sage filler. some groups: $C_n, S_n, A_n, D_n; GF(p), Aut(E/F)$,
classic Lie type over $\mathbf{R}, \mathbf{C}, \mathbf{H} : GL, SO, SL, PSL, Sp, SU$

$$\mathrm{Dic}_n := \langle a, x \mid a^{2n} = 1,\ x^2 = a^n,\ x^{-1}ax = a^{-1} \rangle$$

alt def by exact sequence $1 \to C_{2n} \to \mathrm{Dic}_n \to C_2 \to 1$
G-actions
$f : H \leq G \curvearrowright G; \ell_h(x) \stackrel{\text{def}}{=} hx \in G$
other way may not work? $G \curvearrowright H; ah \notin H$
however $N \triangleleft G, G \curvearrowright N; c_g(x) \stackrel{\text{def}}{=} gxg^{-1}$
$G \curvearrowright G/H, f(g, aH) := (ga)H$

1. PERMUTATIONS & CYCLES

$\sigma \in Aut\mathbf{N}$, e.g.,

- $n \mapsto n$
- $\sigma \in \mathbf{Z}_p : n \mapsto n^2$
- $n \mapsto n + 1$

These are really permutations, an *N-cycle* satisfies

(1) $o(\sigma) = N$, possibly infinity

Remember, permutations form a symmetric group, with function composition as the binary operation. Thus for *any* permutations, σ, τ, you can compose and invert them $\tau \circ \sigma^{-1}$. Whem $\sigma \circ \sigma' = \sigma' \circ \sigma$, we say they are *disjoint* and write $\sigma \coprod \sigma'$

Consider the strictly nondecreasing 2-cycles $\sigma_i \geq \sigma_j$ equality iff equal etcetc.

MILNE

PROPOSITION 1.25. Let H be a subgroup of a group G.
(a) An element a of G lies in a left coset C of H if and only if $C = aH$
(b) Two left cosets are either disjoint or equal.
(c) $aH = bH$ if and only if $a^{-1}b \in H$
(d) Any two left cosets have the same number of elements
(possibly infinite).

Proof. Recall $a \in H \implies aH = H$. If this is the case, any left coset of H via elements of H will be $aH (= H)$.
Otherwise for $a \neq c \in G - H : a \in cH \implies aH \subset cH$ (since $\exists h \in H : a = ch, h = c^{-1}a$)
Using this, $cH = chH = cc^{-1}aH = aH$
$\implies$ (a).
and since, by (a), any intersection implies equality of cosets, only disjunct cosets remain
$\implies$ (b)
Going the other way, if $aH = cH$:

$$ca^{-1}H = H, ca^{-1} \in H$$

$\implies$ (c)
Define as follows

$$\phi : aH \to bH : x \mapsto (ba^{-1})x, \phi^{-1} : x \mapsto ab^{-1}c, \phi\phi^{-1} = \phi^{-1}\phi = 1$$

This defines a inverse system between aH, bH, thus iso ie same cardinality $\implies$ (d) □

[Note 1: Cosets partition G, since $a \in aH$ along with 1.25(b).]
[Note 2:In regards to right cosets, if we modify the function in 1.25(c) slightly

$$\phi : aH \to Hb : ah \mapsto (ah)^{-1}ab = h^{-1}b \in Hb$$

$$\phi^{-1} : Hb \to aH : hb \mapsto ab(hb)^{-1} = ah^{-1} \in aH$$

we get a isomorphism between left and right cosets.]

Definition 1. *The* ***index*** $(G : H)$ *is the number of left (equivalently right) H-cosets in G*

THEOREM 1.26 (LAGRANGE). If G is finite, then

$$(G : 1) = (G : H)(H : 1)$$

In particular, the order of every subgroup of a finite group divides the order of the group.

Proof. $(G, 1) = \sum_{a \in G}$ Cosets partition G so $\sum_{aH \subset G} |aH| = |G| = (G : 1)$
Cosets have equal cardinality relative to a given subgroup (which is itself the coset eH), and since the (left) multiplier determines the number of unique cosets

$$(G : 1) = |G| = \sum_{a \in G} |aH| = (G : H)(H : 1)$$

□

COROLLARY 1.27. The order of each element of a finite group divides the order of the group.

Proof. Set $H = \langle a \rangle$, then $|H| = o(a)$ □

One of the Sylow theorems is a partial converse of Lagrange for prime-powers p^n:

THEOREM 5.2 (SYLOW I). Let $G \in$ **FinGp** be a finite group, and let p be prime. If $p^n | (G : 1)$, then G has a subgroup of order p^n

Proof. TBA □

Toshow: nexted subgroups $K < H < G : (G : K) = (G : H)(H : K)$

Normal subgroups, conjugacy

Definition 2. $N \lhd G$ *if* $\forall g \in G, gNg^{-1} = N$

What about if $g^{-1}Ng = N$?

$$g^{-1}Ng = N \iff Ng = gN \iff gNg^{-1} = N$$

So it doesn't matter how you conjugate.

REMARK 1.32. suffices to show $gNg^{-1} \subset N (\forall g \in G)$

Proof.

$$gNg^{-1} \subset N \implies N \subset g^{-1}Ng = gNg^{-1}$$

$\therefore gNg^{-1} = N$. □

important note: this is only the case if *every* $g \in G$ fulfills this criterion, and in the following example $G = GL(2, \mathbf{Q}), g = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $H = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)\}_{n \in \mathbf{Z}} \cong \mathbf{Z}$

```
C= matrix(SR, 2, [1,'n',1,0])
```

$$\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{5} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5n \\ \frac{1}{5} & 0 \end{pmatrix} \cong 5\mathbf{Z}$$

$$\begin{pmatrix} \frac{1}{5} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{5}n \\ 5 & 0 \end{pmatrix}$$

In the first case conjugation yields a proper subset, but conjugation by the inverse isn't even in H.

EXAMPLE 1.36. (a) Every subgroup of index two is normal.
(b) Dihedral group, its cyclic and translational symmetries, $n = 2, n > 2$.
(c) Subgroups in **Ab** are normal, but converse not true, e.g., Q

Proof. (a) The subgroup H of index 2 has two cosets: namely itself $aH = H$, and $gH : g \in G - H$. In other words, G is partitioned into $H \coprod gH$. Then by exclusion, $gH = Hg$
(b) by commutivity, $C_n \triangleleft D_n \forall n$, but □

Definition 3. *When $1 \trianglelefteq N$ is the only series of normal subgroups, N is **simple***

PROPOSITION 1.37. If H and N are subgroups of G and N is normal, then HN is a subgroup of G. If H is also normal, then HN is a normal subgroup of G.

Proof. (1) First the case of mutual normalcy: $H, N \triangleleft G$,

$$gHNg^{-1} = g(g^{-1}Hg)(g^{-1}Ng)g^{-}1 = HN$$

(2) Relaxing the normalcy condition on H:

$$(HN)^{-1} = NH = HN$$

□

Moreover, if we let $X = N \cap N'$

Definition 4. $\langle X \rangle_{N \triangleleft G} \overset{def}{=} \bigcap_{X \subset N} N$*, the **normal subgroup generated by** X, is the intersection of normal subgroups containing X. As we will see this is equivalent to the **normal closure** $g^{-1}Xg$.*

LEMMA 1.38. If X is normal, then the subgroup $\langle X \rangle$ generated by it is also normal.

Proof. Say elements of $\langle X \rangle$ are of the form $a = a_1 \dots a_n$, then □

LEMMA 1.39. $\bigcup_{g \in G} gXg^{-1}$ is the smallest normal set containing X.

Proof. TBA □

PROPOSITION 1.40. $\langle X\rangle = \left\langle \bigcup_{g\in G} gXg^{-1}\right\rangle \triangleleft G$

Proof. TBA $\square$

Ch1 exercises

```
var('q w r k')
P = PermutationGroup(['(1,2,3)','(2,3)'])
p = P.gen(0)
IsoZ = matrix(SR, 2, [[1,'n'],[0,1]])
a = matrix(SR, 3, 3, [[1, 'a', 'b'], [0, 1, 'c'], [0, 0, 1]])
K = matrix(SR, [[q,w+r],[0,q^2*r]])
A = matrix(2, [0,i, i,0])
B = matrix(2, [0,1, -1,0])
```

1-1. Using

$$Q := \langle A^2 = B^2, A^4 = 1, A^3 = BAB^{-1}\rangle = \left\langle \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$$

Show $\forall H \leq Q, H \triangleleft Q, \exists! a : oa = 2, Q \notin \mathbf{Ab}$

Proof.

$$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

so Q nonabelian. $AXA^{-1} = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$ $BXB^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$

$\square$

1-2. Using matrices in $GL(2, \mathbf{Z}[i])$, show $\left\langle a, b | a^4 = b^3 = 1\right\rangle \notin \mathbf{FinGp}$

Proof. $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \left\{(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\right\} \cong \mathbf{Z}$ $\square$

1-3. Show $G : |G| \in 2\mathbf{Z}$ has an element $a : oa = 2$.

Proof. oa — 2n, $\square$

1-4. Let $n = \sum_1^r n_i$, use lagrange to show $\prod_1^r n_i! | n!$

Proof. Consider $\square$

1-5. Let $N \triangleleft G : (G : N) = n$. Show $g^n \in N$, and that in nonnnormal subgroups this may not be true.

Proof. TBA $\square$

1-6. We say $m \in \mathbf{N}$ is the **exponent** of G if it's the smallest annihilator of G.
(a) Show $m = 2 \implies G \in \mathbf{Ab}$
(b) Let G be the following group. Verify that $m = p$ and $G \notin \mathbf{Ab}$

$$G := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right\} \subset GL(3, \mathbb{F}_p)$$

Proof. (a) $abab = e, a^{-1}b^{-1} = ab = ba$ □
(b) Show $a, b, c \in p\mathbf{Z}/$
TBA □

1-7. Two subgroups H and H' of a group G are said to be **commensurable** if $H \cap H'$ is of finite index in both H and H'. Show that commensurability is an equivalence relation on subgroups of G.

1-8. Show that a nonempty finite set with an associative binary operation satisfying the cancellation laws is a group. cancellation law: $an = am \implies n = m$