1. Let $e \neq a \in G$.

The order of a divides $|G| = p$, a prime (and is not equal to 1 because $a \neq e$).

So a has order p, i.e., $|\langle a \rangle| = p$, so $\langle a \rangle = G$

and
$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\xrightarrow{\sim} \langle a \rangle = G \\ i &\longmapsto a^i \end{aligned}$$

2. We follow the hint:-

Let $e \neq a \in G$

& $b \in G \setminus \{e, a, a^{-1}\}$

Then $G = \{e, a, b, ab\}$

<u>Cases</u>
$$ba = \begin{cases} e & \Rightarrow b = a^{-1} \text{ ※} \\ a & \Rightarrow b = e \text{ ※} \\ b & \Rightarrow a = e \text{ ※} \\ ab & \end{cases}$$

$\therefore$ $ba = ab$.

Now clearly $a^i b^j \cdot a^k b^l \overset{\text{using } ba=ab \text{ repeatedly}}{=} \cancel{a^i \cdot b^j}\ a^i \cdot a^k \cdot b^j \cdot b^l = a^{i+k} b^{j+l} = a^k b^l a^i b^j$

$\forall\, i, j, k, l \in \mathbb{Z}_{\geq 0}$, so G is abelian. $\square$

3. We follow the hint

$$a = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\begin{aligned} bab &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta & -\sin\theta \\ -\sin\theta & -\cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = a^{-1} \end{aligned}$$
$\square$

4. a. We follow the hint:

Pick $\underline{q} \in \mathbb{R}^2$, consider $O = \{ g \cdot \underline{q} \mid g \in G \}$ & $\underline{p} = \frac{1}{|G|} \cdot \sum_{\underline{x} \in O} \underline{x} = \frac{1}{n}(\underline{p}_1 + \dots + \underline{p}_n)$

$= \{ \underline{p}_1, \dots, \underline{p}_n \}$

Claim: $\forall\, g \in G$, $g \cdot \underline{p} = \underline{p}$.

Proof: Every isometry of $\mathbb{R}^2$ has the form $g(\underline{x}) = A \cdot \underline{x} + \underline{b}$ where A is a 2×2 orthogonal matrix & $\underline{b} \in \mathbb{R}^2$

(this is proved in MATH235 (linear algebra) for the case $g(\underline{0}) = \underline{0}$. In general, one can compose with a translation to reduce to this case.)

Thus
$$g(\underline{p}) = A \cdot \left(\frac{1}{n} \sum_{i=1}^{n} \underline{p}_i\right) + \underline{b}$$
$$= \left(\frac{1}{n} \cdot \sum_{i=1}^{n} A\underline{p}_i\right) + \underline{b} = \frac{1}{n} \cdot \sum_{i=1}^{n} (A\underline{p}_i + \underline{b})$$
$$= \frac{1}{n} \cdot \sum_{i=1}^{n} g(\underline{p}_i)$$

But, since $\mathcal{O} = \{\underline{p}_1, \ldots, \underline{p}_n\}$ is an orbit of G, $g \in G$ permutes $\mathcal{O}$.

Thus
$$\frac{1}{n} \sum_{i=1}^{n} g(\underline{p}_i) = \frac{1}{n} \sum_{i=1}^{n} \underline{p}_i = \underline{p}. \quad \square$$

b. Let $g_0 \in G$ be the rotation w/ smallest possible nonzero angle θ_0 (measured ccw, say) $\dagger$

If $g \in G$ is a rotation w/ angle θ, we can write $\theta = q \cdot \theta_0 + r$, $0 \le r < \theta_0$, $q \in \mathbb{Z}_{\ge 0}$.

& $g \cdot g_0^{-q} \in G$ is a rotation thru angle r. So $r = 0$ by choice of θ_0,

& $g = g_0^q$, thus $\langle g_0 \rangle \le G$ is the subgroup of rotations.

($\dagger$: here we assume $\exists$ nontrivial rotation in G; otherwise we're done.)

c. The subgroup $G' \le G$ of rotations is the kernel of the hom. $\det : G \to \{\pm 1\}$
$$(g(\underline{x}) = A\underline{x}) \longmapsto \det A$$

(where we have chosen coords so that the fixed point $\underline{p} = \underline{0}$.)

Thus either $G' = G$ (& we're done) or $G' < G$ has index 2, & G is generated by G' & a single element $g \in G \setminus G'$, necessarily a reflection in a line passing through p (recall from 235: a 2×2 orthogonal matrix A satisfies $\det A = +1$ or -1 & defines a rotation or reflection respectively).

Now it follows that G is the dihedral group of symmetries of the regular n-gon with vertices the orbit under G' of a point $q \in l \setminus \{p\}$ where l is the line of reflection and $n = |G'|$.

(The cases $n=1$ & 2 need to be treated separately as described in the parenthetical remark).

5. $D_4 = \{\underbrace{e, a, a^2, a^3}_{\text{rotations}}, \underbrace{a, ab, a^2b, a^3b}_{\text{reflections}}\}$

a = rotation by $2\pi/n$ ccw about center of mass of reg. n-gon.

b = reflection in an axis of symmetry

(here $n=4$.)

orders: $1, 4, 2, 4, 2, 2, 2, 2$

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

orders $1, 2, 4, 4, 4, 4, 4, 4$

Thus $D_4 \not\cong Q_8$ e.g. because D_4 has 5 elements of order 2, Q_8 has 1.

6. $\theta : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is a well defined group homomorphism

$\bar{x} \longmapsto (x \bmod m, x \bmod n)$

$\ker \theta = \{\bar{x} \in \mathbb{Z}/mn\mathbb{Z} \mid m | x \text{ \& } n | x\} \overset{\gcd(m,n)=1}{=} \{\bar{x} \in \mathbb{Z}/mn\mathbb{Z} \mid mn | x\}$

$= \{0\}$.

Thus θ injective. $\therefore$, by pigeonhole principle, θ is surjective, so θ is an isom.

7. G is finite $\iff$ $s = 0$.

We show the factors are uniquely determined by counting elements of different orders.

We order the factors so that $p_1 \le \cdots \le p_r$, say $p_1 = p_2 = \cdots = p_{r_1}$, $p_{r_1+1} = \cdots = p_{r_2}$, etc

and $\alpha_1 \le \cdots \le \alpha_{r_1}$, $\alpha_{r_1+1} \le \cdots \le \alpha_{r_2}$, etc.

We see: # elements of order each power of p_1 is the same as for $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{\alpha_{r_1}}\mathbb{Z}$, etc.

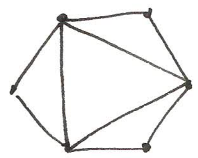
So we can reduce to the case $p_1 = \cdots = p_r =: p$, $r = r_1$.

Observe: $\#(\text{elements of order dividing } p^\alpha) = p^{f(\alpha)}$ where $f(\alpha) = \sum_{i=1}^{r} \min(\alpha_i, \alpha)$

Now $f(\alpha+1) - f(\alpha) = \#\{ i \mid \alpha_i > \alpha \} =: g(\alpha)$; $g(\alpha-1) - g(\alpha) = \#\{i \mid \alpha_i = \alpha\}$.

So, given f we can recover the sequence of exponents $\alpha_1, \dots, \alpha_r$. $\square$.

8. The regular n-gon is inscribed in the regular $2n$-gon.



$n=3$

Choose a vertex of the regular n-gon & let b be the reflection in the axis of symmetry thru that vertex.

Then $D_n = \langle a', b\rangle \leq D_{2n} = \langle a, b\rangle$ where a is rotation about the centre of mass thru $2\pi/2n$ ccw & $a' = a^2$.

The element $a^n \in D_{2n}$ is central (i.e. commutes with all elements of D_{2n} (e.g. because it corresponds to $-I \in GL_2(\mathbb{R})$ under the injective hom $D_{2n} \hookrightarrow GL_2(\mathbb{R})$).

It follows that the map
$$\varphi : D_n \times \mathbb{Z}/2\mathbb{Z} \longrightarrow D_{2n}$$
$$(g, i) \longmapsto g \cdot (a^n)^i$$
is a hom. of groups. Now suppose n is odd.

The kernel of φ is trivial, $\ker\varphi = \{e\}$, because $D_n \cap \langle a^n \rangle = \{e\}^{\dagger}$ (using n odd) :
$$\varphi(g,i) = e \iff g \cdot a^{ni} = e \iff g = (a^n)^{-i} \overset{\dagger}{\iff} g = e.$$

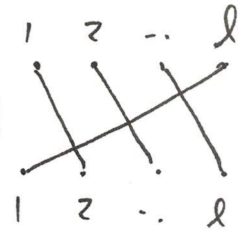
Since $|D_n \times \mathbb{Z}/2\mathbb{Z}| = |D_{2n}| = 4n$, φ is an isomorphism.

Conversely: if n is even then $D_n \times \mathbb{Z}/2\mathbb{Z} \not\cong D_{2n}$ because e.g. D_{2n} contains an element of order $2n$ and $D_n \times \mathbb{Z}/2\mathbb{Z}$ does not.* $\square$

(* Note: The order of $(a,b) \in G \times H$ equals the lcm of the order of $a \in G$ & the order of $b \in H$.)

9. a) Recall from class:

$(12\cdots l) = \sigma \downarrow$



$\rightsquigarrow \quad (12\cdots l) = (12)(23)\cdots(l-1,l)$

Similarly,

$$(a_1 a_2 \cdots a_l) = (a_1 a_2)(a_2 a_3)\cdots(a_{l-1} a_l)$$

So, if now σ has cycle type $(l_1, \ldots, l_r)$ it can be written as a product of $(l_1 - 1) + \cdots + (l_r - 1)$ transpositions, so $\operatorname{sgn}(\sigma) = (-1)^{(l_1-1)+\cdots+(l_r-1)}$.

b) $S_3 = \{e, (12), (13), (23), (123), (132)\}$

$A_3 = \{e, (123), (132)\}$

$S_4 = \{e, (12), (13), (14), (23), (24), (34), (123), (132), (124), (142), (134), (143),$
$(234), (243), (12)(34), (13)(24), (14)(23),$
$(1234), (1243), (1324), (1342), (1423), (1432)\}$

$A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$.

c). $\sigma(i) = j \iff g\sigma g^{-1}(g(i)) = g(j)$

Thus, if $\sigma = (a_1 \cdots a_l)(b_1 \cdots b_m)(c_1 \cdots c_n)\cdots$ is the cycle decomp. of a permutation $\sigma \in S_N$ then

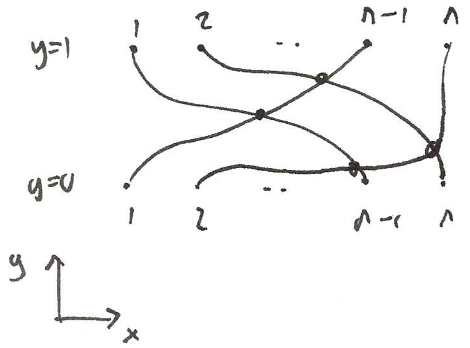
$$g\sigma g^{-1} = (g(a_1)\cdots g(a_l))(g(b_1)\cdots g(b_m))(g(c_1)\cdots g(c_n))\cdots$$

Thus $g\sigma g^{-1}$ & σ have the same cycle type.

& conversely, if τ & σ have the same cycle type, $\exists g \in S_N$ s.t. $\tau = g\sigma g^{-1}$

$\square$.

d.



$1 = t_0 > t_1 > \dots > t_m = 0$

Divide $\mathbb{R} \times [0,1]$ into strips $\mathbb{R} \times [t_{i-1}, t_i]$ $i = 1, \dots, m$, such that there is a unique crossing in the interior of each strip

Labelling the endpoints of the paths in each strip from left to right, we see that the paths define a transposition τ_i in the i^{th} strip (in fact $\tau_i = (j, j+1)$ for some j).

Thus σ is the product of m transpositions, $\sigma = \tau_m \tau_{m-1} \cdots \tau_1$

In the example pictured above ($n=4$) $\sigma = (13)(24)$

$= (23)(34)(12)(23)$

10a Consider the action of the group D_3 on the set of vertices of the triangle (labelled 1,2,3); this gives a group hom.

$$\varphi : D_3 \longrightarrow S_3$$
$$g \longmapsto (x \mapsto g \cdot x)$$

φ is clearly injective (e.g. because, choosing coordinates so that the centre of mass is the origin, g is a linear transformation, & two distinct vertices v & w of the triangle form a basis of $\mathbb{R}^2$, so g is determined by gv & gw.)

Now $|D_3| = |S_3| = 6$, so φ is an isom.

b. Reasoning as in a., we obtain an injective hom. $\varphi : G \longrightarrow S_4$

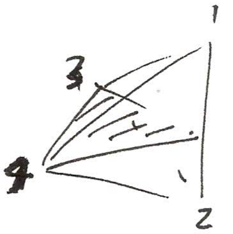
Also $|G| = |O_x| \cdot |G_x| = 4 \cdot 6 = 24 = |S_4|$

taking x a vertex of the tetrahedron (so that O_x is the set of vertices of the tetrahedron & G_x is the subgroup of G isomorphic to D_3 given by rotations about the axis through x & the center of mass & reflections in the planes containing this axis.)

So φ is an isomorphism.

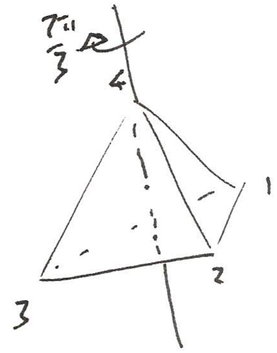
e identity

(12) reflection

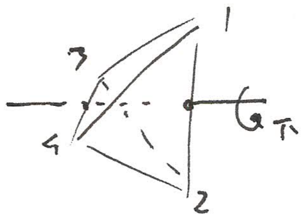


plane of reflection shaded.

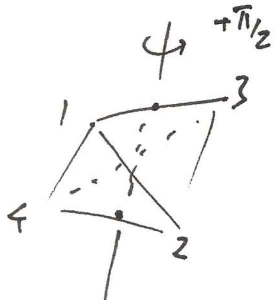
(123) rotation thru $\pm \frac{2\pi}{3}$ about axis joining center of mass & a vertex



$(12)(34)$ rotation thru π about axis joining midpoints of two opposite edges



(1234) rotary reflection w/ angle $\pm \pi/2$ about axis joining midpoints of two opposite edges



$+\pi/2$, then reflect in normal plane thru origin.

In particular,

The subgroup of rotations corresponds to A_4

The 3-cycles in A_4 form two conjugacy classes of size 4, corresponding to ccw/cw rotations thru $\frac{2\pi}{3}$ when viewed from the fixed vertex

11. With notation as in Q5,

$D_6 = \{e, a, a^2, a^3, a^4, a^5, b, ab, \dots, a^5 b\}$

orders $\quad 1, 6, 3, 2, 3, 6, 2, 2, \dots \quad 2$

$A_4 = \{e, \underbrace{(12)(34), (13)(24), (14)(23)}_{2}, \underbrace{(123), (132), (124), (142), (134), (143), (234), (243)}_{3}\}$

order $\quad 1$

$\mathbb{Z}/4\mathbb{Z} \leq G \Rightarrow \exists$ element $g \in G$ of order 4

$\Rightarrow G \not\cong D_6, \ G \not\cong A_4.$

Also $D_6 \not\cong A_4$ because e.g. D_6 has an element of order 6 while A_4 has no such element.

12. a. The inverse is given by $F \cup \{\infty\} \xrightarrow{g} \mathbb{P}^1_F$

$F \ni z \longmapsto [(z,1)]$

$\infty \longmapsto [(1,0)]$

(Check: $f : \mathbb{P}^1_F \to F \cup \{\infty\}$, $[(x,y)] \longmapsto \begin{cases} x/y & y \neq 0 \\ \infty & y = 0 \end{cases}$ is well defined,

& $fg = id$, $gf = id$. (details omitted).)

b. Similarly $\quad \mathbb{P}^n_F \to F^n \cup \mathbb{P}^{n-1}_F$

$$[(x_0, \dots, x_n)] \longmapsto \begin{cases} (x_1/x_0, \dots, x_n/x_0) \in F^n \text{ if } x_0 \neq 0 \\ [(x_1, \dots, x_n)] \in \mathbb{P}^{n-1}_F \text{ if } x_0 = 0. \end{cases}$$

is a bijection, w/ inverse $\quad F^n \cup \mathbb{P}^{n-1}_F \longrightarrow \mathbb{P}^n_F$

$F^n \ni (y_1, \dots, y_n) \longmapsto [(1, y_1, \dots, y_n)]$

$\mathbb{P}^{n-1}_F \ni [(z_1, \dots, z_n)] \longmapsto [(0, z_1, \dots, z_n)].$

c. Recall $G \circlearrowright X \leftrightarrow \varphi : G \to S_X$ group hom.

$g \longmapsto (x \mapsto g \cdot x)$

In our case, $|\mathbb{P}^1_F| = |F \cup \{\infty\}| = q+1$.

So $S_{\mathbb{P}^1_F} \simeq S_{q+1}$

$PGL_2(F) \curvearrowright \mathbb{P}^1_F \quad \rightsquigarrow \quad \varphi : PGL_2(F) \longrightarrow S_{q+1}$

(NB. $GL_{n+1}(F) \curvearrowright F^{n+1}$, $\quad g \cdot \underline{x} =$ matrix-vector product.

$PGL_{n+1}(F) = GL_{n+1}(F) \Big/ \{\text{scalar matrices}\} = GL_{n+1}(F) \big/ \sim \qquad g \sim h \iff g = \lambda \cdot h$, $\lambda \in F^\times$.

$\mathbb{P}^n_F = F^{n+1} \setminus \{0\} \big/ \sim \qquad \underline{x} \sim \underline{y} \iff \underline{x} = \lambda \underline{y}$, some $\lambda \in F^\times := F \setminus \{0\}$

The induced action is $[g] \cdot [\underline{x}] = [g \cdot \underline{x}]$. (check well defined)

here $[a]$ denotes the equiv. class of a.)

d) φ is injective: $[g] \in PGL_2(F)$ determined by $\left[g \cdot \begin{pmatrix}1\\0\end{pmatrix}\right], \left[g \cdot \begin{pmatrix}0\\1\end{pmatrix}\right], \left[g \cdot \begin{pmatrix}1\\1\end{pmatrix}\right]$

– the first two determine the cols of g up to independent scale factors,

& the third the determines g up to an overall scale factor, i.e., determines $[g] \in PGL_2(F)$.

Alternative argument: We show $\ker \varphi = \{e\}$:–

If $g \in \ker \varphi$, $g = \left[\begin{pmatrix}a & b\\ c & d\end{pmatrix}\right]$, then

$$g \cdot \left[\begin{pmatrix}1\\0\end{pmatrix}\right] = \left[\begin{pmatrix}1\\0\end{pmatrix}\right] \Rightarrow c = 0$$

$$g \cdot \left[\begin{pmatrix}0\\1\end{pmatrix}\right] = \left[\begin{pmatrix}0\\1\end{pmatrix}\right] \Rightarrow b = 0.$$

$$g \cdot \left[\begin{pmatrix}1\\1\end{pmatrix}\right] = \left[\begin{pmatrix}a\\d\end{pmatrix}\right] = \left[\begin{pmatrix}1\\1\end{pmatrix}\right] \Rightarrow a = d.$$

Thus $g = \left[\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\right] = e \in PGL_2(F)$.

e) $$|PGL_2(F)| = \frac{(q^2-1)(q^2-q)}{(q-1)} = (q+1)(q-1)\cdot q = \begin{cases} 6 & q=2 \\ 24 & q=3 \\ 60 & q=4 \end{cases}$$

Thus $|PGL_2(F)| = |S_{q+1}|$ for $q = 2,3 \overset{d)}{\Rightarrow} \varphi$ isom for $q = 2,3$

$|PGL_2(F)| = \frac{1}{2}|S_{q+1}|$ for $q=4 \overset{d)}{\Rightarrow} PGL_2(F) \xrightarrow{\sim} A_5$ for $q=4$:—

Proof: $H := \varphi(PGL_2(\mathbb{F})) \leq S_5$, $|H| = \frac{1}{2}|S_5| \Rightarrow H \triangleleft S_5$

Thus $H = \ker \theta$, $\theta : S_5 \longrightarrow S_5/H \simeq \mathbb{Z}/2\mathbb{Z}$.

Now restricting to A_5, get $\psi : A_5 \longrightarrow \mathbb{Z}/2\mathbb{Z}$, $\ker \psi = A_5 \cap H \triangleleft A_5$

Either $A_5 \subset H$ & ψ is trivial

or ψ is surjective & $|\ker \psi| = \frac{1}{2}|A_5| = 30$, $\ker \psi \triangleleft A_5$ # A_5 is simple.

So $A_5 \subset H$, & $|A_5| = |H|$ $\Rightarrow$ $A_5 = H$ $\square$.