Basic Algebra definitions

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
27 March, 2024 (at *17:36*)

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 $(\Gamma,+,0)$ is a commutative group.

R3: Triple $(\Gamma,\cdot,1)$ 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 $\mathbf{U}(F)=F\smallsetminus\{0\}$] is a ***field***. That is to say, F is a commRing where triple $(F\smallsetminus\{0\},\cdot,1)$ 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 $\{\pm2,\pm3,\pm4,6\}$.

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 $\{\pm1,\pm5\}$. 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 $\{\pm1,\pm\mathbf{i}\}$. [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[♡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, 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.*

1: Lemma. *In a commRing*[♡1] *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

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

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

[♡1] More generally, a commutative monoid.

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

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

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

Bézout produces $S,T \in \Gamma$ with

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

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

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

4: 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. ♦

[♡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.

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

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

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 $g \equiv \mathbf{0}$.]

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 $\mathcal{E} \cdot g \equiv \mathbf{0}$.] □

Back to Semigroups/Monoids

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 $x \bullet y$.

5: 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.

6: 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:*

6a: *If $y \ltimes y = y$, then $y = \mathbf{e}$.*

Moreover:

6b: *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 (6a). 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 (6b). First let's show that every RInv, y', of y, is also a LInv of y. Let $b := [y' \ltimes y]$. Courtesy (6a), it is enough to show that $b \ltimes b = b$. And

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

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, $\mathbf{e} \ltimes y = y$. ♦

Terms. A general group might be written $(G, \cdot, \mathbf{e})$ or $(\Gamma, \cdot, \varepsilon)$ 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 $(\mathbf{V}, +, \mathbf{0})$ or $(\mathbf{U}, +, \mathbf{0})$. A group of *functions*, under composition, might be written $(G, \circ, Id)$.

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 $(\mathbb{Z}_N, +)$ when written additively, but use $\mathbb{Y}_N$ or $(\mathbb{Y}_N, \cdot)$ 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).

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 $\{\mathbf{e}\}$. □

7: 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,

$$\text{H-Ord}_G(x) \mathrel{\bullet\!|} \text{K-Ord}_G(x) \mathrel{\bullet\!|} \text{Ord}_G(x).$$ ◊

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

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 $N = D \mathrel{\bullet\!|} k$. ♦

8: *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,

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

Dihedral groups

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

9: $V := \left\langle \mathsf{a}, \mathsf{b}, \mathsf{c} \;\middle|\; \text{Each of } \{\mathsf{a},\mathsf{b},\mathsf{c}\} \text{ is an involution, each pair commutes, and the product of each two equals the third.} \right\rangle$.

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

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

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

10: $\mathbb{D}_N := \langle \mathtt{R}, \mathtt{F} \mid \mathtt{F}^2 = \mathbf{e},\ \mathtt{FRFR} = \mathbf{e},\ \mathtt{R}^N = \mathbf{e} \rangle$;
$\mathbb{D}_\infty := \langle \mathtt{R}, \mathtt{F} \mid \mathtt{F}^2 = \mathbf{e},\ \mathtt{FRFR} = \mathbf{e} \rangle$, for $N = \infty$.

Now for some straightforward facts.

11: 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 $\text{Ord}(\mathbb{D}_\infty) = \aleph_0$. ◊

12: 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 $\text{Inn}()$-group.*

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

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

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

$$\mathtt{R}^j \mapsto J_{\mathtt{R}^k} \quad \text{and} \quad \mathtt{FR}^j \mapsto J_{\mathtt{FR}^k}$$ *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 $2j \mathrel{|\!\bullet} N$. So the only possible nt-element in the center is $\mathtt{R}^K$, where $N = 2K < \infty$. And $\mathtt{R}^K$ commutes with each $\mathtt{FR}^j$. ♦

Some theorems (Lame title; I know)

Results to be proved in class.

13: Lagrange's theorem. *Suppose H is a subgroup of finite group G. Then $\text{Ord}(H)$ divides $\text{Ord}(G)$.* ◊

Proof. Define equiv-rel $\sim$ on G by $\alpha \sim \beta$ by $\alpha\beta^{-1} \in H$. Etc. ♦

14: 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. ♦

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 (23), 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.

15: *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. □

16: *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 $\boxed{\mathsf{X}\mathsf{S}\mathsf{X}^{-1} = \mathsf{S}^2}$. Consequently,

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

This is a *proper* subset of H. □

17: *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 $\mathtt{R}^2$. □

18: 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 $\Gamma\mathsf{N} = \mathsf{N}\Gamma$. ♦

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

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

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

20: Direct-product Lemma. *Suppose $\mathsf{N}, \Gamma \subset \widehat{G}$ groups, with $\mathsf{N} \lhd \widehat{G}$, 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 (19), the following are equivalent:

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

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

Pf (ii)⇒(iii). Always $\{\mathbf{e}\}\times\Gamma \lhd \mathsf{N}\times\Gamma$. 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 $\mathsf{N} \lhd \widehat{G}$. Hence

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

And $x\alpha x^{-1} \in \Gamma$, since $\Gamma \lhd G$. 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

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

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 $\psi{:}G\circlearrowright$ send H into itself.

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

22:

	Which Homs?	Then written as
	... $\psi \in \mathrm{Inn}(G)$	$H \lhd G$
	... $\psi \in \mathrm{Aut}(G)$	$H \overset{\mathrm{Aut}}{\lhd} G$
	... $\psi \in \mathrm{SurEnd}(G)$	$H \overset{\mathrm{Sur}}{\lhd} G$
	... $\psi \in \mathrm{End}(G)$	$H \overset{\mathrm{End}}{\lhd} G$

23: *Note.* In the $H \lhd G$ and $H \overset{\mathrm{Aut}}{\lhd} G$ 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 $\psi := \alpha$ *and* $\psi := \alpha^{-1}$.□

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. □

24: *E.g.* Each $x \in G$ engenders a ***conjugation map*** $J_x{:}G\circlearrowright$ 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

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

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

26: $$\mathrm{Inn}(G) \cong \tfrac{G}{\mathcal{Z}(G)}.$$

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

25′: $$\mathcal{J}_H : \mathcal{N}G(H) \to \mathrm{Aut}(H) : x \mapsto J_x\restriction_H.$$

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

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

27: Lemma. *Suppose* $|G{:}H| = 2$. *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 $|G{:}H| = 2$ need *not* imply the stronger $H \overset{\mathrm{Aut}}{\lhd} G$. In the Vierergruppe, (**??′**), the $\langle a \rangle_V$ subgroup has index 2 in V. Yet the automorphism that exhanges a and b moves $\langle a \rangle$.

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

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

29: $$[H \overset{\mathrm{Aut}}{\lhd} G \overset{\mathrm{Aut}}{\lhd} F] \implies H \overset{\mathrm{Aut}}{\lhd} F.$$

30: $$[H \overset{\mathrm{Aut}}{\lhd} G \lhd F] \implies H \lhd F.$$

And $[H \overset{\mathrm{End}}{\lhd} G \overset{\mathrm{End}}{\lhd} F] \Rightarrow H \overset{\mathrm{End}}{\lhd} F$. *Proof.* Use (23). ♢

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

31: 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* $\mathcal{Z}(G) \overset{\mathrm{Sur}}{\lhd} G$, *but not necessarily* $\overset{\mathrm{End}}{\lhd}$.

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

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

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

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 $\{\boldsymbol{\varepsilon}\}{\times}F$. $\blacklozenge$

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 $\alpha \in \mathrm{Aut}(\mathbb{D}_4)$ 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 $A := \mathrm{Aut}(\mathbb{D}_4) \cong \mathbb{D}_4$. Its subgp $S := \mathrm{Inn}(\mathbb{D}_4) \cong \mathbb{D}_2$ is isomorphic to a Vierergruppe. One can interpret the above α as in $\mathrm{Aut}(A)$, and as carrying S to the *other* copy of the Vierergruppe. $\blacklozenge$

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

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

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

Proof. Let G be

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

By (12)...

Unfinished: as of 27Mar2024 $\blacklozenge$

Examples of homomorphisms. For posints K,L and cyclic gps $\mathbf{(}\mathbb{Z}_K, +\mathbf{)}$ and $\mathbf{(}\mathbb{Z}_L, +\mathbf{)}$, 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, $DA \cdot f(1) \;\text{⧓}\; DB$. Hence we need $A \cdot f(1) \;\text{⧓}\; B$. Since $A \perp B$, this latter is equiv to $f(1) \;\text{⧓}\; B$. 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

33a: *Defn.* 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 relation: $x \sim_D y$ IFF $\langle x\rangle_G = \langle y\rangle_G$. □

33b: Phi-divides Lemma (Chap4#4.4Coro P84). *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*

†: $\varphi(D)$ *divides* $|S_{D,G}|$. *Indeed,*

$$\varphi(D) \cdot M = |S_{D,G}|,$$

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

Pf (⇐). 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. ♦

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

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

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

Ques. *Q1.* Suppose $N := \mathrm{Ord}(G)$ is finite, and posint $D \bullet\!\!\mid N$. 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 a *flip* F and an order-N *rotation* 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", $\mathrm{F}\mathrm{R}^i$, 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 $\langle \mathrm{R}\rangle$ of each of these orders is

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

And $8 + 4 + 2 + 1 = 15$.[♡3]

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

35: 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 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 $4 \not\mid 6$.

The upshot is that no elt of $H \smallsetminus \{\mathrm{e}\}$ is $\lceil 2,2\rfloor$, so each is a $\lceil 3,1\rfloor$. And there are 5 of them. Courtesy (33b), then, $5 \bullet \varphi(3)$. But $5 \not\mid 2$. ♦

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

36: Cauchy's Thm for finite *abelian* groups. *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

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

is onto, since $f\big((1, 0, \ldots, 0)\big) = g_1$, 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 (36). WELOG $p := 5$. We may assume that

37: *If Q is a finite abelian group with $\mathrm{Ord}(Q) \bullet\!\!| 5$, 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 $\mathrm{Ord}_G(y) \bullet\!\!| 5$. [*Why? Power $y^{\mathrm{Ord}(y)/5}$ has order 5.*]

Since $|G| > 1$ we can pick a nt-element $h \in G$; WLOG $K := \mathrm{Ord}(h) \nmid 5$. 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 (37) 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. ♦

Group actions. The symbol $G \circlearrowright \Omega$ means that gp G ***acts on*** set Ω; there is a gp-hom $\boxed{\psi{:}G{\to}\mathbb{S}_\Omega}$. 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:

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

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

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

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

40: Burnside's Lemma. *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,

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

Proof. The number of G-orbits equals

$$\sum_{\omega\in\Omega}\frac{1}{|\mathcal{O}(\omega)|} \overset{\text{Orb-Stab, (39}*\text{)}}{=\!=\!=} \frac{1}{|G|}\cdot\sum_{\omega\in\Omega}|\mathrm{Stab}(\omega)|\,.$$

Now apply (40†) to earn (40‡). ♦

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 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 2^{nd} 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

$$41: \qquad K^2\cdot[K^4+3K^2+12K+8]\big/24\,. \quad (\textit{Faces})$$

Coloring a cube's vertices. K-color the eight vertices of a cube. How many rotationally-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

$$42: \qquad K^2\cdot[K^6+17K^2+6]\big/24\,. \quad (\textit{Vertices})$$

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

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

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

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

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

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

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

$$43: \qquad |\Omega| = |\mathrm{Fix}(G)| + \sum_{\omega\in\mathcal{O}\mathit{Reps}}\frac{|G|}{|\mathrm{Stab}_G(\omega)|}\,.$$

Specializing to conjugation. We now let $\Omega:=G$, and have G act on Ω by conjugation. So we have a homomorphism $\mathcal{J}:G\to\mathbb{S}_\Omega$ 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

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

A conjugacy class is "non-trivial" if it has more than one point. So $\mathfrak{C}(h)$ 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 $\mathfrak{C}$. Let NT-$\mathfrak{CC}$ comprise one representative per **Non-Trivial** $\mathfrak{C}$.

44: Class-Equation Thm (After$^{\#}$**24.1**^{P}*388*). *For a finite group G,*

$$44': \qquad |G| \;=\; |\mathcal{Z}(G)| + \sum_{h\in \text{NT-}\mathfrak{CC}} \frac{|G|}{|\mathcal{C}(h)|}\,.$$

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 $\text{Fix}(G)$ is the center $\mathcal{Z}(G)$. ♦

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

45: Center-pop Thm (P.403). *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 $|\mathcal{Z}(G)|$. ♦

46: Cauchy's Thm for finite groups (P.406). *Suppose $N := |G| < \infty$. If prime $p \bullet\!\!| N$, then there exists $y \in G$ with $\text{Ord}(y) = p$.* ♢

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

If $p \bullet\!\!| \text{Ord}(Q)$ then Q has an order-p 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 $p \bullet\!\!| \text{Ord}(\mathcal{Z}(G))$.

We may now apply (36), 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 (37) uses induction on quotient groups, but does not use the Class-Eqn, whereas Center-pop Thm (45) uses the class equation but no induction. The above Cauchy's thm (46), used quotient-induction to put the class equation in play.

An jazzed-up (46) argument will give Sylow's first theorem. □

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

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

We now show that this holds universally. □

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

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

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

So WLOG $p^K \nmid \mathcal{C}_G(h)$, for each h in NT-$\mathfrak{CC}(G)$. Thus p divides the $\sum$-sum in (**??'**). So $p \bullet\!\!| \text{Ord}(\mathcal{Z}(G))$.

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 (48), 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.

49: 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 $x_1 x_2$ equals

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

And this equals $x_2 x_1$. ♦

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

50: 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

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

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 $[zH]^n$. ♦

51: 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 $a \leftrightarrows c$,

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

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

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

52: Prop'n (Chap7#**7.2**P144). *Suppose K,$L \subset G$ are groups. Then*

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

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

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

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

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

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. ♦

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.

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

†:
$$p{-}1 \not\vdots q{-}1 \quad \textit{and} \quad p \not\vdots q{-}1 \,.$$

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

54: *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 (54). 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 (53†).

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 (52†), then,

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

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

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

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

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

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

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 $\big(\Phi(q), \cdot\big)$. Thus p divides $\varphi(q) \overset{\text{note}}{=\!=} q-1$. But this annoys (53†). ♦

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.

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

$*$: $$p \;\nmid\; |G\!:\!Y| \overset{\text{note}}{=\!=} \tfrac{\#G}{\#Y}\,.$$

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. □

56: 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 $|G:Y|$ is coprime to p. But $|G:Y| = |G:N| \cdot |N:Y|$, so $p \nmid |N:Y|$. We may thus apply (55) to groups $Y \lhd N$, to conclude:

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

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:

57: *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 $K \mapsto xKx^{-1}$.

58: Sylow Thm.

a: *For each Po5 $5^k \leq 625$, 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 $K \supset H$.*

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

$$^{\#}\mathcal{Y} \bullet\!| \mathrm{Ord}(G)$$
$$^{\#}\mathcal{Y} \equiv_5 1\,.$$ ◊

Whoa! The fol. lemma and proof is broken.

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

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

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

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

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

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

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 $\mathcal{N}G(H) = \mathcal{C}_G(H)$, since (Lagrange) r divides $|G|$. ◊

Grouply-unique

Unfinished: as of 27Mar2024

Further results on Sylow subgroups

60: 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

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

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,

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

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

61: 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:

62: Thm. *For each $N \in \mathbb{N} \setminus \{4\}$, 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 $\text{Ord}(\mathbb{A}_3)=3$ 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 $3, 1, 1, \overset{N-3}{\ldots} 1$. □

63: 3-cycle Lemma. *The solo 3-cycles generate $\mathbb{A}_N$.* ♢

Proof.

64: 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.

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

§Index for Basic Algebra

Filename: `Problems/Algebra/algebra.basic-defns.latex`
As of: *Friday 27Jul2018.* Typeset: *27Mar2024* at *17:36.*