

Solns to HW problems from Gallian

Jonathan L.F. King
 University of Florida, Gainesville FL 32611-2082, USA
 squash@ufl.edu
 Webpage <http://squash.1gainesville.com/>
 20 July, 2016 (at 09:07)

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

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

Use Cyc_N , \mathbb{S}_N , \mathbb{D}_N for the N^{th} *cyclic*, *symmetric* and *dihedral* groups. So $|Cyc_N|=N$ 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 $(\text{Aut}(G), \circ, Id)$.

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

1: All Involution Lemma. *If every element of (G, \cdot, \mathbf{e}) is an involution, then G is abelian.* \diamond

Pf. Fix $a, b \in G$. So $\mathbf{e} = [ab]^2 = aba^{-1}b^{-1} = \llbracket a, b \rrbracket$. \blacklozenge

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 $\langle x \rangle_G = \langle y \rangle_G$.

2: 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. \blacklozenge

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,

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

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

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

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

5: Lemma. *Suppose that $f: (G, \mathbf{e}) \rightarrow (\Gamma, \boldsymbol{\varepsilon})$ is a group-homomorphism. Then TFAEivalent:*

*i: $\text{Ker}(f)$ is **trivial**, i.e, is $\{\mathbf{e}\}$.*

ii: f is injective.

iii: When $\text{Ord}(G) = \text{Ord}(\Gamma) < \infty$: f is surjective. \blacklozenge

#37^P53. Let $J := \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$. Note $J^2 = 2J$. Hence

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} c & \\ & c \end{bmatrix} = aJ \cdot cJ = ac \cdot J^2 = 2ac \cdot J.$$

So we can think of G as $\mathbb{R} \setminus \{0\}$ and equipped with multiplication $a \odot c := 2ac$. Let $\mathbb{R}^\circ := \mathbb{R} \setminus \{0\}$. Note that $\frac{1}{2}$ is a neutral elt for \odot , since $\frac{1}{2} \odot c = 2 \cdot \frac{1}{2}c = c$. We will show that

$$(\mathbb{R}^\circ, \odot, \frac{1}{2}) \cong (\mathbb{R}^\circ, \cdot, 1).$$

Indeed, the bijection $f: \mathbb{R}^\circ \rightarrow \mathbb{R}^\circ$ by $x \mapsto 2x$, is a group-isomorphism. After all

$$f^{-1}(f(a) \cdot f(c)) = \frac{1}{2} \cdot [2a \cdot 2c] = 2ac = a \odot c.$$

◆

#28^P67. In $G := \text{SL}_2(\mathbb{R})$, matrices $A := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B := \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$, have orders 4 and 3, resp.. Their product $AB \stackrel{\text{note}}{=} \begin{bmatrix} 1 & \\ 0 & 1 \end{bmatrix}$ is a nt-shear, hence has ∞ -order. ◆

#7^P82. The Klein-4 group, $\mathbb{Z}_2 \times \mathbb{Z}_2$, has all proper subgps being cyclic.

[Prove or give CEX: Dihedral group \mathbb{D}_N has all proper subgroups cyclic IFF $N=2$ or N is odd.] ◆

#14^P82. $G \cong (\mathbb{Z}_{49}, +)$. See #34^P90. ◆

#16^P82. Note $240 = 2^4 \cdot 3^1 \cdot 5^1$. Writing additively,

$$\begin{aligned} \langle 0 \rangle &= \langle 240 \rangle \subset \langle \frac{240}{5} \rangle \subset \langle \frac{240}{5 \cdot 3} \rangle \subset \langle \frac{240}{5 \cdot 3 \cdot 2} \rangle \\ &\subset \langle \frac{240}{5 \cdot 3 \cdot 2^2} \rangle \subset \dots \subset \langle \frac{240}{5 \cdot 3 \cdot 2^4} \rangle = \langle 1 \rangle. \end{aligned}$$

This is a length-seven chain. ◆

#51^P82. Suppose $a^2 = \mathbf{e} = b^2$, yet $a \neq b$ and neither one is \mathbf{e} . We'll prove that at least one of

$$x := aba \quad \text{and} \quad y := ab$$

is an involution that is not in $\{\mathbf{e}, a, b\}$.

Firstly, $x^2 = aba^2ba = abba = \mathbf{e}$. Now

$$\begin{aligned} 6: \quad [x = \mathbf{e}] &\Rightarrow [ab = a^{-1} = a] \Rightarrow [b = \mathbf{e}]. \quad \times \\ [x = a] &\Rightarrow [ab = \mathbf{e}] \Rightarrow [a = b^{-1} = b]. \quad \times \end{aligned}$$

If $x \neq b$, then x is our desired involution. So WLOG $\boxed{x = b}$. Thus $\mathbf{e} = aba \cdot b^{-1} = [ab]^2$, and so y is an involution. Could $y \in \{\mathbf{e}, a, b\}$? No, since:

$$\begin{aligned} [y = \mathbf{e}] &\Rightarrow [b = a^{-1} = a]. \quad \times \\ [y = a] &\Rightarrow [b = \mathbf{e}]. \quad \times \end{aligned}$$

And $[y = b] \Rightarrow [a = \mathbf{e}]$; contradiction. ◆

#61^P82. Let G be the cyclic gp of order $[p^N] - 1$; necessarily $N \geq 1$, so

$$*: \quad p \perp \text{Ord}(G).$$

Our goal is to show that $x \mapsto x^p$ maps onto all of G . Since G is finite, this is equiv to showing that $x \mapsto x^p$ is injective.

Suppose some $a^p = b^p$. Since G is abelian, then, $[ab^{-1}]^p = \mathbf{e}$. So the order of ab^{-1} is either p or 1. It can not be p , by (*). Hence $ab^{-1} = \mathbf{e}$, i.e, $a = b$. ◆

#64^P82. Fix $z \in Z(G) \setminus \{\mathbf{e}\}$; so $p := \text{Ord}(z)$ is prime. FTSOC, suppose $\exists x \in G$ st. $q := \text{Ord}(x)$ is a different prime. Since $z \triangleleft x$,

$$[zx]^{pq} = [z^p]^q \cdot [x^q]^p = \mathbf{e}.$$

Thus $N := \text{Ord}(zx)$ is a divisor of pq . Yet $N \neq 1$, since $\text{Ord}(z) \neq \text{Ord}(x)$. And $N \neq p$, since $[zx]^p = x^p \neq \mathbf{e}$. Ditto $N \neq q$. Thus $N = pq$, which is composite. ◆

#7^P90. In $\mathbb{S}_{\{0,1,2\}}$, let $a := (12)$ and $b := (012)$ and $c := (02)$. Now $a \triangleright b \triangleright c = (012)$. OTOHand, $c \triangleright b \triangleright a$ is the identity permutation. ◆

#8^P90. Goal: $\exists x: \boxed{\dagger: xax = b}$ IFF $\exists y: \boxed{\ddagger: y^2 = ab}$.

Well, (\dagger) implies a common value

$$ax = x^{-1}b =: y.$$

So $y^2 = ax \cdot x^{-1}b = ab$.

Conversely, let $x := by^{-1}$. Inexorably,

$$ax = a \cdot by^{-1} \stackrel{\text{by } (\ddagger)}{=} y^2 \cdot y^{-1} = y.$$

So $x \cdot ax = by^{-1} \cdot y = b$, which is what (\dagger) requested. ◆

#9^P90. We'll show that this a commutes with an arbitrary $g \in G$. Let $\gamma := gag^{-1}$. Squaring,

$$\gamma^2 = ga^2g^{-1} = gg^{-1} = \mathbf{e}.$$

Could $\gamma = \mathbf{e}$? If yes, then $ga = g$, so $a = \mathbf{e}$; \times .

Thus $\gamma \neq \mathbf{e}$, whence $\text{Ord}(\gamma) = 2$. By the uniqueness hyp., γ must be a . In other words, $a \trianglelefteq g$. \blacklozenge

#17^P90. FTSOContradiction, suppose we have proper subgps $H_0 \cup H_1 = G$. Since they are proper, there exist elements $a_i \in H_i \setminus H_{1-i}$. Now

$$b := a_0a_1 \in G = H_0 \cup H_1;$$

WLOG $b \in H_0$. Thus $H_0 \ni a_0^{-1} \cdot b \stackrel{\text{note}}{=} a_1$. \times

In contrast, the Klein-4 group is a union of three proper subgroups. \blacklozenge

#20^P90. Squaring $\boxed{*: x^2 = xyx^{-1}}$ gives

$$x^4 = yx^2y^{-1} \stackrel{\text{by } (*)}{=} y[xyx^{-1}]y^{-1} = y^2xy^{-2}.$$

Since y is an involution, $x^4 = x$. Thus $\text{Ord}(x)$ equals 1 or 3. And $x \neq \mathbf{e}$. So $\text{Ord}(x) = 3$. \blacklozenge

#23^P90. Conjugating, $xy = y[xy]y^{-1} = yx$. \blacklozenge

#29^P90. For each $b \in S$, write its forward-orbit as $\widehat{b} := \{b, b^2, b^3, \dots\}$.

Existence of 2-sided id in \widehat{b} . Since \widehat{b} is finite, \exists posints j, K with $b^{j+K} = b^j$. If $j = 1$, then $(*)$, below. Else, left-cancel b^{j-1} from each side, to conclude that

$$*: b^{1+K} = b.$$

Let $\mathbf{e} := \mathbf{e}_b := b^K$. So for an arbitrary $c \in S$,

$$bec = bc.$$

By left-cancellation, then, $\mathbf{e}c = c$. So \mathbf{e} is a universal left-identity. Using right-cancellation similarly shows that \mathbf{e} is a universal right-identity.

Uniqueness of identity elt. Each $c \in G$ yields a 2-sided identity \mathbf{e}_c . But $\mathbf{e}_b = \mathbf{e}_c\mathbf{e}_b = \mathbf{e}_c$.

Existence of inverses. Consider the b and K from $(*)$. We have that

$$\mathbf{e} \stackrel{\text{def}}{=} b^K = b^{K-1} \cdot b = b \cdot b^{K-1},$$

so b^{K-1} is a 2-sided inverse to b . **Wait!** Expression ' b^{K-1} ' is well-defined for $K \geq 2$, but what about the $K=1$ case? We're ok, because the above work now makes $b^0 := b^K \stackrel{\text{def}}{=} \mathbf{e}$ well-defined. (Whew!) \blacklozenge

#34^P90. Note that $G^\circ := G \setminus \{\mathbf{e}\}$ is not empty. Could an element $u \in G^\circ$ have ∞ -order?; no, since then $\langle u^2 \rangle_G$ and $\langle u^3 \rangle_G$ would be distinct non-trivial subgroups. Hence: **Every element of G has finite order.** (I.e, G is a *torsion group*.)

Take an $x \in G^\circ$ of minimum order. So $G \not\supseteq \langle x \rangle$, and thus $p := \text{Ord}(x)$ is prime, since $\langle x \rangle$ can have no nt-subgps.

Take any $y \in G^\circ \setminus \langle x \rangle$. Nec., $\langle y \rangle$ is a nt-subgp, hence includes $\langle x \rangle$. This inclusion must be proper, since $y \notin \langle x \rangle$. Thus $\langle y \rangle = G$, as G has only one nt-subgp. So G is cyclic of order $N := \text{Ord}(y)$.

Automatically, $p \nmid N$ properly. Hence $\langle y^{N/p} \rangle$ is a nt-subgp of G . Thus it must equal $\langle x \rangle$. In particular, $\frac{N}{p} = p$. I.e, G is cyclic of order p^2 . \blacklozenge

#35^P90. [Aside: Our goal, if G has ≤ 2 nt-subgps, is to show that G is cyclic, and... Note that the (abelian) Klein-4 gp has three nt-subgps. And the non-abelian S_3 has four nt-subgps.]

[*Ques Q1:* Is the Klein-4 group, the *only* non-cyclic group with ≤ 3 non-trivial proper subgps?]

As in **#34^P90**, G must be a torsion group.

Pick an $x \in G^\circ := G \setminus \{\mathbf{e}\}$ of minimum-order. So $X := \langle x \rangle$ is cyclic, and $p := |X|$ is prime. Hence $\exists y \in G \setminus X$. And $Y := \langle y \rangle$ is cyclic.

CASE: $\exists u \in X \cap Y$ with $u \neq \mathbf{e}$. Now $\{\mathbf{e}\} \subsetneq \langle u \rangle \subset X$, so min-order implies $\langle u \rangle = X$. Hence $Y \supseteq X$. Thus $\text{Ord}(Y) = qp$, for some posint q .

Now $\text{Ord}(y^p) = q < qp = \text{Ord}(y)$. But y has *minimum* order in $G \setminus X$. Thus $y^p \in X$. So $\text{Ord}(y^p)$ divides p , i.e, $q \nmid p$. Thus $q = p$ (since $q \geq 2$ and p is prime). So subgp $Y = \langle y \rangle$ is cyclic of order p^2 .

Seeing as Y has only one nt-subgp, $\exists z \in G \setminus Y$. Since X and Y are nt-subgps of G , necessarily $\langle z \rangle$ is not, and therefore $\langle z \rangle = G$. So G is cyclic, with order $\text{OTForm } r \cdot p^2$. *Every $\widehat{z} \in G \setminus Y$ must generate G , so*

r has to be prime. But $\langle z^r \rangle$ will be a *new* nt-subgp, unless $r = p$. The upshot: G is cyclic of order p^3 .

CASE: $X \cap Y = \{e\}$.

Now $x \in X \setminus Y$ and $y \in Y \setminus X$, so the product $z := xy$ can be in *neither* X nor Y . I.e, $z \in G \setminus [X \cup Y]$. Thus $\langle z \rangle$ is all of G , since X, Y are nt-subgps. Unsurprisingly, G is cyclic.

Let $q := \text{Ord}(y)$. Since Y and X exhaust all the non-trivial G -subgps, this Y can have no nt-subgp (since $X \not\subseteq Y$). Thus q is prime.

Note that $z^p = x^p y^p$, since G is abelian. Were $q=p$, then $z^p = e$, so $\#G \leq p$. This contradicts that X is a *proper* subgp of G . Thus $q \neq p$.

The result: G is cyclic of order qp . ◆

#37^P90. Strengthening, we just need that S be equipped with an associative binary op; i.e S is a semigroup. We are given a partitioning $S = T \sqcup U$ of S .

FTSOC, suppose that neither T nor U is sealed under multiplication. So $\exists a, b \in T$ st.

$$x := a \cdot b \in S \setminus T \stackrel{\text{note}}{=} U.$$

Similarly, $\exists y, z \in U$ with $c := y \cdot z \in T$.

Multiplying gives an element

$$abc = xyz$$

which is simultaneously in T and U ; *contradiction*, since each is sealed under triple-products. ◆

#39^P90. Let $G := (\mathbb{Q}, +)$ let $H_n := \langle 1/2^n \rangle_G$, i.e $H_n = \{ \frac{k}{2^n} \mid k \in \mathbb{Z} \}$. So $\dots H_{-1} \subsetneq H_0 \subsetneq H_1 \subsetneq H_2 \dots$ ◆

#40^P90. Given: $a^{-1}ba = b^2$. For N a natnum,

$$a^{-1}b^N a = [a^{-1}ba]^N = [b^2]^N = b^{2^N}.$$

So by induction on ℓ : For $\ell = 0, 1, 2, \dots$

$$a^{-\ell} b a^\ell = b^{[2^\ell]}.$$

Let $K := \text{Ord}(a) < \infty$. Then $b = a^{-K} b a^K = b^{2^K}$, so

$$\text{Ord}(b) \blacklozenge [2^K - 1].$$

E.g, if $\text{Ord}(a) = 3$ then $\text{Ord}(b) \blacklozenge 7$. By hypothesis, $b \neq e$. So $\text{Ord}(b) = 7$. Similarly, if $\text{Ord}(a) = 5$ then $\text{Ord}(b) = 32 - 1 = 31$, since 31 is prime. ◆

#42^P90. Given $H := \{h \in G \mid \text{Ord}(H) \perp 3\}$. I take this to imply that each $h \in H$ has finite order. (Of course, $\#H$ could be infinite.) Evidently, $H \ni e$ and $[H \ni h \Rightarrow H \ni h^{-1}]$. Suppose we could show that

$$\dagger: \quad \forall g, h \in H: \quad g \trianglelefteq h.$$

Consequently, $\text{Ord}(gh)$ divides $\text{Lcm}(\text{Ord}(g), \text{Ord}(h))$. Thus $\text{Ord}(gh) \perp 3$. So H would be shown sealed under multiplication.

To prove (\dagger) , ISTEEstablish that each element

$$\ddagger: \quad f \in H \text{ has a cube-root.}$$

With $F := \langle f \rangle_G$ the generated cyclic subgroup, let $N := \#F$. The map $F \rightarrow F$ by $x \mapsto x^3$ is necessarily *injective*, since $3 \perp N$. Consequently, this map is *surjective*, since $\#F$ is finite. Hence (\ddagger) . ◆

(The argument works with “3” replaced by any posint.)

#43^P90. The set $S^{-1} := \{t^{-1} \mid t \in S\}$ has more than half the elements of G ; hence so does $x \cdot S^{-1}$. So $S \cap xS^{-1}$ is non-void. We can thus pick an element

$$s \in S \cap xS^{-1}.$$

So there is a elt $t \in S$ st. $s = xt^{-1}$. Thus $s \cdot t = x$. ◆

#10^P112. In \mathbb{S}_N : A perm π yields cycle-lengths $\ell_1 \geq \ell_2 \geq \dots \geq \ell_K$. And $\text{Ord}(\pi) = \text{Lcm}(\ell_1, \dots, \ell_N)$. Thus

$$7: \quad \text{Maximum}_{\ell_1 + \dots + \ell_K = N} \text{Lcm}(\ell_1, \dots, \ell_K)$$

is the $\text{MaxOrd}(\mathbb{S}_N) =: f(N)$. This $f()$ is called **Landau’s function**.

Note that $g(N) := \text{MaxOrd}(\mathbb{A}_N)$ equals (7), *but* with tuple (ℓ_1, \dots, ℓ_K) only ranging over those tuples with *evenly many* even lengths ℓ_k . In particular,

$$f(10) = \text{Lcm}(5, 3, 2) = 30.$$

$$g(10) = \text{Lcm}(7, 3) = 21.$$

◆

#50^P112. I’ll use ‘T’ for the 10-card. In cycle-notation, the given permutation and its square-root are

$$\sigma^2 := \langle \text{A T J 6 3 Q 2 9 5 K 7 4 8} \rangle$$

$$\sigma = \langle \text{A 9 T 5 J K 6 7 3 4 Q 8 2} \rangle.$$

After all, σ^2 is a solo odd-cycle and so has a unique sqroot. Finally to see the order that the cards came out of the shuffler, after the first pass,

A	2	3	4	5	6	7	8	9	T	J	Q	K
9	A	4	Q	J	7	3	2	T	5	K	8	6

we have put σ into two-line notation. ◆

#46^P286. Suppose $f:\mathbb{R}\circlearrowleft$ is a ring-auto. Evidently $f(0) = 0$ and $f(1) = 1$. Easily $f|_{\mathbb{Z}} = Id$. Thus $f|_{\mathbb{Q}} = Id$. Since \mathbb{Q} is dense w.r.t “ \leq ”, ISTShow that f respects “ \leq ”. Since $f(c) - f(b)$ equals $f(b - c)$ we need but show that f respects non-negativity.

Lastly, a real is non-negative IFF it has a real square-root. ◆

#35^P132. Rename conjugation to $J_a(x) := axa^{-1}$. To show divisibility, WLOG $N := \text{Ord}_G(a)$ is finite. And note that the composition $[J_a]^{\circ N}$ equals J_{a^N} , which is Id . Hence $\text{Ord}(J_a)$ divides N .

As for the example, let \mathbf{f} be a flip in the dihedral group \mathbb{D}_3 . Fix a $K \in [3.. \infty]$, and let C be the cyclic group of order- K , with $c \in C$ a generator. So $a := (\mathbf{f}, c)$ is in the cartesian product

$$G := \mathbb{D}_3 \times C.$$

This C is abelian, so $\text{Ord}(J_a) = \text{Ord}_{\mathbb{D}_3}(\mathbf{f}) = 2$.

On the other hand, since C is cyclic, $\text{Ord}_G(a) = \text{Lcm}(2, K)$, which certainly exceeds 2. ◆

#37^P132. Well $|\mathbb{R}_+| \neq |\mathbb{Q}|$, so there is not a bijection. Let’s, instead, show that $H := (\mathbb{Q}_+, \cdot)$ is *not* gp-isomorphic to $\tilde{H} := (\mathbb{Q}, +)$; indeed, there isn’t even an injective homomorphism.

FTSOC, let $x \mapsto \tilde{x}$ be an injective-hom $H \hookrightarrow \tilde{H}$. Thus $\frac{a}{b} := \tilde{2}$ and $\frac{x}{y} := \tilde{3}$ are two non-zero elts of \tilde{H} . Evidently $by \cdot \tilde{2} = ax \cdot \tilde{3}$. Pulling this back over the *injective* hom, tells us that $\boxed{2^{by} = 3^{ax}}$. But this violates the FTArithmetic, since each of b, y, a, x is a non-zero integer. ◆

#41^P132. Let $G := (\mathbb{Q}_+, \cdot)$. The problem is equivalent to finding an non-surjective, yet injective, group-endomorphism $f:G \hookrightarrow G$. For then f realizes an isomorphism of G onto $\text{Range}(f)$.

Our G is commutative, so $x \mapsto x^3$ is a group-endomorphism. The only rational cube-root of 1 is 1; i.e “ $\text{Ker}(f)$ is trivial”, i.e f is injective. And f is *not* onto, since $2 \notin \text{Range}(f)$. (Aside: The same argument and f work when G is $\mathbb{Q}_+ \sqcup \mathbb{Q}_-$). ◆

#42^P132. Let $H := (\mathbb{Q}, +)$. It will certainly suffice (see **#41^P132**) to show that every non-trivial endomorphism $f:H \circlearrowleft$ is surjective. Letting $\mathbf{q} := f(1)$, then, ISTShow that

$$\text{PROP}(x): \quad f(x) = \mathbf{q} \cdot x,$$

holds for every $x \in \mathbb{Q}$. Since f respects negation, our goal is $\text{PROP}(x)$ for each $x \in \mathbb{Q}_+$.

Fix a posint D and note that

$$\begin{aligned} D \cdot f\left(\frac{1}{D}\right) &= f\left(\frac{1}{D}\right) + f\left(\frac{1}{D}\right) + \cdots + f\left(\frac{1}{D}\right) \\ &= f\left(\frac{1}{D} + \cdots + \frac{1}{D}\right) = f(1) = \mathbf{q}. \end{aligned}$$

Dividing gives $f\left(\frac{1}{D}\right) = \mathbf{q} \cdot \frac{1}{D}$, i.e $\text{PROP}\left(\frac{1}{D}\right)$. Adding N copies together gives $\text{PROP}(N/D)$, as needed.

As a corollary, we have that

$$8: \quad (\text{End}(H), \circ, Id) \cong (\mathbb{Q}, \cdot, 1).$$

◆

#43^P132. With $G := \mathbb{R}_+ \sqcup \mathbb{R}_-$, our group is $(G, \cdot, 1)$. Evidently a point $x \in \mathbb{R}_+$ IFF $\exists y \in G$ with $y^2 = x$. This property is preserved under gp-automorphism. ◆

Notation. In the exercises below, let

$$\begin{aligned} \text{HasOrd}_G(d) &:= \{x \in G \mid \text{Ord}_G(x) = d\} \quad \text{and} \\ \text{Ords}(G) &:= \{\text{Ord}_G(x) \mid x \in G\}. \end{aligned}$$

With G implicit, I’ll typically use T_d for the cardinality $|\text{HasOrd}(d)|$. Letting $N := \text{Ord}(G)$, recall that

- For each posint d , necessarily $T_d \mid \varphi(d)$.
 And if $d \nmid N$, then $T_d = 0$.
 9: Further, when $T_d \neq 0$ then $T_\delta \neq 0$, for each posint divisor $\delta \mid d$.

When $N := |G| < \infty$, we always have that

$$10: \quad \sum_{d \mid N} T_d = N.$$

#10^P148. WLOG neither a nor b has order 155. Since $155 = 5 \cdot 31$, both prime, WLOG $\text{Ord}(a) = 5$ and $\text{Ord}(b) = 31$. Applying Lagrange to $H := \langle a, b \rangle$ gives $\#H \mid 5$ and $\#H \mid 31$. Thus $\#H \mid \text{Lcm}(5, 31)$. So H is all of G . \blacklozenge

11: Lemma. Suppose $N := |G|$ is odd. Then the only fixed-point of $x \mapsto x^{-1}$ is e . \blacklozenge

Pf. FTSOC, suppose there is a fixed-pt $p \neq e$. Then $H := \langle p \rangle$ has order 2. But $2 \nmid N$, contradicting Lagrange. \blacklozenge

#21^P148. Let $p := \prod_{x \in G} x$; this is well-defined since G is abelian and finite. Because H is a bijection

$$p^{-1} = \prod_{x \in G} x^{-1} \stackrel{\text{note}}{=} p,$$

since G is abelian. So p equals e . \blacklozenge

#23^P148. We have $|G| = pq$. FTSOC, suppose $T_{pq} = 0$. By the uniqueness hypothesis,

$$T_p = \varphi(p) = p-1, \quad \text{and} \quad T_q = q-1.$$

CASE: $p \neq q$ WLOG $p < q$. Note that $\#G$ equals

$$T_1 + T_p + T_q = 1 + [p-1] + [q-1] = q + [p-1].$$

And $q \mid \#G$, so q must divide $[p-1]$. \otimes

CASE: $p = q$ Here $\#G = T_1 + T_p \stackrel{\text{note}}{=} p$. So $p^2 = p$. This implies that $p = 1$, which, alas, is not prime. \blacklozenge

#25^P148. We have $T_1 + T_{11} + T_3 + T_{33} = 33$. FTSOC, suppose $T_3 = 0$; thus $T_{33} = 0$. So $T_{11} = 33 - T_1 = 32$. Thus $32 \mid \varphi(11) \stackrel{\text{note}}{=} 10$. \otimes \blacklozenge

#28^P148. [Show $(\mathbb{Q}, +)$ has no proper subgp G of finite index.] FTSOC, consider an intermediate subgp G with $\{0\} \subsetneq G \subsetneq \mathbb{Q}$; call its elements *good*. Take a non-zero $h \in G$, set $q := 1/h$, and let qG be our new G ; it is a proper subgp. But now, $\boxed{1 \text{ is good}}$.

Since G is not all of \mathbb{Q} , there exists a posint D where $\boxed{\frac{1}{D} \text{ is bad}}$. Consequently

$$\forall \text{ posints } N : \quad 1/D^N \notin G.$$

(Why? If $\frac{1}{D^N}$ were good, then adding D^{N-1} copies together would show $1/D$ good.) ISTShow that the numbers $\{1/D^N\}_{N=1}^\infty$ are in different cosets of G .

FTSOC, suppose $\frac{1}{D^j}$ and $\frac{1}{D^{j+K}}$ are in the same coset, where $j, K \in \mathbb{Z}_+$. Thus $\frac{1}{D^j} - \frac{1}{D^{j+K}} = \frac{D^K - 1}{D^{j+K}}$ is good. Adding D^{j+K-1} copies together shows that $\frac{D^K - 1}{D} = [D^{K-1}] - \frac{1}{D}$ is good. But D^{K-1} is good, since 1 is. This yields the contradiction that $\frac{1}{D}$ is good. \blacklozenge

12: Lemma. Group $(\mathbb{Q}, +)$ includes no non-trivial direct-product $H \times K$ of subgps. \blacklozenge

Proof. FTSOC, pick non-zero $\frac{a}{b} \in H$ and non-zero $\frac{x}{y} \in K$. By repeated addition, $H \ni bx \cdot \frac{a}{b} = ax$ and $K \ni ay \cdot \frac{x}{y} = ax$. But $ax \neq 0$. \blacklozenge

#33^P148. We have $|G| = p^N$, with N a posint. FTSOC, suppose that $|Z(G)| = p^{N-1}$. Consequently $Q := \frac{G}{Z(G)}$ has order p , and is therefore cyclic. By our Cyclic center-extension thm, then, G is abelian. \otimes \blacklozenge

#34^P148. FTSOC, suppose $T_2 = 0$. Thus each $T_{\text{Even}} = 0$. But the only odd positive factors $12 = 4 \cdot 3$ are 1 and 3. Consequently,

$$12 - T_1 = T_3 \mid \varphi(3) = 2.$$

But $12 - T_1$ equals 11, which is not even. \blacklozenge

#37^P148. First suppose G abelian. Then $f(x) := x^2$ is an endo $G \circ$. Now, $\text{Ker}(f)$ is trivial, since $|G|$ is odd; so f is injective. And $|G|$ is finite, so f is surjective.

For a general G , we can apply this argument to $A := \langle a \rangle_G$, since $N := |A|$ is odd. (Courtesy Lagrange, every G -subgp has odd order.) Thus A has a *unique* sqroot of a . (It is $a^{\frac{N+1}{2}}$.)

Were there a sqroot $r \in G \setminus A$, then subgroup

$$\langle r \rangle_G \stackrel{\text{note}}{=} A \sqcup rA \quad (\text{Distinct cosets must be disjoint.})$$

would have cardinality $2N$. But no G -subgroup has even order. \blacklozenge

#32^P191. A proper subgp $H \subset \mathbb{D}_4$ must have $\text{Ord}(H) \nmid 4$, so H is abelian. Were \mathbb{D}_4 a nt-direct-prod, it would be a product of abelian subgps, hence would be abelian. \otimes . \blacklozenge

#38^P191. Fix an $x \in \mathcal{C}(H)$, i.e $J_x \downarrow_H = \text{Id}_H$. For a $g \in G$ and $h \in H$, necessarily $h' := J_{g^{-1}}(h)$ is in H . So $J_x(h') = h'$. Consequently,

$$J_g(J_x(h')) = J_g(h') = h.$$

I.e, $[J_g J_x J_{g^{-1}}](h) = h$. So $g x g^{-1} \in \mathcal{C}(H)$. \blacklozenge

#46^P191. (Generalize) Allow G to be non-abelian. Let $F \subset G$ be the set of elts of finite order. Consider some G -subgp $H \subset F$, fix a $g \in G \setminus H$ and set $N := \text{H-Ord}(g)$. If H were G -normal, then this N would be the $\frac{G}{H}$ -order of coset gH , so it is this N that we wish to show infinite.

Were N finite, then $h := g^N$ is in H and thus has some finite order, say $K \in \mathbb{Z}_+$. By the Periods Lemma, $\text{Ord}_G(g)$ must divide K ; in particular, this order is finite, contradicting that g was not in H . \blacklozenge

#53^P191. In a cyclic group N each subgroup has $H \triangleleft^a N$, since the index $|H:N|$ characterizes H .

Returning, $H \triangleleft^a N \triangleleft G$ implies $H \triangleleft G$. \blacklozenge

#55^P191. With $Q := \frac{G}{H}$, divisibility (3') gives $\text{Ord}_Q(xH) \nmid \text{Ord}_G(x)$. So $\text{Ord}_Q(xH) \perp \text{Ord}(Q)$. But always $\text{Ord}_Q(xH) \nmid \text{Ord}(Q)$, so $\text{Ord}_Q(xH) = 1$. \blacklozenge

#56^P191. a Stronger, we show G' to be a characteristic subgroup of G . Fix $\alpha \in \text{Aut}(G)$ and element $w \in G'$. Write $w = c_1 \cdots c_L$ as a product of commutators. Since

$$\alpha(w) = \prod_{j=1}^L \alpha(c_j),$$

ISTShow that $\alpha(\text{commutator } c)$ is a commutator. But

$$\alpha([a, b]) = [[\alpha(a), \alpha(b)]] .$$

b To show the quotient G/G' abelian, we note that

$$[[aG', bG']] \stackrel{\text{def}}{=} [[a, b]G'] \stackrel{\text{note}}{=} G' .$$

Similarly, $[[bG', aG']] = G'$.

c Since G/N is abelian, necessarily

$$N = [[aN, bN]] \stackrel{\text{note}}{=} [[a, b]N] .$$

Thus $N \ni [[a, b]]e = [[a, b]]$.

d Fixing $g \in G$ and $h \in H$, we want $ghg^{-1} \in H$, which is implied by $\overline{ghg^{-1}H \subset H}$. But H owns all commutators, so $[[a^{-1}, b^{-1}]]H = H$. Left-multiplying by ba gives

$$abH = baH .$$

Setting $a := gh$ and $b := g^{-1}$ yields the ovalbox. \blacklozenge

#59^P191. We prove the contrapositive. Since $\text{Aut}(G)$ is cyclic, so is its subgroup $\text{Inn}(G)$. Since $\text{Inn}(G) \cong \frac{G}{Z(G)}$, the G/Z lemma applies (P.185 Gallian), to say that G is abelian. \blacklozenge

Ques. Does cyclicity of $\text{Aut}(G)$ force G to be cyclic? \square

#61^P191. (We have $H \triangleleft G$, with $|G| < \infty$, and some $y \in G$. In the quotient group $Q := G/H$, let N denote the order of element yH .)

ISTShow that $\text{Ord}_G(y)$ is a (finite) multiple of N ; for then $y^{\text{Ord}(y)/N}$ has order N . By hypothesis,

$$y^N H \stackrel{\text{normality}}{=} [yH]^N = H .$$

So $y^N \in H$. And N is the least positive k with $y^k \in H$. In the notation of the Periods Lemma, (3), the set

$$P_H := \{k \in \mathbb{Z} \mid y^k \in H\}$$

is the set of multiples of N . And $\text{Ord}(y) \in P_H$. \blacklozenge

#66^P191. Write $H = \langle h \rangle$ take $x \in G$. But $xhx^{-1} \neq e$, and $xhx^{-1} \in H$. So $xhx^{-1} = h$. \blacklozenge

#68^P191. We have groups $G \supset H$, where $D := |H|$ is odd and $|G:H| = 2$. Fixing a $y \in G \setminus H$, we have

$$y^D H = G \setminus H,$$

since $H \triangleleft G$. Take the product of some enumeration,

$$p := g_1 \cdot g_2 \cdot g_3 \cdot \dots \cdot g_{2D-1} \cdot g_{2D},$$

of G . We can write each g_j as $h_j z_j$, where each $h_j \in H$ and z_j is either \mathbf{e} (if $g_j \in H$) or is y (if $g_j \in G \setminus H$). Thus

$$p = [h_1 z_1] \cdot \dots \cdot [h_{2D} z_{2D}] \stackrel{*}{=} [z_1 \cdot z_2 \cdot \dots \cdot z_{2D}] \cdot \eta,$$

where η is a product of $2D$ many elements of H . Equality (*) used $H \triangleleft G$.

Lastly, $[z_1 \cdots z_{2D}]$ equals $y^D \cdot \mathbf{e}^D$. Thus $p \in y^D H$. \blacklozenge

#24^P230. Recall that $N := |G|$ is odd (and finite). Also, subgroup $H \subset G$ has order 5, so $H \cong \text{Cyc}_5$. Consequently, $A := \text{Aut}(H)$ has order $\varphi(5) = 4$. (Indeed, $A \cong \text{Cyc}_4$.) The map $f: G \rightarrow A$ by $f(x) := J_x|_H$ is well-defined, since $H \triangleleft G$. And f is a gp-hom so

$$|\text{Range}(f)| \text{ divides both } N \text{ and } |A|=4.$$

But the only odd factor of 4 is 1, so $\text{Range}(f)$ is the trivial group. I.e, $\text{Ker}(f) = G$. I.e, $H \subset \text{Z}(G)$. \blacklozenge

#21^P230. FTSCContradiction, suppose that quotient $Q := \mathbb{S}_4/H$ is not iso to \mathbb{D}_3 ; hence $G \cong \text{Cyc}_6$. So there exists $g \in \mathbb{S}_4$ with $\text{H-Ord}(g) = 6$. Thus $\text{Ord}(g) \mid 6$, and so some element in $\langle g \rangle$ has order 6. But \mathbb{S}_4 has no order-6 element. \blacklozenge

#30^P230. We have map $G \rightarrow G : x \mapsto \hat{x}$ so that

$$[g_1 g_2 g_3 = \mathbf{e}] \xrightarrow{\dagger} [\hat{g}_1 \hat{g}_2 \hat{g}_3 = E^3].$$

Applying (\dagger) to xex^{-1} and $\mathbf{e}xx^{-1}$, yields $\hat{x}\hat{\mathbf{e}} = \hat{\mathbf{e}}\hat{x}$. So $T := \hat{\mathbf{e}}^{-1}$ commutes with each \hat{x} . Define $\tilde{x} := T \cdot \hat{x}$; so $\tilde{\mathbf{e}} = \mathbf{e}$. Commutativity yields $\tilde{g}_1 \tilde{g}_2 \tilde{g}_3 = T^3 \cdot \hat{g}_1 \hat{g}_2 \hat{g}_3$. Thus $g_1 g_2 g_3 = \mathbf{e}$ implies

$$\dagger: \quad \tilde{g}_1 \tilde{g}_2 \tilde{g}_3 = T^3 \cdot \hat{\mathbf{e}}^3 = \mathbf{e} = \tilde{\mathbf{e}}.$$

And applying (\dagger) to $x^{-1}x\mathbf{e} = \mathbf{e}$ produces $\tilde{x}^{-1} = \tilde{x}^{-1}$.

The last step is to show that $\tilde{}$ respects multiplication. Now always $[yx]x^{-1}y^{-1} = \mathbf{e}$, so

$$\mathbf{e} = [\tilde{y}\tilde{z}] \cdot \tilde{z}^{-1} \cdot \tilde{y}^{-1} = [\tilde{y}\tilde{z}] \cdot \tilde{z}^{-1} \cdot \tilde{y}^{-1}.$$

Thus $\tilde{y}\tilde{z} = [\tilde{y}\tilde{z}]$. \blacklozenge

#35^P230. If $\exists \alpha \in G \setminus \text{Z}(G)$ then $J_\alpha \neq \text{Id}_G$. Else G is a abelian, so $x \mapsto x^{-1}$ is an aut; this aut differs from Id IFF there exists a $\beta \neq \beta^{-1}$. So, WLOG, G is abelian group with every element an involution.

Let $\hat{I} \subset G$ be a maximal indep. set; each $g \in G$ has a *unique* description as a (finite) product of elts from \hat{I} . Since $|G| \geq 3$, we can write \hat{I} as $\{\gamma_0, \gamma_1\} \sqcup I$. Define $\psi \in \text{Aut}(G)$ by $\psi(\gamma_j) := \gamma_{1-j}$ and $\psi|_I := \text{Id}_I$. \blacklozenge

13: Lemma. Suppose $M \subsetneq G$ is a maximal-proper subgp. If $M \triangleleft G$ then the quotient $Q := G/M$ is cyclic of prime order. \blacklozenge

Proof. It suffices to show that the only proper subgp of Q is the trivial group. So suppose $Q' \subsetneq Q$. Then

$$M' := \bigcup_{yM \in Q'} yM \stackrel{\text{note}}{\supset} M$$

is a proper subgroup of G . Since M is maximal, M' simply is M . Hence $Q = \{\mathbf{e}\}$. \blacklozenge

#36^P230. By (13), if \mathbb{Q} has a max-proper subgp then \mathbb{Q} has a subgp of finite index, \otimes ing **#28^P148**. \blacklozenge

#25^P254. The ring is a notnec-commutative “integral domain”. Given elements with $ab = 1$, note that $aba = 1 \cdot a = a \cdot 1$. So

$$0 = aba - a \cdot 1 = a \cdot [ba - 1].$$

But $a \neq 0$ (since $ab = 1$), so $ba - 1$ must be zero. \blacklozenge

Miscellaneous Problems

First, a tool.

14: Lemma. Consider a homomorphism $f: G \rightarrow A$ between groups. Then the index $I := |G:\text{Ker}(f)|$ divides both $\text{Ord}(G)$ and $\text{Ord}(A)$. \blacklozenge

Proof. This I is $|\text{Range}(f)|$, hence divides $\text{Ord}(A)$. \blacklozenge

15: Theorem. Fix an $N \in [2.. \infty)$. Consider a group G with $\#Z(G) \nmid N$. If ^{♥1}

$$\dagger: \quad \text{Ord}(G) \perp \varphi(N)$$

then G has no cyclic normal subgroup of order N . (So if N is prime, then G has no normal order- N subgroup.) \diamond

Proof. FTSOC, fix an order- N subgroup $B \triangleleft G$. By Lagrange, $B \not\subset Z(G)$.

Recall conjugation $J_x: G \rightarrow G$ by $J_x(g) := xgx^{-1}$. Letting $A := \text{Aut}(B)$, the restriction

$$f: G \rightarrow A \quad \text{by} \quad f(x) := J_x|_B,$$

is a homomorphism. By the foregoing lemma, the index $|G: \text{Ker}(f)|$ divides both $\text{Ord}(G)$ and $\text{Ord}(A)$. And $\text{Ker}(f)$ is *not* all of G , since B is not a subset of $Z(G)$. Thus

*: $\text{Ord}(G)$ and $\text{Ord}(A)$ have a non-trivial common factor.

Lastly, since B is cyclic, $\text{Aut}(B)$ is isomorphic to the units group $\Phi(N)$, whose order is $\varphi(N)$. Thus (\dagger) and $(*)$ contradict ^{♥2} each other. \diamond

16: Prop. Suppose \mathbf{V} a vectorspace over field \mathcal{F} , and N a posint. If $|\mathcal{F}| > N$, then \mathbf{V} can not be written as a union of N or fewer proper subspaces. \diamond

Proof. Let $\mathbf{E}_1, \mathbf{E}_2, \dots$ be a list of proper subspaces. Suppose, inductively at stage k , we have a vector \mathbf{y} which is in *none* of $\mathbf{E}_1, \dots, \mathbf{E}_{k-1}$.

Pick a $\mathbf{x} \in \mathbf{V} \setminus \mathbf{E}_k$ and consider vectors $\mathbf{y} + \alpha\mathbf{x}$, as scalar α ranges over some $k+1$ values in \mathcal{F} . FTSOC, suppose that each of these sums is in at least one of $\mathbf{E}_1, \dots, \mathbf{E}_{k-1}, \mathbf{E}_k$. The some two, $\mathbf{y} + \alpha\mathbf{x}$ and $\mathbf{y} + \beta\mathbf{x}$, lie in the same subspace. If both are in the last, \mathbf{E}_k ,

^{♥1} Assumption (\dagger) forces G to be finite *except* in the $N=2$ case, since $\varphi(2) = 1$. So an odd center, $Z(G)$, precludes even an *infinite* group from having a normal order-2 subgroup.

^{♥2} Whether or not B is cyclic, always $\text{Ord}(A) \mid [N-1]!$ since A can be viewed as a subgroup of the group of permutations of $B \setminus \{\mathbf{e}\}$. So we *could* try to replace (\dagger) with a stronger assumption, $\text{Ord}(G) \perp [N-1]!$, and try to preclude even *non-cyclic* normal subgroups. But this gains nothing, since when N is composite, this strengthening forces $\text{Ord}(G) \perp N$, so G has no order- N subgroups, normal nor not.

then their difference $[\alpha - \beta]\mathbf{x}$ is in \mathbf{E}_k ; a contradiction, since $\alpha - \beta \neq 0$.

Conversely, if both lie in an earlier subspace, say \mathbf{E}_1 , then \mathbf{E}_1 owns this scaled-difference,

$$\alpha[\mathbf{y} + \beta\mathbf{x}] - \beta[\mathbf{y} + \alpha\mathbf{x}] \stackrel{\text{note}}{=} [\alpha - \beta]\mathbf{y}.$$

But this forces \mathbf{y} in \mathbf{E}_1 . \otimes \diamond

#32^P347. Follows from Prop. 16, above. \blacklozenge

#P.377. \blacklozenge

#35^P377. [Ambiguously stated: Refers to \sqrt{a}, \sqrt{b} , but doesn't say what sqroot to chose when a, b are negative. I'll restate here, then correct.]

We have complex numbers s and t , with s^2 and t^2 each rational. Define the field $\mathcal{F} := \mathbb{Q}((s+t))$. GOAL: $\mathbb{Q}((s+t)) = \mathbb{Q}((s, t))$.

Soln. Can be FALSE, when $s = -t$; for then \mathcal{F} equals \mathbb{Q} , yet $\mathbb{Q}((s, t)) = \mathbb{Q}((s))$ need not. So assume $s+t \neq 0$. \diamond

Certainly $\mathcal{F} \supset \mathbb{Q} \ni s^2+t^2$, so \mathcal{F} owns the ratio $\frac{s^2+t^2}{s+t} \stackrel{\text{note}}{=} s-t$. Thus \mathcal{F} owns $[s+t] + [s-t] \stackrel{\text{note}}{=} 2s$. And $\text{Char}(\mathcal{F}) \neq 2$, so \mathcal{F} owns s . Hence \mathcal{F} owns t . \blacklozenge

Filename: Problems/Algebra/gallian.tex

As of: Tuesday 22Apr2008. Typeset: 20Jul2016 at 09:07.