

Group Notes

Jonathan L.F. King

University of Florida, Gainesville FL 32611-2082, USA

1 February, 2022 (at 13:14)

Terms. A general group might be written (G, \cdot, \mathbf{e}) or $(\Gamma, \cdot, \epsilon)$ 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 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*. 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 arbitrary set Ω engenders its symmetric group \mathbb{S}_Ω 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 $[xgx^{-1}]^n = [xg^n x^{-1}]$.

The “*commutator of elements α and β* ” is

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

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

Morphisms

A map $F: G \rightarrow \Gamma$ is a *homomorphism* [more precisely, a “*group homomorphism*”] if

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

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

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

1: Fact. *If a homomorphism is a bijection, then it automatically is an isomorphism.* *Proof.* Exercise. \diamond

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

$G \rightarrow \Gamma$	$G \rightarrow G$
<i>hom</i> = homomorphism,	<i>endo</i> = endomorphism,
<i>iso</i> = isomorphism,	<i>aut</i> = <i>auto</i> = automorphism.

The set $\text{Aut}(G)$ of automorphisms $G \rightarrow G$ forms a group under composition: the group $(\text{Aut}(G), \circ, Id_G)$. [The endomorphisms $f: G \rightarrow G$ form $(\text{End}(G), \circ, Id_G)$; a monoid.]

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

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

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

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

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

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

The centralizer of a subset $S \subset G$ is

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

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

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

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

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

For a subgroup $H \subset G$, automatically $\mathcal{N}G(H) \supset H$. When its normalizer is everything, $\mathcal{N}G(H) = G$, then we say “ H is *normal* in G ” and write $H \triangleleft G$ or $G \triangleright H$. By defn, $H \triangleleft \mathcal{N}G(H)$.

!!

2: N/C Theorem (#17^E203). Consider G , subgroup H , its normalizer $\mathcal{N} := \mathcal{N}G(H)$ and centralizer $\mathcal{C} := \mathcal{C}_G(H)$. This leads to a group-homomorphism $F: \mathcal{N} \rightarrow \text{Aut}(H)$ defined by restricting an inner-automorphism to H :

$$*: \quad F(x) := J_x|_H.$$

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

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

$$**: \quad \text{Index } |\mathcal{N}:\mathcal{C}| \text{ divides } \text{Ord}(\text{Aut}(H)). \quad \diamond$$

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

^{♥1}From German *Zentrum*.

Equiv-relation result

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

$$\dagger: \quad \kappa \cdot M = |\Lambda|$$

where M is the number of equiv-classes.

3a: Lagrange's theorem (#7.1^P142). Consider H , a subgroup of finite group G . Then

$$\dagger: \quad |H| \cdot \left[\begin{array}{l} \text{Number left-cosets} \\ \text{of } H \text{ in } G \end{array} \right] = |G|.$$

Hence $\text{Ord}(H)$ divides $\text{Ord}(G)$. ◇

Pf. Define equiv-rel \sim on G by $\alpha \sim \beta$ by $\beta^{-1}\alpha \in H$. The equiv-classes are the left cosets of H in G . Each coset is bijective with H . Etc. ◇

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

No. The N^{th} dihedral group \mathbb{D}_N is generated by a flip F and an order- N rotation R .

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

BTWay, the divisors k of 15 are 15, 5, 3, 1. The number of elts in $\langle R \rangle$ of each of these orders is

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

And $8 + 4 + 2 + 1 = 15$.^{♡2}

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

3b: Really really No. Although $\text{Ord}(\mathbb{A}_4) = 12$ and $6 \bullet | 12$, nonetheless \mathbb{A}_4 has no subgroup of order 6: ◇

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 $H \setminus \{e\}$ is [2, 2], so each is a [3, 1]. And there are 5 of them. Courtesy (4b), then, $5 \nmid \varphi(3)$. But $5 \nmid 2$. ◇

4a: Defn. 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 relation: $x \sim_D y$ IFF $\langle x \rangle_G = \langle y \rangle_G$. □

4b: Phi-divides Lemma (#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

$$\dagger: \quad \begin{array}{l} \varphi(D) \text{ divides } |S_{D,G}|. \text{ Indeed,} \\ \varphi(D) \cdot M = |S_{D,G}|, \end{array}$$

where M is the number of *cyclic* order- D subgroups of G . ◇

Proof. 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. ◇

^{♡2}Indeed, this yields a proof that $\sum_{d \bullet | N} \varphi(d)$ equals N .

5a: Prop'n (#7.2^P144). Suppose $K, L \subset G$ are groups. Then

$$\dagger: \quad |K \cap L| \cdot |KL| = |K \times L| \quad \text{I.e., product-set}$$

$$|KL| = \frac{|K| \cdot |L|}{|K \cap L|}.$$

[Note: Product-set KL may or may not be a group.] \diamond

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

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

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

5b: 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

5c: 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 $x\alpha = \alpha^{-1}x^{-1} \in \Gamma N = N\Gamma$. \diamond

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

$$\dagger: \quad |F(G)| \text{ divides } |G|. \quad \text{Indeed,}$$

$$|H| \cdot |F(G)| = |G|$$

where $H := \text{Ker}(F)$. \diamond

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

7a: Group actions. The symbol $G \curvearrowright \Omega$ means that gp G acts on set Ω ; there is a gp-hom $(F: G \rightarrow \mathbb{S}_\Omega)$. For $g \in G$ and $\omega \in \Omega$, write the gp-action as $F_g(\omega)$ 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 :

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

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

$$7b: \quad \forall f \in G: \quad f \cdot \text{Stab}(\omega) \cdot f^{-1} = \text{Stab}(f\omega). \quad \square$$

7c: Orbit-Stabilizer Lemma. For each token $\omega \in \Omega$:

$$\dagger: \quad \text{Ord}(\text{Stab}_F(\omega)) \cdot |\mathcal{O}_F(\omega)| = \text{Ord}(G). \quad \diamond$$

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

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.

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

$$\begin{aligned} \dagger: & \quad p-1 \nmid q-1 \quad \text{and} \\ \ddagger: & \quad p \nmid q-1. \end{aligned}$$

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

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

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

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

Proof of ().* 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 . Hence the Phi-divides Lemma says $\varphi(p) \stackrel{\text{note}}{=} p-1$ must divide $\text{Ord}(G) - 1$. Observe

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

so this would imply $p-1 \mid q-1$. But this \nexists s (8 \dagger).

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

This order- q subgp is unique. Were there

another, call it \widehat{K} , then

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

since q is prime. From (5a \dagger), then,

$$|\widehat{K}K| = \frac{q \cdot q}{1}.$$

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

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

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

$$q \mid \text{Ord}(\mathcal{C}) \mid pq.$$

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

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

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

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

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

But K is cyclic so $\text{Aut}(K)$ is isomorphic to $\mathbf{U}(q)$; i.e $|\text{Aut}(K)| = \varphi(q)$. Thus p divides $\varphi(q) \stackrel{\text{note}}{=} q-1$. But this annoys (8 \ddagger). \blacklozenge

What are some examples of this thm?

Works: $p < q$	Hypothesis fails: $p < q$	What exactly fails?
	$3 < q$	$2 \mid q-1$ (\dagger)
	$3 < 7$	$3 \mid 6$ (\ddagger)
$5 < 23$	$5 < 13$	$4 \mid 12$ (\dagger)
$5 < 19$	$5 < 11$	$5 \mid 10$ (\ddagger)
$7 < 11$	$7 < 13$	$6 \mid 12$ (\dagger)
$7 < 17$	$7 < 29$	$7 \mid 28$ (\ddagger)
$7 < 53$	$7 < 51$	<i>Ahem!</i>
$11 < 13$	$11 < 67$	$11 \mid 66$ (\ddagger)

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

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

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

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

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

Multiplying two such matrices gives

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

(arithmetic mod-7), showing the mult. is well-defined.

The inverse of $\begin{bmatrix} \alpha & x \\ 0 & 1 \end{bmatrix}$ is $\begin{bmatrix} \alpha^{-1} & -\alpha^{-1}x \\ 0 & 1 \end{bmatrix}$, so \mathcal{G} is a group, whose order is $\text{Ord}(\Omega) \cdot \text{Ord}(\mathbb{Z}_7) = 3 \cdot 7$.

Finally, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$, whereas in the other order, $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix}$. So \mathcal{G} is non-abelian. \square

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

First take $\alpha = 1$: Computing, $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^N = \begin{bmatrix} 1 & Nx \\ 0 & 1 \end{bmatrix}$. Hence $Nx \equiv 0$; so $N \equiv 0$ since $x \neq 0$. Thus

$$\text{Ord}\left(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\right) = 7,$$

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

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

$$\text{Ord}\left(\begin{bmatrix} \alpha \neq 1 & x \\ 0 & 1 \end{bmatrix}\right) = 3,$$

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

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}_∞ 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 $\{\mathbf{e}\}$. □

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

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

$$\text{H-Ord}_G(x) \bullet \text{K-Ord}_G(x) \bullet \text{Ord}_G(x). \quad \diamond$$

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

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

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

$$10': \quad \forall x \in G: \text{Ord}_{G/H}(xH) = \text{H-Ord}_G(x) \bullet \text{Ord}_G(x).$$

Dihedral groups

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

$$12: \quad V := \left\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \mid \begin{array}{l} \text{Each of } \{\mathbf{a}, \mathbf{b}, \mathbf{c}\} \text{ is an involution,} \\ \text{each pair commutes, and the prod-} \\ \text{uct of each two equals the third.} \end{array} \right\rangle.$$

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

$$12': \quad V = \langle \mathbf{a}, \mathbf{b} \mid \mathbf{a}^2 = \mathbf{e} = \mathbf{b}^2, \mathbf{a} \triangleleft \mathbf{b} \rangle.$$

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

$$13: \quad \begin{aligned} \mathbb{D}_N &:= \langle \mathbf{R}, \mathbf{F} \mid \mathbf{F}^2 = \mathbf{e}, \mathbf{FRFR} = \mathbf{e}, \mathbf{R}^N = \mathbf{e} \rangle; \\ \mathbb{D}_\infty &:= \langle \mathbf{R}, \mathbf{F} \mid \mathbf{F}^2 = \mathbf{e}, \mathbf{FRFR} = \mathbf{e} \rangle, \text{ for } N = \infty. \end{aligned}$$

Now for some straightforward facts.

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

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

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

$$*: \quad \mathbf{R}^j \mapsto J_{\mathbf{R}^j} \quad \text{and} \quad \mathbf{R}^j \mathbf{F} \mapsto J_{\mathbf{R}^j \mathbf{F}}. \quad \diamond$$

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

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

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

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

Misc. theorems

Temporarily here.

16: Lemma. For each $N \geq 2$, the full symmetric group \mathbb{S}_N is generated by an N -cycle $\nu := \langle b_0, b_1, b_2, \dots, b_{N-1} \rangle$ together with $\tau := \langle b_0, b_1 \rangle$; an “adjacent” 2-cycle. \blacklozenge

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 $\nu^{-1}\tau\nu = \langle b_1, b_2 \rangle$. Etc. \blacklozenge

17a: Cauchy's Thm for abelian groups (#9.5^P182). Suppose $N := |G| < \infty$ where G is an abelian group, written multiplicatively. If prime $p \mid N$, then there exists $y \in G$ with $\text{Ord}(y) = p$. \blacklozenge

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

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

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

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

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

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

A more standard proof uses induction on quotient groups.

Pf of (17a). WELoG $p := 5$. We may assume that

17b: If Q is a finite abelian group with $\text{Ord}(Q) \mid 5$, 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 $\text{Ord}_G(y) \mid 5$. [Why? Power $y^{\text{Ord}(y)/5}$ has order 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 $Q := \frac{G}{H}$, where $H := \langle h \rangle$. Automatically $H \triangleleft G$ since G is abelian. Finally, $h \neq \mathbf{e}$ so $|Q| < |G|$.

Since quotient Q is abelian, our (17b) 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 $\text{Ord}_G(y) \stackrel{\text{note}}{=} 5 \cdot \text{Ord}_H(y^5)$ is a multiple of 5. \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 (24), 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.

18: 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

19: E.g. [See file.] 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

Strengthening normality

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

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

$$20: \quad f: N \times \Gamma \rightarrow N\Gamma, \quad \text{by } (x, \omega) \mapsto x\omega,$$

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

21: 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 (20), the following are equivalent:

- i: $N \rightleftharpoons \Gamma$, 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 $N \rightleftharpoons \Gamma$. And this equals $f((xy, \alpha\beta))$. \diamond

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

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 $\llbracket x, \alpha \rrbracket = \mathbf{e}$. \diamond

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

$$22: \quad \text{Inn}(G) \subset \text{Aut}(G) \subset \text{SurEnd}(G) \subset \text{End}(G).$$

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

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

	WHICH HOMS?	THEN WRITTEN AS
	... $F \in \text{Inn}(G)$	$H \triangleleft G$
23:	... $F \in \text{Aut}(G)$	$H \stackrel{\text{Aut}}{\triangleleft} G$
	... $F \in \text{SurEnd}(G)$	$H \stackrel{\text{Sur}}{\triangleleft} G$
	... $F \in \text{End}(G)$	$H \stackrel{\text{End}}{\triangleleft} G$

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

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

$$26: \quad \mathcal{J}: G \rightarrow \text{Inn}(G) : x \mapsto J_x$$

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

$$27: \quad \text{Inn}(G) \cong \frac{G}{\mathcal{Z}(G)}.$$

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

$$26': \quad \mathcal{J}_H: \mathcal{N}G(H) \rightarrow \text{Aut}(H) : x \mapsto J_x \downarrow_H.$$

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

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

28: 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 $H \triangleleft G$. \blacklozenge

Remark. Index $|G:H| = 2$ need *not* imply the stronger $H \triangleleft^{\text{Aut}} G$. In the Vierergruppe, (12'), 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. [Conjugating, $J_R(\mathbf{F}) = \mathbf{RFR}^{-1} = \mathbf{R}^2\mathbf{F} \neq \mathbf{F}$.] [Also: The natural embedding of \mathbb{D}_4 has index-3 in \mathbb{S}_4 , yet is not a normal subgp.] \square

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

$$30: \quad [H \triangleleft^{\text{Aut}} G \triangleleft^{\text{Aut}} F] \implies H \triangleleft^{\text{Aut}} F.$$

$$31: \quad [H \triangleleft^{\text{Aut}} G \triangleleft F] \implies H \triangleleft F.$$

And $[H \triangleleft^{\text{End}} G \triangleleft^{\text{End}} F] \implies H \triangleleft^{\text{End}} F$. *Proof.* Use (24). \diamond

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

32: 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 $\mathcal{Z}(G) \triangleleft^{\text{Sur}} G$, but not necessarily $\triangleleft^{\text{End}}$.

iii: $\text{Inn}(G) \triangleleft \text{Aut}(G)$, but not necessarily $\triangleleft^{\text{Aut}}$. \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 $z \in \mathcal{Z}(G)$. To show $\hat{z} \in \mathcal{Z}(G)$, 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 $z \stackrel{\text{onto}}{\mapsto} \gamma$, 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 $\mathcal{Z}(G)$ *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

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

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). [See file.] 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 \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* $\mathbb{R}^{\mathfrak{D}\circ}$.

Proof. On $\mathbf{V} := \mathbb{R}^{\mathfrak{D}}$, 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

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

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

Proof. Let $G := \mathbb{D}_2 \times \mathbb{D}_4 \times \mathbb{D}_8 \times \mathbb{D}_{16} \times \dots$. By (15), group $\text{Inn}(G)$ equals

$$\begin{aligned} & \text{Inn}(\mathbb{D}_2) \times \text{Inn}(\mathbb{D}_4) \times \text{Inn}(\mathbb{D}_8) \times \text{Inn}(\mathbb{D}_{16}) \times \dots \\ & \cong \mathbb{1} \times \mathbb{D}_2 \times \mathbb{D}_4 \times \mathbb{D}_8 \times \dots, \end{aligned}$$

which is isomorphic to G . \blacklozenge

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

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 $f_M(y) := [M \cdot y]_{\text{mod } L}$.

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

34: Burnside's Lemma (#29.1^P474). *Counting cardinalities,*

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

Counting the number of G-orbits, then,

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

Proof. The number of G-orbits equals

$$\sum_{\omega \in \Omega} \frac{1}{|\mathcal{O}(\omega)|} \stackrel{\text{Orb-Stab, (7c*)}}{=} \frac{1}{|G|} \cdot \sum_{\omega \in \Omega} |\text{Stab}(\omega)|.$$

Now apply (34†) to earn (34‡). ♦

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

How many distinct colorings are there, up to orientation-preserving isometry? We will use Burnside's Lemma. The group, G , of orientation-preserving rotations of the cube has $6 \cdot 4 = 24$ elts, and is group-isomorphic to S_4 .

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

What isometry g ?	How many such g ?	$\# \text{Fix}(g) = 3^F$.	$F := \#$ [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

$$35a: \quad K^2 \cdot [K^4 + 3K^2 + 12K + 8] / 24. \quad \left[\begin{array}{l} \text{Coloring} \\ \text{faces} \end{array} \right]$$

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

What isometry g ?	$\#\{\text{such } g\}$	$\# \text{Fix}(g) = K^V$.	$V := \#$ [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

$$35b: \quad K^2 \cdot [K^6 + 17K^2 + 6] / 24. \quad \left[\begin{array}{l} \text{Coloring} \\ \text{vertices} \end{array} \right]$$

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

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

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

$$\frac{1}{24} \cdot [K^{12} + 6K^7 + 3K^6 + 8K^4 + 6K^3] \text{ i.e,}$$

$$35c: \quad K^3 \cdot [K^9 + 6K^4 + 3K^3 + 8K + 6] / 24. \quad \left[\begin{array}{l} \text{Coloring} \\ \text{edges} \end{array} \right]$$

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

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

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

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

since $[1 - K]$ is even. □

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

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

Unfinished: as of 1Feb2022 [The formulas are correct, but there is not much explanation.]

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

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

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

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

$$\begin{aligned} \text{Flips}_N &= N \cdot K^{H+1}. \quad \text{Thus} \\ \mathcal{B}_N(K) &= \frac{1}{2} \mathcal{L}_N(K) + \frac{1}{2} K^{H+1}. \end{aligned}$$

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

$$\begin{aligned} \text{Flips}_N &= H \cdot [K^H + K^{H+1}] = H \cdot K^H [1 + K]. \quad \text{Thus} \\ \mathcal{B}_N(K) &= \frac{1}{2} \mathcal{L}_N(K) + \frac{1}{4} K^H [1 + K]. \end{aligned}$$

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 $|\Omega| = \sum_{O \in S} |O|$ leads to a useful formula, when we consider G acting on itself via conjugation.

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

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

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

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

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

Ex: 3x3 TTT. The TTT-aut group of $\Omega := [1..3] \times [1..3]$ is \mathbb{D}_4 . And $\text{UnivFix}(\mathbb{D}_4)$ is singleton $\{(2, 2)\}$, since only the center-cell $(2, 2)$ of the 3x3 board is unmoved by each automorphism. □

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

$$\text{NT-Reps} := \text{All-Reps} \setminus \text{UnivFix}(G);$$

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

$$36: \quad |\Omega| = |\text{UnivFix}(G)| + \sum_{\omega \in \text{NT-Reps}} \frac{|G|}{|\text{Stab}_G(\omega)|}.$$

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

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

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

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 $h \in \mathcal{Z}(G)$, where $\mathcal{Z}(G) := \bigcap_{h \in G} \mathcal{C}(h)$ is the *center* of G . Below, let “ $h \in \text{All-CC}$ ” mean to take one representative h per \mathbb{C} . Let **NT-CC** comprise one representative per **Non-Trivial CC**.

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

$$37': \quad |G| = |\mathcal{Z}(G)| + \sum_{h \in \text{NT-CC}} \frac{|G|}{|\mathcal{C}(h)|}.$$

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

$$|G| = \sum_{h \in \text{All-CC}} \frac{|G|}{|\mathcal{C}(h)|}. \quad \square$$

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

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

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

Proof. The centralizer of each $h \in \text{NT-CC}(G)$ is a proper subgroup, so p divides $|G|/|\mathcal{C}(h)|$. Hence p divides the sum on RhS(37'). So p divides $|\mathcal{Z}(G)|$. ◇

39: Cauchy’s Thm for finite groups (After#24.3^P391). Suppose $N := |G| < \infty$. If prime $p \nmid N$, then there exists $y \in G$ with $\text{Ord}(y) = p$. ◇

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

If $p \nmid \text{Ord}(Q)$ 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 **NT-CC**(G), has order not a multiple of p . Thus p divides the RhS(37') sum. So $p \nmid \text{Ord}(\mathcal{Z}(G))$.

We may now apply (17a), 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 (17b) uses induction on quotient groups, but does not use the Class-Eqn, whereas p -group non-trivial center (38) uses the class equation but no induction. The above Cauchy’s thm (39), used quotient-induction to put the class equation in play.

A jazzed-up (39) argument will give Sylow’s first theorem. □

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

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

We now show that this holds universally. \square

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

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 $\text{Ord}(G) \bullet p^K$ and

41: $P(K-1, *)$ 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 $\text{NT-CC}(G)$. Thus p divides the \sum -sum in (37'). 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 (41), 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.

42: 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 $y_1 \rightleftharpoons y_2$. Then G is abelian. \diamond

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

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

And this equals $x_2 x_1$. \blacklozenge

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

43: G/Z Lemma. We have a subgroup $H \subset \mathcal{Z}(G)$; necessarily $H \triangleleft G$. If G/H is cyclic, then G is abelian. \diamond

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

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

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 $\{\mathbf{F}, \mathbf{FR}^2\}$ 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

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

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

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

Since $a \rightleftharpoons c$,

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

Were $\text{Ord}(y) \bullet p$, then $\mathbf{e} = [ac]^p = c^p$, 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

Sylow Theorems

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

Normal subgroups

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

45: 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, $\overline{N-3}1$. \square

46: 3-cycle Lemma. The solo 3-cycles generate \mathbb{A}_N . \diamond

Proof.

47: 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.

§A Appendix: (Semi)group Axioms

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

Axiomatically:

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

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

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

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

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

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

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

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

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

R2: Triple $(\Gamma, +, 0)$ 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 $\alpha \blacklozenge \beta$ [α *divides* β] if *there exists* $\mu \in \Gamma$ s.t $\alpha\mu = \beta$. This is the same relation as $\beta \blacklozenge \alpha$ [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

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

[E.g: In the \mathbb{Z}_{15} ring, note $9 \neq 0$ and $10 \neq 0$, 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, $\text{ZD}_\Gamma = \{0\}$] is called an *integral domain* (*intDomain*), or sometimes just a *domain*.

An intDomain F in which every non-zero element is a unit [i.e $\mathbf{U}(F) = F \setminus \{0\}$] is a *field*. That is to say, F is a commRing where triple $(F \setminus \{0\}, \cdot, 1)$ 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 $\{\pm 2, \pm 3, \pm 4, 6\}$.

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

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 , written as u^{-1} , is called the **reciprocal** [or **multiplicative-inverse**] of u . [When an elt has a mult-inverse, this mult-inverse is unique.]

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

Exer 1b: If $\gamma \mid z$ with $z \in \text{ZD}$, then γ is a zero-divisor.

Exer 2: In an arbitrary ring Γ , the set $\text{ZD}(\Gamma)$ is *disjoint* from $\text{Units}(\Gamma)$.

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 $p \mid [c \cdot d]$ then *either* $p \mid c$ or $p \mid d$.

Associates. In a commutative ring, els 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 $\alpha \mid \beta$ and $\alpha \nmid \beta$ [i.e, $\alpha \in \beta\Gamma$ and $\beta \in \alpha\Gamma$].

Ex 3: Prove **Assoc** \Rightarrow **weak-Assoc**.

Ex 4: If $\alpha \sim \beta$ and $\alpha \notin \text{ZD}$, 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 $d \mid \alpha$, prove: *If α is a non-ZD, then d is a non-ZD.* And: *If α is a unit, then d is a unit.*

48: Lemma. In a commRing Γ , each prime α is irreducible. \diamond

Proof. Consider factorization $\alpha = xy$. Since $\alpha \mid xy$, WLOG $\alpha \mid x$, i.e $\exists c$ with $\alpha c = x$. Hence

$$*: \quad \alpha = xy = \alpha cy.$$

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

There are rings^{♥3} with irreducible elements p which are nonetheless not prime. However...

^{♥3}Consider the ring, Γ , of polys with coefficients in \mathbb{Z}_{12} . There, $x^2 - 1$ factors as $[x - 5][x + 5]$ and as $[x - 1][x + 1]$.

49: Lemma. Suppose commRing Γ satisfies the Bézout condition, that each GCD is a linear-combination. Then each irreducible α is prime. \diamond

Pf. Suppose $\alpha \mid c \cdot d$. WLOG $\alpha \nmid c$. Let $g := \text{GCD}(\alpha, c)$. Were $g \approx \alpha$, then $\alpha \mid g \mid c$, a contradiction. Thus, since α is irreducible, our $g \approx 1$.

Bézout produces $S, T \in \Gamma$ with

$$1 = S\alpha + Tc. \text{ Hence}$$

$$*: \quad d = S\alpha d + Tcd = Sd\alpha + Tcd.$$

By hyp, $\alpha \mid cd$, hence α divides RhS(*). So $\alpha \mid d$. \diamond

50: Lemma. In commRing Γ , if prime p divides a project $\alpha_1 \cdots \alpha_K$ then $p \mid \alpha_j$ for some j . [Exer. 7] \diamond

51: 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 $p_k \approx q_k$. \diamond

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 $q_L \mid p_K$. 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. \diamond

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** \nRightarrow **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 $t \geq 0$:

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

And for $t \leq 0$ define

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

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

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

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 $[-2, 2] \setminus \{0\}$. Cty of g then forces $g \equiv \mathbf{0}$.]

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

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

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

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

Inverses

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

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

52: 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. \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

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).] \diamond

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

53: 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 [wrt \mathbf{e}] righthand inverse, y' . Then:

53a: If $y \times y = y$, then $y = \mathbf{e}$.

Moreover:

53b: 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 (53a). 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 $y = y \times y' \stackrel{\text{note}}{=} \mathbf{e}$. \diamond

Pf of (53b). First let's show that every RInv, y' , of y , is also a LInv of y . Let $b := [y' \times y]$. Courtesy (53a), it is enough to show that $b \times b = b$. And

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

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 LHInverse. I.e, $\mathbf{e} \times y = y$. \blacklozenge

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

§B Appendix: Miscellaneous results

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

54: Min-prime normality lemma. Consider finite groups $G \supset H$ with index $p := |G:H|$ prime. Moreover, p is the smallest prime dividing $|G|$. Then $H \triangleleft G$. \diamond

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

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

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

§Index for Group Notes

$\Phi_N, \varphi(N)$, **18**
 \triangleleft , *see* Group binrel, normal
 \perp , *see* Group binrel, transverse

alternating group, **1**
 annihilator, **18**
 associates, **19**
 associative, **18**
 automorphism, **1**

center, **2**
 center of a group, $\mathcal{Z}(G)$, **15**
 centralizer, **2**
 class equation, **15**
 commutative, **18**
 conjugacy class, **15**
 conjugate an element, **1**
 conjugation map, **10**

dihedral group, **7**
 distributes-over, **18**

endomorphism, **1**

field, **18**
 fixed-point, **4**

Gaussian integers, **18**

Group, **18**
 p -group, **17**
acting on a set, **4**
 alternating, **1**
 dihedral, **7**
 Klein-4, **7**
 of units, **18**
 stabilizer, **4**

Group binrel
 normal, \triangleleft , **9**
 transverse, \perp , **10**

Grouply unique, **5**

homomorphism, **1**

identity element, **18**
 inner automorphism, **1**, **10**
 integral domain, **18**
 inverse element, **18**
 irreducible element, **19**
 isomorphism, **1**

Klein-4, *see* Group

monoid, **18**

normalizer, **2**

orbit, **4**

p -group, *see* Group, p -group
 prime element, **19**

ring, **18**
 annihilator, **18**
 domain, **18**
 zero-divisor, **18**

semigroup, **18**
 stabilizer, *see* Group

token, **4**
 torsion, *see* Group, torsion
 transverse groups, \perp , **10**

unit, **18**, **19**
 $\mathbf{U}(N)$, **18**
 \mathbf{U}_Γ , **18**

Vierergruppe, *see* Group, Klein-4

ZD, *i.e.*: zero-divisor
 zero-divisor, **18**, **19**