathbf{0}$.]

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

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

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

Back to Semigroups

Consider a not-nec-commutative semigroup $(S, \bullet, \mathbf{e})$ 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 $x \bullet y$.

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

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 r is both a left and right inverse to x. Etc. ♦

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

4: 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 righthand inverse, y'. Then:*

4a: *If $y \ltimes y = y$, then $y = \mathbf{e}$.*

Moreover:

4b: *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 (4a). 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 (4b). First let's show that every RInv, y', of y, is also a LInv of y. Let $b := [y' \ltimes y]$. Courtesy (4a), 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, $\mathbf{e} \ltimes y = y$. ♦

Henceforth, groups[♡3] are the subject.

Cyclic groups

I use Cyc_N for the order-N *cyclic group*. By default, it is written multiplicatively, but I may write $(\mathrm{Cyc}_N, \cdot)$ or $(\mathrm{Cyc}_N, +)$ to indicate specifically. The infinite group Cyc_∞ is iso to $(\mathbb{Z}, +)$.

For $y \in G$ we use $\mathrm{Periods}_G(y)$ for the set of integers k with $y^k = \mathbf{e}$. A *subgroup* $H \subset G$ determines a similar set. Let $P_H(y) = P_{H,G}(y)$ be $\{k \in \mathbb{Z} \mid y^k \in H\}$. So $\mathrm{Periods}(y)$ is simply $P_H(y)$, when H is the trivial subgp $\{\mathbf{e}\}$.

5: Periods Lemma. *Fix G, H, y as above, and let P_H mean $P_H(y)$. 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,

$$\text{H-Ord}_G(y) \bullet\!| \ \text{K-Ord}_G(y) \bullet\!| \ \mathrm{Ord}_G(y) . \qquad ♢$$

[♡3] Here is my generic footnote: Typical group notation: $(G, \cdot, \mathbf{e})$ or $(\Gamma, \cdot, \boldsymbol{\varepsilon})$ or $(G, \cdot, 1)$ or $(G, +, 0)$. 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 $(\mathbf{V}, +, \mathbf{0})$. A group of *functions*, under composition, might be written $(G, \circ, \mathit{Id})$.

We'll use $\mathbb{1}$ (a blackboard bold '1') for the *trivial group*, but in specific cases may write $\{\mathbf{e}\}$ or $\{0\}$.

Use Cyc_N, $\mathbb{S}_N$, $\mathbb{D}_N$ for the N^{th} *cyclic*, *symmetric* and *dihedral* groups. So $|\mathrm{Cyc}_N| = N$ and $|\mathbb{S}_N| = N!$ and $|\mathbb{D}_N| = 2N$. The *alternating group* $\mathbb{A}_N$ has $|\mathbb{A}_1| = 1$; otherwise, $|\mathbb{A}_N|$ is $N!/2$. Use $\mathrm{Z}(G)$ for the *center* of G. The automorphisms of G form a group $(\mathrm{Aut}(G), \circ, \mathit{Id})$.

Each $x \in G$ yields an ***inner automorphism*** of G defined by $J_x(g) := xgx^{-1}$. The set $\{J_x\}_{x \in G}$ is written $\mathrm{Inn}(G)$; it is a normal subgp of $\mathrm{Aut}(G)$. The map $\mathcal{J}: G \to \mathrm{Aut}(G)$ by $\mathcal{J}(x) := J_x$, is a group homorphism.

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

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

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

Suppose $H \lhd G$. Now $[yH]^k = y^k H$, so $[yH]^k{=}H$ IFF $y \in H$. In terms of the quotient group,

5′: $\forall y \in G$: $\mathrm{Ord}_{G/H}(yH) = \text{H-Ord}_G(y) \bullet \mathrm{Ord}_G(y)$.

Dihedral groups

The ***Klein-4*** group is isomorphic to $\mathrm{Cyc}_2 \times \mathrm{Cyc}_2$. Often called the ***Vierergruppe***, it has presentation

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

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

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

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

8: $$\mathbb{D}_N := \langle \mathtt{r}, \mathtt{f} \mid \mathtt{f}^2 = \mathbf{e},\ \mathtt{frfr} = \mathbf{e},\ \mathtt{r}^N = \mathbf{e} \rangle;$$
$$\mathbb{D}_\infty := \langle \mathtt{r}, \mathtt{f} \mid \mathtt{f}^2 = \mathbf{e},\ \mathtt{frfr} = \mathbf{e} \rangle, \text{ for } N = \infty.$$

Now for some straightforward facts.

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

$$\mathtt{r}^j \cdot \mathtt{f} = \mathtt{f} \cdot \mathtt{r}^{-j}.$$

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

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

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

Both $\mathrm{Z}(\mathbb{D}_\infty)$ and $\mathrm{Z}(\mathbb{D}_{N\ odd})$ are trivial. Consequently $\mathrm{Inn}(\mathbb{D}_\infty) \cong \mathbb{D}_\infty$ and $\mathrm{Inn}(\mathbb{D}_{N\ odd}) \cong \mathbb{D}_N$.

When $N = 2K$ is even: The center $\mathrm{Z}(\mathbb{D}_{2K}) = \{\mathbf{e}, \mathtt{r}^K\}$. Consequently $\mathbb{D}_K \cong \mathrm{Inn}(\mathbb{D}_{2K})$ via the map

$$\mathtt{r}^j \mapsto J_{\mathtt{r}^k} \quad \text{and} \quad \mathtt{fr}^j \mapsto J_{\mathtt{fr}^k}, \quad \textit{Improve this!}$$

where $k := [j \mod K]$. ♢

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 $2j \bullet N$. So the only possible nt-element in the center is $\mathtt{r}^K$, where $N = 2K < \infty$. And $\mathtt{r}^K$ commutes with each $\mathtt{fr}^j$. ♦

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 (19), 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.

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

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

†: $$n \xmapsto{x} n{-}5 \xmapsto{h} n{-}5 \xmapsto{x^{-1}} n,$$

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. □

12: *E.g.* Kevin Keating tells me that the following is a standard example.

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. □

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

I.e, let $\mathtt{r}, \mathtt{f}$ be the rotation and flip in $G := \mathbb{D}_3$. Subgroups $\mathrm{N} := \{\mathbf{e}, \mathtt{f}\}$ and $\Gamma := \{\mathbf{e}, \mathtt{fr}\}$ make $\mathrm{N}\Gamma$ equal $\{\mathbf{e}, \mathtt{f}, \mathtt{fr}, \mathtt{r}\}$. This is not a group, since it does not own $\mathtt{r}^2$. □

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

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

Why is $\mathrm{N}\Gamma$ sealed under multiplication? Well, $y\beta \cdot x\alpha$ equals $yx'\beta\alpha \in \mathrm{N}\Gamma$. Finally, the inverse $x\alpha = \alpha^{-1}x^{-1} \in \Gamma\mathrm{N} = \mathrm{N}\Gamma$. ♦

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

15: $$f : \mathrm{N}\times\Gamma \to \mathrm{N}\Gamma, \quad \text{by } (x, \omega) \mapsto x\omega,$$

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

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

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

Recalling the bijection. $f : \mathrm{N}\times\Gamma \to G$ from (15), the following are equivalent:

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

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

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

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

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

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

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

$$x \cdot \alpha x^{-1}\alpha^{-1} \in \mathrm{NN} \subset \mathrm{N} .$$

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

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

17: $\mathrm{Inn}(G) \subset \mathrm{Aut}(G) \subset \mathrm{SurEnd}(G) \subset \mathrm{End}(G)$.

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 $\psi : G \circlearrowleft$ send H into itself.

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

	Which Homs?	Then written as
	... $\psi \in \mathrm{Inn}(G)$	$H \triangleleft G$
18:	... $\psi \in \mathrm{Aut}(G)$	$H \overset{a}{\triangleleft} G$
	... $\psi \in \mathrm{SurEnd}(G)$	$H \overset{se}{\triangleleft} G$
	... $\psi \in \mathrm{End}(G)$	$H \overset{e}{\triangleleft} G$

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

In the examples below, $H, K \subset (G, \cdot, \mathbf{e})$ 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. □

20: *E.g.* Each $x \in G$ engenders a ***conjugation map*** $J_x : G \circlearrowleft$ 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

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

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

22: $$\mathrm{Inn}(G) \cong \frac{G}{\mathrm{Z}(G)} .$$

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

21′: $$\mathcal{J}_H : \mathcal{N}_G(H) \to \mathrm{Aut}(H) : x \mapsto J_x\!\downharpoonright_H .$$

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

$$A := \mathrm{Range}(\mathcal{J}_H) \subset \mathrm{Aut}(H) .$$ □

23: Lemma. *Suppose* $|G \colon H| = 2$. *Then* $H \triangleleft G$. ◊

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

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

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

Remark. Index $|G \colon H| = 2$ need *not* imply the stronger $H \overset{a}{\triangleleft} G$. In the Vierergruppe, (7′), the $\langle a \rangle_V$ subgroup has index 2 in V. Yet the automorphism that exhanges a and b moves $\langle a \rangle$.

Also, $|G \colon H| = 3$ is not sufficient to imply normality. In $\mathbb{D}_3$, the non-normal subgp $\langle \mathtt{f} \rangle$ has index 3. □

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

25: $$[H \overset{a}{\triangleleft} G \overset{a}{\triangleleft} F] \implies H \overset{a}{\triangleleft} F\,.$$

26: $$[H \overset{a}{\triangleleft} G \triangleleft F] \implies H \triangleleft F\,.$$

And $[H \overset{e}{\triangleleft} G \overset{e}{\triangleleft} F] \Rightarrow H \overset{e}{\triangleleft} F$. *Proof.* Use (19). ◊

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

27: Normal Grabbag.

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

ii: *The center* $Z(G) \overset{se}{\triangleleft} G$, *but not necessarily* $\overset{e}{\triangleleft}$.

iii: $\operatorname{Inn}(G) \triangleleft \operatorname{Aut}(G)$, *but not necessarily* $\overset{a}{\triangleleft}$. ◊

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 $z \in Z(G)$. To show $\widehat{z} \in Z(G)$, 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 $Z(G)$ *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

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

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

$$\mathcal{A}\big((\omega, \mathbf{e})\big) \;:=\; (\boldsymbol{\varepsilon}, \mathtt{f}) \quad \text{and}$$
$$\mathcal{A}\big((\boldsymbol{\varepsilon}, \mathtt{f})\big) \;:=\; (\omega, \mathbf{e})\,.$$

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

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

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). [Keating emailed me this. This in fact may have been my original example.] Note that $\mathbb{D}_4$ has exactly two subgroups isomorphic to the Vierergruppe,

$$V \;:=\; \langle \mathtt{r}^2, \mathtt{f} \rangle \;=\; \{\mathbf{e}, \mathtt{r}^2, \mathtt{f}, \mathtt{fr}^2\} \quad \text{and}$$
$$V' \;:=\; \langle \mathtt{r}^2, \mathtt{fr} \rangle \;=\; \{\mathbf{e}, \mathtt{r}^2, \mathtt{fr}, \mathtt{fr}^3\}\,.$$

And $\alpha(V) = V'$, where $\alpha \in \operatorname{Aut}(\mathbb{D}_4)$ 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 $A := \operatorname{Aut}(\mathbb{D}_4) \cong \mathbb{D}_4$. Its subgp $S := \operatorname{Inn}(\mathbb{D}_4) \cong \mathbb{D}_2$ is isomorphic to a Vierergruppe. One can interpret the above α as in $\operatorname{Aut}(A)$, 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

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

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

Proof. Let G be

$$\mathbb{D}_2 \times \mathbb{D}_4 \times \mathbb{D}_8 \times \mathbb{D}_{16} \times \ldots\,.$$

By (10)...

Unfinished: as of 3Oct2018 $\blacklozenge$

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

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

I.e, $DA \cdot f(1) \,|\!\bullet\, DB$. Hence we need $A \cdot f(1) \,|\!\bullet\, B$. Since $A \perp B$, this latter is equiv to $f(1) \,|\!\bullet\, B$. 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 $f_M(y) := [M \cdot y]_{\text{ mod } L}$.

When $L = K$. Let E be the set of endomorphisms of $(\mathbb{Z}_K, +)$. So $(E, \circ)$ is a semigroup; indeed, a commutative semigp. 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

For a (possibly infinite) group G and posint D, define

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

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

29: Phi Lemma. *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 $\boxed{\varphi(D) \text{ divides } |S_{D,G}|}$.*

Moreover, the ratio $|S_{D,G}| / \varphi(D)$ equals the number of cyclic order-D subgroups of G. $\lozenge$

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

An elt $x \in G$ 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. $\blacklozenge$

Divisibility ideas. All these come from splitting G into equal-sized subsets.

30: Lemma. *Suppose $\psi: G \twoheadrightarrow Q$ is a surjective group-homomorphism. Then $\mathrm{Ord}(Q) \bullet\!|\, \mathrm{Ord}(G)$. Indeed, $|Q| \cdot |K| = |G|$, where $K := \mathrm{Ker}(\psi)$.* $\lozenge$

Proof. The ψ-inverse-image of each $q \in Q$ is a left-coset of K in G. (Using right-cosets also works, since $K \lhd G$.) $\blacklozenge$

31: Lagrange's Theorem. *Given groups $H \subset G$, then, $\mathrm{Ord}(H) \bullet\!|\, \mathrm{Ord}(G)$.* $\lozenge$

Proof. The left-cosets of H form a partition of G. $\blacklozenge$

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

No. The N^{th} dihedral group $\mathbb{D}_N$ is generated by a *flip* $\mathtt{f}$ and an order-N *rotation* $\mathtt{r}$.

Although $\mathrm{Ord}(\mathbb{D}_{15}) = 30$ and $6 \bullet\!\!\mid 30$, nonetheless $\mathbb{D}_{15}$ has <u>no</u> elt of order 6: Its 15 "flip elts", $\mathtt{fr}^i$, 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 $\langle \mathtt{r} \rangle$ of each of these orders is

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

And $8 + 4 + 2 + 1 = 15$.[♡4]

Although $\mathbb{D}_{15}$ has no *element* of order-6, it <u>does</u> have a sub*group* of order 6. The subgp $\langle \mathtt{f}, \mathtt{r}^5 \rangle$ is isomorphic to $\mathbb{D}_3$. ♦

32: Really really No. *Although $\mathrm{Ord}(\mathbb{A}_4) = 12$ and $6 \bullet\!\!\mid 12$, nonetheless $\mathbb{A}_4$ has <u>no</u> 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 G. Necessarily there is a $\beta \in H$ with cyc-struct $\lceil 3,1 \rfloor$. If H owned a $\lceil 2,2 \rfloor$ α, then $\alpha' := \beta\alpha\beta^{-1}$ would have to be a *different* $\lceil 2,2 \rfloor$ (they couldn't commute). But then H includes the Klein-4 group $\langle \alpha, \alpha' \rangle$. Yet $4 \not\mid\!\bullet\, 6$.

The upshot is that no elt of $H \setminus \{\mathbf{e}\}$ is $\lceil 2,2 \rfloor$, so each is a $\lceil 3,1 \rfloor$. And there are 5 of them. Courtesy (29), then, $5 \mid\!\!\bullet\, \varphi(3)$. But $5 \not\mid\!\bullet\, 2$. ♦

33: Cauchy's Thm for finite abelian groups. *Suppose $N := |G| < \infty$ where G is an abelian group, written multiplicatively. If prime $p \bullet\!\!\mid N$, 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

$$p \bullet\!\!\mid \widetilde{K} := \prod_{j=1}^{N} K_j \,,$$

since then, WLOG, $p \bullet\!\!\mid K_2$; so ${g_2}^{[K_2/p]}$ has order p.

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

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

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

A more standard proof uses induction on quotient groups.

Pf of (33). WELOG $p := 5$. We may assume that

34: *If Q is a finite abelian group with $\mathrm{Ord}(Q) \mid\!\!\bullet\, 5$, 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 $\mathrm{Ord}_G(y) \mid\!\!\bullet\, 5$.

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

Thus (34) applies to produce an element $y \in G$ with $\mathrm{Ord}_Q(yH) = 5$. And by (5,5′), the Periods Lemma, $\mathrm{Ord}_G(y) \mid\!\!\bullet\, \mathrm{Ord}_Q(yH)$. ♦

Group actions. The symbol $G \circlearrowleft \Omega$ <u>means that gp G</u> ***acts on*** set Ω; there is a gp-hom $\boxed{\psi\colon G \to \mathbb{S}_\Omega}$. For $g \in G$ and $\omega \in \Omega$, write the gp-action as $\psi_g(\omega)$ or $g(\omega)$ or just $g\omega$. Define the ***orbit*** and ***stabilizer*** of a point ω, and the ***fixed-pt set*** of a group-element g:

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

This $\mathrm{Stab}(\omega)$ is a subgp, but is rarely normal in G:

35: $\forall f \in G\colon \quad f \cdot \mathrm{Stab}(\omega) \cdot f^{-1} = \mathrm{Stab}(f\omega)\,.$

36: Orbit-Stabilizer Lemma. *For each $\omega \in \Omega$:*

$*$: $\quad \mathrm{Ord}(\mathrm{Stab}_\psi(\omega)) \cdot |\mathcal{O}_\psi(\omega)| = \mathrm{Ord}(G)\,.$ ♢

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

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

37: Burnside's Lemma. *Counting cardinalities,*

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

Counting the number of G-orbits, then,

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

Proof. The number of G-orbits equals

$$\sum_{\omega\in\Omega}\frac{1}{|\mathcal{O}(\omega)|} \;\overset{\text{Orb-Stab, (36*)}}{=\!=\!=}\; \frac{1}{|G|}\cdot\sum_{\omega\in\Omega}|\mathrm{Stab}(\omega)|\,.$$

Now apply (37†) to earn (37‡). ♦

Application: Coloring a cube's faces. Color the six faces of a cube red, white and blue. How many distinct colorings are there, up to orientation-preserving rotation? 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

$$38: \quad K^2\cdot[K^4 + 3K^2 + 12K + 8]\Big/24\,. \quad (\mathit{Faces})$$

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

What isometry g?	${}^{\#}$\{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

$$39: \quad K^2\cdot[K^6 + 17K^2 + 6]\Big/24\,. \quad (\mathit{Vertices})$$

Class equation

Consider a finite group acting on a finite set, $G \circlearrowleft \Omega$, 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. Firstly, the Orbit-Stabilizer thm restates the circled as

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

where "$\mathit{All}\mathcal{O}\mathit{Reps}$" stands for "all orbit representatives"; this is one token ω per G-orbit. Now let

$$\mathrm{Fix}(G) \;:=\; \bigcap\nolimits_{g\in G}\mathrm{Fix}(g)\,.$$

This is the set of ω in 1-point orbits, i.e, $\mathcal{O}(\omega) = \{\omega\}$. Let's pull out these ***trivial orbits*** and define

$$\mathcal{O}\mathit{Reps} \;:=\; \mathit{All}\mathcal{O}\mathit{Reps} \smallsetminus \mathrm{Fix}(G)\,;$$

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

$$40: \quad |\Omega| \;=\; |\mathrm{Fix}(G)| + \sum_{\omega\in\mathcal{O}\mathit{Reps}}\frac{|G|}{|\mathrm{Stab}_G(\omega)|}\,.$$

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

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

$$\mathbb{C}(\omega) := \{g\omega g^{-1} \mid g \in G\}.$$

A conjugacy class is "non-trivial" if it has more than one point. So $\mathbb{C}(h)$ is trivial IFF $\mathcal{C}(h) = G$ IFF $h \in \mathrm{Z}(G)$, where $\mathrm{Z}(G) := \bigcap_{h\in G} \mathcal{C}(h)$ is the ***center*** of G. Below, let "$h \in PECC$" mean to take one representative h "Per Each Conjugacy Class". Let ***PCC*** mean "Per *non-trivial* Conjugacy Class".

41: Class-Equation Thm. *For a finite group G,*

$$41': \qquad |G| = |\mathrm{Z}(G)| + \sum_{h\in PCC} \frac{|G|}{|\mathcal{C}(h)|}.$$

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

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

$$|G| = \sum_{h\in PECC} \frac{|G|}{|\mathcal{C}(h)|}.$$ □

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

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

42: Center-pop Thm (P.403). *Suppose $|G| = p^L$, where p is prime and $L \in \mathbb{Z}_+$. Then $\mathrm{Z}(G)$ is non-trivial. (So $|\mathrm{Z}(G)| = p^K$ for some $K \in [1..L]$.)* ◊

Proof. The centralizer of each $h \in PCC(G)$ is a *proper* subgroup, so p divides $|G|/|\mathcal{C}(h)|$. Hence p divides the sum on RhS(41′). So p divides $|\mathrm{Z}(G)|$. ♦

43: Cauchy's Thm for finite groups (P.406). *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

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

holds for each group Q with $|Q| < |G|$. So WLOG we may assume that each centralizer $\mathcal{C}(h)$, for h in $PCC(G)$, has order not a multiple of p. Thus p divides the RhS(41′) sum. So $p \bullet\!| \; \mathrm{Ord}(\mathrm{Z}(G))$.

We may now apply (33), Cauchy's thm for *abelian* groups, to $\mathrm{Z}(G)$, to get a order-p element. ♦

Remark. We get a nice progression of proofs. Note that (34) uses induction on quotient groups, but does not use the Class-Eqn, whereas Center-pop Thm (42) uses the class equation but no induction. The above Cauchy's thm (43), used quotient-induction to put the class equation in play.

An jazzed-up (43) argument will give Sylow's first theorem. □

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

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

We now show that this holds universally. □

44: Sylow's First Thm. *For each prime p, for each natural number k and finite group G, proposition $\mathrm{P}(k,G)$ holds.* ◊

Pf. Always $\mathrm{P}(0,*)$ holds, so fixing a $K \geqslant 1$ and finite group G, we show that $\mathrm{P}(K,G)$. We may assume that $\mathrm{Ord}(G) \,|\!\bullet\, p^K$ and

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

So WLOG $p^K \nmid \mathcal{C}_G(h)$, for each h in $PCC(G)$. Thus p divides the $\sum$-sum in (41′). So $p \bullet\!| \; \mathrm{Ord}(\mathrm{Z}(G))$.

Cauchy's thm for abelian groups now gives us a subgroup $H \subset \mathrm{Z}(G)$ 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 (45), 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.

46: Lemma. *We have a subgroup $H \subset Z(G)$. 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 $x_1 x_2$ equals

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

And this equals $x_2 x_1$. ♦

An immediate corollary is this "G mod Z" lemma.

47: G/Z Lemma. *We have a subgroup $H \subset Z(G)$; 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, $[zH]^n = z^n H$. So we let z^n be our representative of coset $[zH]^n$. ♦

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

$$\operatorname{Ord}(ac) = p \cdot q .$$ ♢

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

Since $a \leftrightarrows c$,

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

Were $\operatorname{Ord}(y) \bullet\!| p$, then $\mathbf{e} = [ac]^p = c^p$, so $p \bullet\!| \operatorname{Ord}(c)$. I.e $p \bullet\!| q$. Contradiction.

So $\operatorname{Ord}(y) \nmid p$. Ditto $\operatorname{Ord}(y) \nmid q$. But $\operatorname{Ord}(y) \bullet\!| pq$. Thus $\operatorname{Ord}(y) = pq$, ♦

49: Prop'n. *Suppose $K, L \subset G$ are groups. Then*

†: $$|KL| = |K| \cdot |L| \Big/ |K \cap L|$$

gives the cardinality of the product-set KL, which may or may not be a group. ♢

Proof. Let $N := |K \cap L|$. Certainly the map

‡: $$K \times L \to KL : (k, \ell) \mapsto k\ell$$

is onto. We show that an elt $\kappa\lambda \in KL$ has precisely N many preimages under (‡). Each $c \in K \cap L$ yields $\kappa c \in K$ and $c^{-1}\lambda \in L$, with $\kappa c \cdot c^{-1}\lambda$ equaling $\kappa\lambda$. Conversely, a product $k\ell = \kappa\lambda$ yields a common element

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

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

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.

50: Theorem. *Suppose $p < q$ are prime numbers st.*

†: $$p-1 \nmid q-1 \quad \text{and} \quad p \nmid q-1 .$$

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, we'll show that

51: *G has a unique order-q subgp; call it K. Moreover, its centralizer $\mathcal{C}_G(K)$ is all of G.*

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

Proof of (51). 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. Since p is prime, the order-p elts come in equivalence classes, $\{x, x^2, \ldots, x^{p-1}\}$, of size $p-1$. Hence $p-1$ must divide $\mathrm{Ord}(G) - 1$. But

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

so this would imply $p-1 \bullet| \; q-1$. But this ⋇s (50†).

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

This order-q subgp is unique. Were there another, call it H, then

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

since q is prime. From (49†), then,

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

But inequality $|G| \geqslant |HK|$ implies $p \geqslant q$; 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 $\mathcal{C} := \mathcal{C}_G(K)$ denote the centralizer. Since K is cyclic, it is abelian. So $K \subset \mathcal{C} \subset G$. By Lagrange's thm, then,

$$q \;\leqslant\; |\mathcal{C}| \;\leqslant\; pq\,.$$

Since p is prime, ISTShow that $|\mathcal{C}| \neq q$.

Were $|\mathcal{C}| = q$, then the quotient gp

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

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

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

But K is finite-cyclic, so $\mathrm{Aut}(K)$ is gp-isomorphic to $(\Phi(q), \cdot)$. Thus p divides $\varphi(q) \stackrel{\text{note}}{=\!=} q-1$. But this annoys (50†). ♦

What are some examples of this thm?

Works: $p < q$	Fails: $p < q$	Why fails
$5 < 7$	$3 < q$	$2 \bullet| \; q-1$
$5 < 19$	$5 < 11$	$5 \bullet| \; 10$
$5 < 23$	$5 < 13$	$4 \bullet| \; 12$
$7 < 11$	$7 < 13$	$6 \bullet| \; 12$
$7 < 17$	$7 < 19$	$6 \bullet| \; 18$

Sylow Thms

First a preliminary.

52: Lemma. *Finite groups $Y \lhd G$ and prime p have*

∗: $$p \nmid |G{:}Y| \;\stackrel{\text{note}}{=\!=}\; \frac{\#G}{\#Y}\,.$$

Suppose an $x \in G$ has $\mathrm{Ord}(x) = p^L$, for some natnum L. Then $x \in Y$. ♢

Proof. Let $Q := \frac{G}{Y}$. The homomorphism $G \twoheadrightarrow Q$ is *surjective*, so $q := \mathrm{Ord}_Q(xY) \bullet| \; \mathrm{Ord}(x) = p^L$. Thus q is a power-of-p. But q must divide $\mathrm{Ord}(Q)k$, by Lagrange, hence is coprime to p. The only such power-of-p is $q = p^0 = 1$. So $xY = Y$, i.e, $x \in Y$. ♦

Remark. Dropping the normality $Y \lhd G$ can cause the result to fail. With $G := \mathbb{S}_3$, let Y be the order-2 subgp generated by a 2-cycle, and let x be a *different* 2-cycle. □

53: Coro. *Suppose $Y \in \mathrm{Syl}_p(G)$, and $H \subset G$ is a p-group. If $H \subset \mathcal{N}_G(Y)$, then $H \subset Y$.* ♢

Proof. Let $N := \mathcal{N}_G(Y)$. Since Y is Sylow-p, index $|G \therefore Y|$ is coprime to p. But $|G \therefore Y| = |G \therefore N| \cdot |N \therefore Y|$, so $p \nmid |N \therefore Y|$. We may thus apply (52) to groups $Y \lhd N$, to conclude:

> $\forall x \in N$: *If* $\mathrm{Ord}(x)$ *is a power-of-p, then* $x \in Y$.

By hyp., $H \subset N$. Each $x \in H$ necessarily has order a power-of-p, since H does. So $x \in Y$. Thus $H \subset Y$. ♦

Conventions. In this section, G is always a finite gp; let $N := \mathrm{Ord}(G)$. Fix a prime p and write $\mathrm{Ord}(G) = p^L \cdot n$, with $n \perp p$. A subgroup $K \subset G$ is a "***p-Sylow*** subgroup of G" if $^{\#}\mathrm{Ord}(K) = p^L$. Our standing convention is:

54: *Subgroups $Y, X \subset G$ are p-Sylow, and $H \subset G$ is a p-subgroup.*

Henceforth I use 5 to represent p and $L = 4$. So $625 \bullet\!| \; N \nmid 3125$. Let $\mathcal{Y}$ be the *set* of 5-Sylow subgps of G.

We will consider G acting on $\mathcal{Y}$ via conjugation: For an $x \in G$, the action of x on $Y \in \mathcal{Y}$ is conjugation $K \mapsto xKx^{-1}$.

55: Sylow Thm.

a: *For each Po5 $5^k \leqslant 625$, there exists a G-subgroup H, with $^{\#}H = 5^k$.*

b: *There exists a Sylow subgp. I.e, $\mathcal{Y}$ is non-empty.*

c: *Each Po5 subgp H lies inside some 5-Sylow subgroup K. Indeed, for each G-orbit $\mathcal{O} \subset \mathcal{Y}$. there exists a $K \in \mathcal{O}$ with $\boxed{K \supset H}$.*

d: *The 5-Sylow subgps $\mathcal{Y}$ form one single G-orbit. Furthermore*

$$\begin{aligned} {}^{\#}\mathcal{Y} &\bullet\!| \quad \mathrm{Ord}(G) \\ {}^{\#}\mathcal{Y} &\equiv_5 \quad 1\,. \end{aligned}$$ ♢

Whoa! The fol. lemma and proof is broken.

56: Lemma. *$G \supset H$ finite groups The index*

$$r \quad := \quad |\mathcal{N}(H) \therefore \mathcal{C}(H)|$$

divides $|\mathrm{Aut}(H)|$. When H is a cyclic p-group, i.e $|H| = p^{K+1}$, then

$$*: \qquad r \bullet\!| \; p^K[p{-}1]\,.$$

Suppose $H \in \mathrm{Syl}_p(G)$ is abelian. Then each of

$$|G \therefore \mathcal{N}_G(H)|,\ |\mathcal{N}_G(H) \therefore \mathcal{C}_G(H)|,\ |\mathcal{C}_G(H) \therefore H|$$

is co-prime to p. Consequently:

†: *If $H \in \mathrm{Syl}_p(G)$ is cyclic then* $r \perp p{-}1$.

If (†) and p is the smallest prime dividing $|G|$, then $\boxed{\mathcal{N}_G(H) = \mathcal{C}_G(H)}$, since (Lagrange) r divides $|G|$. ♢

Grouply-unique

Unfinished: as of 3Oct2018

Further results on Sylow subgroups

57: Thm. *Consider finite gps $G \rhd N$ and $H \in \mathrm{Syl}_5(G)$. Then the intersection $H \cap N$ is $\in \mathrm{Syl}_5(N)$.* ♢

Proof. Since it is a subgroup of H, this $H \cap N$ is a 5-gp. So it has an extension $\widehat{N} \in \mathrm{Syl}_5(N)$ with $\widehat{N} \supset H \cap N$.

This $\widehat{N}$ is a 5-gp, so *it* has an extension to a $\widehat{G} \in \mathrm{Syl}_5(G)$. Evidently $I := \widehat{G} \cap N$ is a 5-group and a subgp of N. But $I \supset \widehat{N}$, and $\widehat{N}$ has maximum cardinality among 5-subgps of N. Consequently

$$*: \qquad \widehat{G} \cap N \quad = \quad \widehat{N}\,,$$

since the groups are finite.

By Sylow, $\widehat{G}$ is conjugate to H; there is an $x \in G$ with $x\widehat{G}x^{-1} = H$. From $(*)$, then,

$$x\widehat{N}x^{-1} \quad = \quad x\widehat{G}x^{-1} \cap xNx^{-1} \quad = \quad H \cap N\,.$$

($xNx^{-1} = N$ since $N \lhd G$.) Thus $H \cap N$ has the cardinality of a 5-Sylow subgp of N, so it is one. (And therefore $H \cap N = \widehat{N}$.) ♦

58: Theorem. *Consider finite gps $G \rhd N$ and suppose $H \in \mathrm{Syl}_5(G)$. Then $\frac{HN}{N}$ is a 5-Sylow subgp of $\frac{G}{N}$.* ♢

Proof.

Normal subgroups

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

59: Thm. *For each $N \in \mathbb{N} \setminus \{4\}$, the alternating group $\mathbb{A}_N$ is simple.* $\Diamond$

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 $\text{Ord}(\mathbb{A}_3)=3$ is prime, group $\mathbb{A}_3$ is simple. So the first case we need consider is $N \geqslant 5$. Some of the lemmas below hold for lower N.

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

60: 3-cycle Lemma. *The solo 3-cycles generate $\mathbb{A}_N$.* $\Diamond$

Proof.

61: 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.* $\Diamond$

Proof.

Notes to me. Bertrand Postulate.

Burnside's Normal p-complement Theorem.

Filename: `Problems/Algebra/algebra.basic-defns.latex`

As of: *Friday 27Jul2018.* Typeset: *3Oct2018 at 08:54.*