

Basic Algebra definitions

Jonathan L.F. King

University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu

Webpage <http://squash.1gainesville.com/>

6 July, 2018 (at 11:20)

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 $\alpha \bullet \beta$.

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

R3: Triple $(\Gamma \setminus \{0\}, \cdot, 1)$ 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 $\alpha, x, y \in \Gamma$.

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

^{♥1}What I’m calling a semigroup is usually called a *monoid*.

\mathbf{ZD} , since $0 \cdot 1 = 0 = 1 \cdot 0$, and $1 \neq 0$. We write the set of Γ -zero-divisors as

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

An $\alpha \in \Gamma$ is a Γ -*unit* if $\exists \beta \neq 0$ st. $\alpha\beta = 1 = \beta\alpha$.
Use Units_Γ or $\text{Units}(\Gamma)$

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 $\varphi(N) := |\Phi_N|$.

Characteristic of a ring. In a ring $(\Gamma, +, 0, \cdot, 1)$, if there is a posint n so that $\mathbf{1} + \mathbf{1} + \dots + \mathbf{1}$ equals $\mathbf{0}$, then the *smallest* such n is called the “*characteristic* of Γ ”, written as $\text{Char}(\Gamma) = n$. If no such posint exists, then it would make sense to write $\text{Char}(\Gamma) = \infty$; however, the *standard term* is $\text{Char}(\Gamma) = 0$. As examples, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ each have characteristic zero, whereas \mathbb{Z}_6 has characteristic 6. (As does $\mathbb{Z}_6[[x]]$, the ring of polynomials with coeffs from \mathbb{Z}_6 .)

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

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

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:** In an arbitrary ring Γ , the set $\mathbf{ZD}(\Gamma)$ is *disjoint* from $\text{Units}(\Gamma)$.

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.

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

Two ring-elements α and β are **associates**, written $\alpha \overset{\text{as}}{\sim} \beta$, if $\alpha \bullet \beta$ and $\alpha \blacktriangleright \beta$ [i.e. $\alpha \in \beta\Gamma$ and $\beta \in \alpha\Gamma$]. They are **strong associates** if there exists a unit u st. $\beta = u\alpha$. **Exer:** Prove *Strong-Assoc* \Rightarrow *Assoc*.

Exer: Ring \mathbb{Z}_N has no irreducible elements, since \mathbb{Z}_N is the disjoint-union $\text{ZD} \sqcup \text{Units}$.

Exer: *PRIME* \Rightarrow *IRRED*. However there are rings^{♥2} with irreducible elements ρ which are nonetheless not prime.

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

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 $x \bullet y$.

1: 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. \diamond

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 $\lambda_1 = \rho = \lambda_2$. \diamond

^{♥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.

Proof of (ii). Given $x \in S$, pick a RInv r and a LInv 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. \diamond

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

2: Lemma. Suppose \times 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:

2a: If $y \times y = y$, then $y = \mathbf{e}$.

Moreover:

2b: Each y' is also a left inverse to y , and \mathbf{e} is also a lefthand-identity.

Thus (S, \times, \mathbf{e}) is a group, \diamond

Pf (2a). Note $y = y \times \mathbf{e} = y \times [y \times y'] = [y \times y] \times y'$. By hypothesis $y \times y = y$, so the above asserts that $y = y \times y' \overset{\text{note}}{=} \mathbf{e}$. \diamond

Pf of (2b). First let’s show that every RInv, y' , of y , is also a LInv of y . Let $b := [y' \times y]$. Courtesy (2a), it is enough to show that $b \times b = b$. And

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

We can now show that \mathbf{e} is also a lefthand identity. After all, $\mathbf{e} \times y = [y \times y'] \times y = y \times [y' \times y] = y \times \mathbf{e}$, since y' is a LInverse. I.e. $\mathbf{e} \times y = y$. \diamond

Henceforth, groups^{♥3} are the subject.

^{♥3}Here is my generic footnote: Typical group notation: (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 $(\mathbf{V}, +, \mathbf{0})$. A group of *functions*, under composition, might be written (G, \circ, Id) .

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

Cyclic groups

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

For $y \in G$ we use $\text{Periods}_G(y)$ 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 $\text{Periods}(y)$ is simply $P_H(y)$, when H is the trivial subgp $\{\mathbf{e}\}$.

3: 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,

$$H\text{-Ord}_G(y) \blacklozenge K\text{-Ord}_G(y) \blacklozenge \text{Ord}_G(y). \quad \blacklozenge$$

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

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

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

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

$$3': \forall y \in G: \text{Ord}_{G/H}(yH) = H\text{-Ord}_G(y) \blacklozenge \text{Ord}_G(y).$$

Dihedral groups

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

$$5: V := \left\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \mid \begin{array}{l} \text{Each of } \{\mathbf{a}, \mathbf{b}, \mathbf{c}\} \text{ is an involution,} \\ \text{each pair commutes, and the prod-} \\ \text{uct of each two equals the third.} \end{array} \right\rangle.$$

Use $\text{Cyc}_N, \mathbb{S}_N, \mathbb{D}_N$ for the N^{th} cyclic, symmetric and dihedral groups. So $|\text{Cyc}_N|=N$ 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 $Z(G)$ for the center of G . The automorphisms of G form a group $(\text{Aut}(G), \circ, \text{Id})$.

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 $\text{Inn}(G)$; it is a normal subgp of $\text{Aut}(G)$. The map $\beta: G \rightarrow \text{Aut}(G)$ by $\beta(x) := J_x$, is a group homorphism.

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

$$5': V = \langle \mathbf{a}, \mathbf{b} \mid \mathbf{a}^2 = \mathbf{e} = \mathbf{b}^2, \mathbf{a} \trianglelefteq \mathbf{b} \rangle.$$

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

$$6: \begin{array}{l} \mathbb{D}_N := \langle \mathbf{r}, \mathbf{f} \mid \mathbf{f}^2 = \mathbf{e}, \mathbf{frfr} = \mathbf{e}, \mathbf{r}^N = \mathbf{e} \rangle; \\ \mathbb{D}_\infty := \langle \mathbf{r}, \mathbf{f} \mid \mathbf{f}^2 = \mathbf{e}, \mathbf{frfr} = \mathbf{e} \rangle, \text{ for } N = \infty. \end{array}$$

Now for some straightforward facts.

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

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

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

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

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

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

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

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

where $k := [j \text{ mod } K]$. \blacklozenge

Proof. The commutator $[\mathbf{r}^j, \mathbf{f}]$ equals

$$\mathbf{r}^j \mathbf{fr}^{-j} \mathbf{f}^{-1} = \mathbf{r}^{2j} \mathbf{f}^2 = \mathbf{r}^{2j}.$$

Thus $\mathbf{r}^j \trianglelefteq \mathbf{f}$ IFF $2j \blacklozenge N$. So the only possible nt-element in the center is \mathbf{r}^K , where $N = 2K < \infty$. And \mathbf{r}^K commutes with each \mathbf{fr}^j . \blacklozenge

Normality

Consider two gps $H \subset G$. Say that “ H is **normal** in G ”, written $H \triangleleft G$, if $[\forall x \in G: xHx^{-1} = H]$. This is equivalent (see (17), below) to $[\forall x \in G: xHx^{-1} \subset H]$. However, an individual element x could give proper inclusion, as the following two examples show.

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

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

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

$$\dagger: \quad n \xrightarrow{x} n-5 \xrightarrow{h} n-5 \xrightarrow{x^{-1}} n,$$

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

Note that (\dagger) 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 $xHx^{-1} \subsetneq H$, proper inclusion. \square

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

In $G := \text{GL}_2(\mathbb{Q})$, the shear $S := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ generates $H := \langle S \rangle_G$, which is a copy of $(\mathbb{Z}, +)$. Conjugating by $X := \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ produces $\boxed{XSX^{-1} = S^2}$. Consequently,

$$XHX^{-1} = \left\{ \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\}.$$

This is a proper subset of H . \square

11: Defn. For subsets $N, \Gamma \subset G$, let $N\Gamma$ mean the set of products $x\alpha$, over all $x \in N$ and $\alpha \in \Gamma$. Even when N and Γ are subgroups, the product $N\Gamma$ need not be a subgroup.

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

12: Lemma. If at least one of the subgroups $N, \Gamma \subset G$ is normal in G , then $\Gamma N = N\Gamma$, and this product is itself a G -subgroup. \diamond

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

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

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

$$13: \quad f: N \times \Gamma \rightarrow N\Gamma, \quad \text{by } (x, \omega) \mapsto x\omega,$$

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

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

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

Recalling the bijection. $f: N \times \Gamma \rightarrow G$ from (13), the following are equivalent:

- i: $N \trianglelefteq \Gamma$, inside G .
- ii: f is a homomorphism, hence isomorphism.
- iii: $\Gamma \triangleleft G$. \diamond

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

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

since $N \trianglelefteq \Gamma$. And this equals $f((xy, \alpha\beta))$. \blacklozenge

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

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

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

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

And $x\alpha x^{-1} \in \Gamma$, since $\Gamma \triangleleft G$. So $x\alpha x^{-1} \cdot \alpha^{-1} \in \Gamma$. Thus $\llbracket x, \alpha \rrbracket \in N \cap \Gamma$, so $\llbracket x, \alpha \rrbracket = \mathbf{e}$. \blacklozenge

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

$$15: \text{Inn}(G) \subset \text{Aut}(G) \subset \text{SurEnd}(G) \subset \text{End}(G).$$

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

Suppose that $\psi(H) \subset H$ for every ...		
	WHICH HOMs?	THEN WRITTEN AS
	... $\psi \in \text{Inn}(G)$	$H \triangleleft G$
16:	... $\psi \in \text{Aut}(G)$	$H \triangleleft^a G$
	... $\psi \in \text{SurEnd}(G)$	$H \triangleleft^{se} G$
	... $\psi \in \text{End}(G)$	$H \triangleleft^e G$

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

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 . \square

18: *E.g.* Each $x \in G$ engenders a *conjugation map* $J_x: G \curvearrowright$ 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 $\text{Inn}(G)$. This map

19: $\mathcal{J}: G \rightarrow \text{Inn}(G) : x \mapsto J_x$

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

20: $\text{Inn}(G) \cong \frac{G}{Z(G)}.$

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

19': $\mathcal{J}_H : \mathcal{N}_G(H) \rightarrow \text{Aut}(H) : x \mapsto J_x \downarrow_H.$

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

$$A := \text{Range}(\mathcal{J}_H) \subset \text{Aut}(H). \quad \square$$

21: **Lemma.** Suppose $|G:H| = 2$. Then $H \triangleleft G$. \diamond

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 $H \triangleleft G$. \diamond

Remark. Index $|G:H| = 2$ need *not* imply the stronger $H \triangleleft^a G$. In the Vierergruppe, (5'), the $\langle a \rangle_V$ subgroup has index 2 in V . Yet the automorphism that exchanges 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 $\langle \mathbf{f} \rangle$ has index 3. \square

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

23: $[H \triangleleft^a G \triangleleft^a F] \implies H \triangleleft^a F.$

24: $[H \triangleleft^a G \triangleleft F] \implies H \triangleleft F.$

And $[H \triangleleft^e G \triangleleft^e F] \implies H \triangleleft^e F$. *Proof.* Use (17). \diamond

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

25: **Normal Grabbag.**

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

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

iii: $\text{Inn}(G) \triangleleft \text{Aut}(G)$, but not necessarily \triangleleft^a . \diamond

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

$$[[H, K]] \ni [[\hat{h}, \hat{k}]] \stackrel{\text{note}}{=} \widehat{[[h, k]]}. \quad \blacklozenge$$

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

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

$$\mathbf{e} = \widehat{\gamma z \gamma^{-1}} = \hat{\gamma} \cdot \hat{z} \cdot \hat{\gamma}^{-1} = g \cdot \hat{z} \cdot g^{-1}. \quad \blacklozenge$$

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

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

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

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

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

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,

$$\begin{aligned} V &:= \langle \mathbf{r}^2, \mathbf{f} \rangle = \{\mathbf{e}, \mathbf{r}^2, \mathbf{f}, \mathbf{fr}^2\} \quad \text{and} \\ V' &:= \langle \mathbf{r}^2, \mathbf{fr} \rangle = \{\mathbf{e}, \mathbf{r}^2, \mathbf{fr}, \mathbf{fr}^3\}. \end{aligned}$$

And $\alpha(V) = V'$, where $\alpha \in \text{Aut}(\mathbb{D}_4)$ is the automorphism which sends $\mathbf{r} \mapsto \mathbf{r}$ and $\mathbf{f} \mapsto \mathbf{fr}$.

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

Examples of normal subgps. On \mathcal{D} -dim'al Euclidean space $\mathbb{R}^{\mathcal{D}}$, 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* $\mathbb{R}^{\mathcal{D} \circ}$.

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

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

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 $\mathsf{L} \circ \mathsf{T}_{\kappa} \circ \mathsf{L}^{-1}$ is some translation. But

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

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

Proof. Let G be

$$\mathbb{D}_2 \times \mathbb{D}_4 \times \mathbb{D}_8 \times \mathbb{D}_{16} \times \dots$$

By (8)...

Unfinished: as of 6Jul2018 \blacklozenge

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

Let $D := \text{Gcd}(K, L)$ 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

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

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

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

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

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

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

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

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. \diamond

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

28: Lemma. *Suppose $\psi: G \rightarrow Q$ is a surjective group-homomorphism. Then $\text{Ord}(Q) \mid \text{Ord}(G)$. Indeed, $|Q| \cdot |K| = |G|$, where $K := \text{Ker}(\psi)$.* \diamond

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

29: Lagrange's Theorem. *Given groups $H \subset G$, then, $\text{Ord}(H) \mid \text{Ord}(G)$.* \diamond

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

Ques. Q1. Suppose $N := \text{Ord}(G)$ is finite, and posint $D \mid N$. 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 \mathbf{f} and an order- N rotation \mathbf{r} .

Although $\text{Ord}(\mathbb{D}_{15}) = 30$ and $6 \mid 30$, nonetheless \mathbb{D}_{15} has no elt of order 6: Its 15 “flip elts”, $\mathbf{f}\mathbf{r}^i$, 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 $\langle \mathbf{r} \rangle$ of each of these orders is

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

And $8 + 4 + 2 + 1 = 15$. \heartsuit^4

Although \mathbb{D}_{15} has no element of order-6, it does have a subgroup of order 6. The subgp $\langle \mathbf{f}, \mathbf{r}^5 \rangle$ is isomorphic to \mathbb{D}_3 . \diamond

30: Really really No. *Although $\text{Ord}(\mathbb{A}_4) = 12$ and $6 \mid 12$, nonetheless \mathbb{A}_4 has no subgroup of order 6:* \diamond

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

Cyc-struct	$[1, 1, 1, 1]$	$[2, 2]$	$[3, 1]$
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 $[3, 1]$. If H owned a $[2, 2]$ α , then $\alpha' := \beta\alpha\beta^{-1}$ would have to be a *different* $[2, 2]$ (they couldn't commute). But then H includes the Klein-4 group $\langle \alpha, \alpha' \rangle$. Yet $4 \nmid 6$.

The upshot is that no elt of $H \setminus \{\mathbf{e}\}$ is $[2, 2]$, so each is a $[3, 1]$. And there are 5 of them. Courtesy (27), then, $5 \mid \varphi(3)$. But $5 \nmid 2$. \diamond

31: Cauchy's Thm for finite abelian groups. *Suppose $N := |G| < \infty$ where G is an abelian group, written multiplicatively. If prime $p \mid N$, then there exists $y \in G$ with $\text{Ord}(y) = p$.* \diamond

\heartsuit^4 Indeed, this yields a proof that $\sum_{d \mid N} \varphi(d)$ equals N .

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

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

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

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

$$f: \widetilde{G} \rightarrow G \text{ by } f((\ell_1, \dots, \ell_N)) := g_1^{\ell_1} g_2^{\ell_2} \dots g_N^{\ell_N}$$

is onto, since $f((1, 0, \dots, 0)) = g_1$, etc.. And f is a group-homomorphism since G is abelian. Thus $\text{Ord}(G) \bullet \text{Ord}(\widetilde{G})$. Hence $p \bullet \text{Ord}(G) \bullet \widetilde{K}$. \blacklozenge

A more standard proof uses induction on quotient groups.

Pf of (31). WELOG $p := 5$. We may assume that

32: *If Q is a finite abelian group with $\text{Ord}(Q) \bullet 5$, 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 $\text{Ord}_G(y) \bullet 5$.

Since $|G| > 1$ we can pick a nt-element $h \in G$; WLOG $K := \text{Ord}(h) \nmid 5$. Thus 5 divides $\frac{N}{K}$, which is the order of $Q := \frac{G}{\langle h \rangle}$, where $H := \langle h \rangle$; note $H \triangleleft G$ since G is abelian. Finally, $h \neq e$ so $|Q| < |G|$.

Thus (32) applies to produce an element $y \in G$ with $\text{Ord}_Q(yH) = 5$. And by (3,3'), the Periods Lemma, $\text{Ord}_G(y) \bullet \text{Ord}_Q(yH)$. \blacklozenge

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

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

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

$$33: \quad \forall f \in G: \quad f \cdot \text{Stab}(\omega) \cdot f^{-1} = \text{Stab}(f\omega).$$

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

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

Proof. Let $H := \text{Stab}(\omega)$. 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 (*). \blacklozenge

35: Burnside’s Lemma. *Counting cardinalities,*

$$\dagger: \quad \sum_{\omega \in \Omega} |\text{Stab}(\omega)| \stackrel{\#}{=} \left\{ (g, \omega) \mid g\omega = \omega \right\} \stackrel{\#}{=} \sum_{g \in G} |\text{Fix}(g)|.$$

Counting the number of G -orbits, then,

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

Proof. The number of G -orbits equals

$$\sum_{\omega \in \Omega} \frac{1}{|\mathcal{O}(\omega)|} \stackrel{\text{Orb-Stab, (34*)}}{=} \frac{1}{|G|} \cdot \sum_{\omega \in \Omega} |\text{Stab}(\omega)|.$$

Now apply (35†) to earn (35‡). \blacklozenge

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 ?	$\# \text{Fix}(g) = 3^F$.	$F := \# [\text{Face-orbits under } \langle g \rangle]$.
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

$$36: \quad K^2 \cdot [K^4 + 3K^2 + 12K + 8] / 24. \quad (\text{Faces})$$

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

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

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

37:
$$K^2 \cdot [K^6 + 17K^2 + 6] / 24. \quad (\text{Vertices})$$

Class equation

Consider a finite group acting on a finite set, $G \curvearrowright \Omega$, and let S be its set of orbits. The trivial assertion $|\Omega| = \sum_{\mathcal{O} \in S} |\mathcal{O}|$ leads to a useful formula, when we consider G acting on itself via conjugation. Firstly, the Orbit-Stabilizer thm restates the circled as

$$|\Omega| = \sum_{\omega \in \text{AllOReps}} \frac{|G|}{|\text{Stab}(\omega)|},$$

where “AllOReps” stands for “all orbit representatives”; this is one token ω per G -orbit. Now let

$$\text{Fix}(G) := \bigcap_{g \in G} \text{Fix}(g).$$

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

$$\text{OReps} := \text{AllOReps} \setminus \text{Fix}(G);$$

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

38:
$$|\Omega| = |\text{Fix}(G)| + \sum_{\omega \in \text{OReps}} \frac{|G|}{|\text{Stab}_G(\omega)|}.$$

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

Acting by conjugation, the stabilizer $\text{Stab}_G(\omega)$ 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 $h \in Z(G)$, where $Z(G) := \bigcap_{h \in G} \mathcal{C}(h)$ 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”.

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

39':
$$|G| = |Z(G)| + \sum_{h \in PCC} \frac{|G|}{|\mathcal{C}(h)|}.$$

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. \diamond

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

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

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

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

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

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(39'). So p divides $|Z(G)|$. \blacklozenge

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

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

If $p \nmid \text{Ord}(Q)$ 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 $PCC(G)$, has order not a multiple of p . Thus p divides the RhS(39') sum. So $p \nmid \text{Ord}(Z(G))$.

We may now apply (31), Cauchy's thm for abelian groups, to $Z(G)$, to get a order- p element. \blacklozenge

Remark. We get a nice progression of proofs. Note that (32) uses induction on quotient groups, but does not use the Class-Eqn, whereas Center-pop Thm (40) uses the class equation but no induction. The above Cauchy's thm (41), used quotient-induction to put the class equation in play.

An jazzed-up (41) argument will give Sylow's first theorem. \square

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

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

We now show that this holds universally. \square

42: Sylow's First Thm. For each prime p , for each natural number k and finite group G , proposition $P(k, G)$ holds. \blacklozenge

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

43: $P(K-1, *)$ holds. Also $P(K, Q)$ 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 Σ -sum in (39'). So $p \nmid \text{Ord}(Z(G))$.

Cauchy's thm for abelian groups now gives us a subgroup $H \subset Z(G)$ 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 (43), 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 $|H'| = |H| \cdot |Q'| = p \cdot p^{K-1} = p^K$. \blacklozenge

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

44: 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 $y_1 \rightleftharpoons y_2$. Then G is abelian. \blacklozenge

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

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

And this equals $x_2 x_1$. \blacklozenge

An immediate corollary is this “ $G \bmod Z$ ” lemma.

45: G/Z Lemma. We have a subgroup $H \subset Z(G)$; necessarily $H \triangleleft G$. If G/H is cyclic, then G is abelian. \blacklozenge

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

$$G = \langle \mathbf{r}, \mathbf{f} \mid \mathbf{f}^2 = \mathbf{e}, \mathbf{f}\mathbf{r}\mathbf{f} = \mathbf{e}, \mathbf{r}^4 = \mathbf{e} \rangle.$$

Its center is $H := \{\mathbf{e}, \mathbf{r}^2\}$ 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 $\{\mathbf{r}, \mathbf{r}^3\}$ and $\{\mathbf{f}, \mathbf{f}\mathbf{r}^2\}$ have *no* representatives which commute. \square

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 $[zH]^n$. \blacklozenge

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

$$\text{Ord}(ac) = p \cdot q. \quad \blacklozenge$$

Proof. Let $y := ac$. Were $y = e$ then $p = \text{Ord}(a) = \text{Ord}(c^{-1}) = \text{Ord}(c) = q; \not\approx$. So $\text{Ord}(y) \neq 1$.

Since $a \leftrightsquigarrow c$,

$$\text{Ord}(y) \bullet \text{Lcm}(p, q) \stackrel{\text{note}}{=} p \cdot q.$$

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

So $\text{Ord}(y) \nmid p$. Ditto $\text{Ord}(y) \nmid q$. But $\text{Ord}(y) \bullet pq$. Thus $\text{Ord}(y) = pq$. \blacklozenge

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

$$\ddagger: \quad |KL| = |K| \cdot |L| / |K \cap L|$$

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

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

$$\ddagger: \quad K \times L \rightarrow KL : (k, \ell) \mapsto k\ell$$

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

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

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

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.

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

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

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

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

49: 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 $h \in G \setminus K$ (an h exists, since $pq > q$) necessarily has order p . And h commutes with each chosen $k \in K \setminus \{e\}$. \square

Proof of (49). We proceed in four steps.

There exists an order- q element in G .

FTSOC, suppose no elt $x \in G \setminus \{e\}$ has order- q ; so each x has order- p . Since p is prime, the order- p elts come in equivalence classes, $\{x, x^2, \dots, x^{p-1}\}$, of size $p-1$. Hence $p-1$ must divide $\text{Ord}(G) - 1$. But

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

so this would imply $p-1 \bullet q-1$. But this $\not\approx$ s (48 \ddagger).

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

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

since q is prime. From (47 \ddagger), then,

$$|HK| = \frac{q \cdot q}{1}.$$

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

$$\frac{N_G(K)}{e} \stackrel{\text{note}}{=} \frac{G}{K}$$

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

$$p \bullet \text{Ord}(\text{Aut}(K)).$$

But K is finite-cyclic, so $\text{Aut}(K)$ is gp-isomorphic to $(\Phi(q), \cdot)$. Thus p divides $\varphi(q) \stackrel{\text{note}}{=} q-1$. But this annoys (48†). \blacklozenge

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.

50: Lemma. *Finite groups $Y \triangleleft G$ and prime p have*

$$*: \quad p \nmid |G:Y| \stackrel{\text{note}}{=} \frac{\#G}{\#Y}.$$

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

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

Remark. Dropping the normality $Y \triangleleft G$ 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. \square

51: Coro. *Suppose $Y \in \text{Syl}_p(G)$, and $H \subset G$ is a p -group. If $H \subset N_G(Y)$, then $H \subset Y$.* \blacklozenge

Proof. Let $N := N_G(Y)$. 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 (50) to groups $Y \triangleleft N$, to conclude:

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

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

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

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

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

$$\begin{aligned} \#\mathcal{y} &\bullet \text{Ord}(G) \\ \#\mathcal{y} &\equiv_5 1. \end{aligned} \quad \blacklozenge$$

Whoa! The fol. lemma and proof is broken.

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

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

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

$$*: \quad r \mid p^K [p-1].$$

Suppose $H \in \text{Syl}_p(G)$ 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 $H \in \text{Syl}_p(G)$ 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 $|G|$. \diamond

Grouply-unique

Unfinished: as of 6Jul2018

Further results on Sylow subgroups

55: Thm. Consider finite gps $G \triangleright N$ and $H \in \text{Syl}_5(G)$. Then the intersection $H \cap N$ is $\in \text{Syl}_5(N)$. \diamond

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

This \widehat{N} is a 5-gp, so it has an extension to a $\widehat{G} \in \text{Syl}_5(G)$. 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

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

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 $N \triangleleft G$.) Thus $H \cap N$ has the cardinality of a 5-Sylow subgp of N , so it is one. (And therefore $H \cap N = \widehat{N}$.) \diamond

56: Theorem. Consider finite gps $G \triangleright N$ and suppose $H \in \text{Syl}_5(G)$. Then $\frac{HN}{N}$ is a 5-Sylow subgp of $\frac{G}{N}$. \diamond

Proof.

Normal subgroups

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

57: 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 $N \geq 5$. Some of the lemmas below hold for lower N .

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

58: 3-cycle Lemma. The solo 3-cycles generate \mathbb{A}_N . \diamond

Proof.

59: 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 06Jul2018. Typeset: 6Jul2018 at 11:20.