MATH 322: PROBLEMS FOR MASTERY

Part 1. Problems

1. Introduction and concerete examples

1.1. Congruences and modular arithmetic.

(1) Find all solutions to the congruence $5x \equiv 1\,(7)$.
(2) Evaluate:
  (a) $[3]_6 + [5]_6 + [9]_6$, $[3]_7 + [5]_7 + [9]_7$, $[2]_{13} \cdot [5]_{13} \cdot [7]_{13}$.
  (b) $([3]_8)^n$ (hint: start by finding $([3]_8)^2$).
(3) Linear equations.
  (a) Use Euclid's algorithm to solve $[5]_7 x = [1]_7$.
  (b) Solve $[5]_7 y = [2]_7$ by multiplying both sides by the element from (a).
  (c) Solve $\begin{cases} 2x+3y+4z &= 1 \\ x+y &= 3 \\ x+2z &= 6 \end{cases}$ in $\mathbb{Z}/7\mathbb{Z}$ (imagine all numbers are surrounded by brackets).

1.2. The symmetric group.

(1) Notation
  (a) Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 1 & 3 & 6 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$ in S_6. Compute $\sigma\tau$, $\tau\sigma$, σ^{-1}, τ^{-1}, $\sigma\tau\sigma^{-1}$.
  (b) Compute the cycle structure of the each of the permutations in part (a).
(2) (more cycles)
  (a) Decompose $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 7 & 1 & 4 & 8 & 2 & 6 \end{pmatrix}$ into cycles
  (b) Let $\tau = (12)$. Find the cycle structure of $\tau\sigma$, $\tau(\tau\sigma)$ and see how the cycles split and merge.
  (c) Let $\rho = (53478)$. Find the cycle structure of $\rho\sigma\rho^{-1}$.

2. Groups

2.1. Definitions: groups, subgroups, homomorphisms.

(1) Which of the following are groups? If yes, prove the group axioms. If not, show that an axiom fails.
  (a) The "half integers" $\frac{1}{2}\mathbb{Z} = \left\{\frac{a}{2} \mid a \in \mathbb{Z}\right\} \subset \mathbb{Q}$, under addition.
  (b) The "dyadic integers" $\mathbb{Z}[\frac{1}{2}] = \left\{\frac{a}{2^k} \mid a \in \mathbb{Z}, k \geq 0\right\} \subset \mathbb{Q}$, under addition.
  (c) The non-zero dyadic integers, under multiplication.
(2) [DF1.1.9] Let $F = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\} \subset \mathbb{R}$.
  (a) Show that $(F, +)$ is a group.
  (b) Show that $(F \setminus \{0\}, \cdot)$ is a group.
  RMK: Together with the distributive law, (a),(b) make F a *field*.
(3) Let G be a commutative group and let $k \in \mathbb{Z}$.
  (a) Show that the map $x \mapsto x^k$ is a group homomorphism $G \to G$.
  (b) Show that the subsets $G[k] = \left\{g \in G \mid g^k = e\right\}$ and $\left\{g^k \mid g \in G\right\}$ are subgroups.
  RMK For a general group G let $G^k = \left\langle \left\{g^k \mid g \in G\right\} \right\rangle$ be the subgroup generated by the kth powers. You have shown that, for a commutative group, $G^k = \left\{g^k \mid g \in G\right\}$.

Date: Last updated November 5, 2015.

2.2. **Cyclic groups; order of elements.**

(1) Let $\kappa = (123456)$ be an 6-cycle in S_n. Find the subgroup $\langle \kappa \rangle$.
(2) For each $n \in \mathbb{Z}$ find the subgroup $\langle n \rangle$.
(3) For each $\sigma \in S_4$ find the subgroup $\langle \sigma \rangle$.
(4) Let $\zeta = e^{2\pi i/n} \in \mathbb{C}$ be a root of unity of order n. Let $g = \begin{pmatrix} 0 & 1 \\ -1 & \zeta + \bar{\zeta} \end{pmatrix}$. Show that $g \in \mathrm{GL}_2(\mathbb{R})$ has order n (hint: diagonalize).
(5) Let $\sigma = \kappa_r \kappa_s \in S_n$ where κ_r, κ_s are disjoint cycles of length r, s respectively.
   (a) Show that $\sigma^k = \kappa_r^k \kappa_s^k$.
   (b) Show that $\sigma^k = \mathrm{id}$ iff $\kappa_r^k = \kappa_s^k = \mathrm{id}$ iff k is divisible by both r, s.
   (c) Show that the order of σ is the *least common multiple* of r, s.
   (d) (Number theory) Show that the least common multiple of r, s satisfies $\mathrm{lcm}(r,s) = \frac{rs}{\gcd(r,s)}$
   (e) Generalize (a),(b),(c) to the case where σ is a product of any number of disjoint cycles.

2.3. **The dihedral group and generalizations.**

(1) Let $D_{2n} = \left\{ c^\epsilon r^i \mid \epsilon \in \mathbb{Z}/2\mathbb{Z}, i \in \mathbb{Z}/n\mathbb{Z} \right\}$ and define $\left(c^\epsilon r^i\right) \cdot \left(c^\delta r^j\right) = c^{\epsilon+\delta} r^{\delta(i)+j}$ where

$$\delta(i) = \begin{cases} i & \delta = [0]_2 \\ -i & \delta = [1]_2 \end{cases}.$$

   (a) Show that $(D_{2n}, \cdot)$ is a group. Write e for its identity element.
      - This group is called the *dihedral group*. It is sometimes confusingly denoted D_n.
   (b) Let $c' = c^{[1]} r^{[0]}$ and $r' = c^{[0]} r^1$. Show that $(c')^2 = e$, $(r')^n = e$ and that $(c')^\epsilon (r')^i = c^\epsilon r^i$.
      - Accordingly we write c, r for these elements from now on.
   (c) Show that $cr \neq rc$ so that D_{2n} is non-commutative.
   (d) Show that every $g \in D_{2n}$ can be written as a product of elements from $S = \{c, r\}$.
      - We say the set $\{c, r\}$ *generates* D_{2n}.
   (e) Show that the map $i \mapsto r^i$ gives an isomorphism of $C_n \simeq (\mathbb{Z}/n\mathbb{Z}, +)$ and the subgroup H of D_{2n} consisting of powers of r.
   (f) Show that for every $g \in D_{2n}$ and $h \in H$ we have $ghg^{-1} \in H$.
   - We say H is *normal* in D_{2n}.

2.4. **Cosets and the index.**

(1) $H = \{\mathrm{id}, (12)\}$ and $K = \{\mathrm{id}, (123), (132)\}$ are two subgroups of S_3. Compute the coset spaces S_3/H, $H\backslash S_3$, S_3/K, $K\backslash S_3$.
(2) Let $H < G$ have index 2 and let $g \in G$. Show that $gHg^{-1} = \left\{ ghg^{-1} \mid h \in H \right\} = H$.
(3) If $H < G$ and $X \subset H$ is non-empty then $XH = H$. In particular, $hH = H$ for any $h \in H$.
(4) Let $K < H < G$ be groups with G finite. Use Lagrange's Theorem to show $[G:K] = [G:H]\,[H:K]$.

2.5. **Direct and semidirect products.**

(1) Let $G = \mathrm{GL}_2(\mathbb{R})$ be the group of 2×2 invertible matrices. We will consider the subgroups $B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \middle| ad \neq 0 \right\}$, $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in G \middle| ad \neq 0 \right\}$ and $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$.
   (a) Show that these really are subgroups with $A \simeq (\mathbb{R}^\times)^2 = \mathbb{R}^\times \times \mathbb{R}^\times$ and $N \simeq \mathbb{R}^+$. Evidently $N, A \subset B \subset G$.
   (b) Show that $B = N \rtimes A$(you need to show that $B = NA$, that $A \cap N = \{I\}$, and that $N \lhd B$).
   (c) Directly show that for any fixed a, d with $ad \neq 0$ we have $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} N = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid b \in \mathbb{R} \right\}$, demonstrating part of 2(c).

(2) Show that $D_{2n} = R \ltimes C$ where $R = \langle r \rangle \simeq C_2$, $C = \langle c \rangle \simeq C_n$.

For more semidirect products see also sheet on examples of group actions.

3. Group actions

3.1. Basic definitions.

(1) Label the elements of the four-group V by $1, 2, 3, 4$ in some fashion, and explicitely give the permutation corresponding to each element by the regular action.
(2) Repeat with S_3 acting on itself by conjugation (you will now have six permutations in S_6).
(3) Find the conjugacy classes in D_{2n}. Verify that the number of conjugacy classes equals the average size of a centralizer (average over elements of D_{2n}).
(4) Find the conjugacy classes of subgroups in S_4.
(5) Suppose the group G acts on sets X, Y.
  (a) Construct a natural action of G on the Cartesian product $X \times Y$, and check this is an action.
  (b) Find the orbits for the action of S_X on $X \times X$.

3.2. Conjugation.

(1) Find the conjugacy classes in D_{2n}.

4. p-groups and Sylow's Theorems

(1) The group $H = \left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \mid x, y, z \in F \right\}$ is called the *Heisenberg group* over the field F.
  (a) Show that H is a subgroup of $\mathrm{GL}_3(F)$ (you also need to show containment, that is that each element is an invertible matrix).
  (b) Show that $Z(H) = \left\{ \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mid z \in F \right\} \simeq (F, +)$.
  (c) Show that $H/Z(H) \simeq (F, +)^2$ via the map $\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \mapsto (x, y)$.
  (d) Show that H is non-commutative, hence is not isomorphic to the direct product $F^2 \times F$.
  (e) Suppose $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p odd. Then $\#H = p^3$ so that H is a p-group. Show that every element of $H(\mathbb{F}_p)$ has order p.
  (f) Find all conjugacy classes in H and write the class equation.
(2) Show that every group of order 35 is cyclic. Classify groups of order 10.

Part 2. Solutions

1. Introduction and concerete examples

1.1. Congruences and modular arithmetic.

(1) Note that $3\cdot 5 = 15 = 14+1$ so that $5\cdot 3 \equiv 1\,(7)$. Thus $5\cdot(3+7k) \equiv 5\cdot 3 \equiv 1\,(7)$ and $\{3+7k \mid k \in \mathbb{Z}\}$ are solutions. Conversely, if x is a solution then $5\,(x-3) \equiv 5x-1 \equiv 0\,(7)$ so $7|5\,(x-3)$. Since 7 is prime and does not divide 5, we must have $7|x-3$ so $x = 3+7k$ for some $k \in \mathbb{Z}$.

(2) Evaluate:

(a) $[3]_6+[5]_6+[9]_6 = [3+5+9]_6 = [14]_6 = [2]_6$, $[3]_7+[5]_7+[9]_7 = [3]_7$, $[2]_{13}\cdot[5]_{13}\cdot[7]_{13} = [70]_{13} = [5]_{13}$.

(b) $([3]_8)^2 = [9]_8 = [1]_8$. It follows that if $n = 2k+\epsilon$ we have $([3]_8)^n = ([3]_8)^{2k+\epsilon} = \left([3]_8^2\right)^k [3]_8^\epsilon$ and hence that

$$([3]_8)^n = \begin{cases} [1]_8 & n \text{ even} \\ [3]_8 & n \text{ odd} \end{cases}.$$

(3) Linear equations.

(a) See problem 1

(b) Suppose $[5]y \equiv [2]$ in $\mathbb{Z}/7\mathbb{Z}$. Multiplying by $[3]$ and using $[3][5] = [1]$ we conclude that $[y] \equiv [3][2] = [6]$. Conversely, $y \equiv [6]$ is a solution since $[5][6] = [30] = [2]$.

(c) We use Gaussian elimination:

$$\begin{cases} 2x+3y+4z & = 1 \\ x+y & = 3 \\ x+2z & = 6 \end{cases} \iff \begin{cases} y+4z & = 2 \\ x+y & = 3 \\ -y+2z & = 3 \end{cases} \iff \begin{cases} 6z & = 5 \\ x+y & = 3 \\ -y+2z & = 3 \end{cases} \iff$$

$$\begin{cases} z & = -5 = 2 \\ x+y & = 3 \\ y & = -3+2z \end{cases} \iff \begin{cases} z & = 2 \\ y & = 1 \\ x & = 3-y = 2 \end{cases}.$$

1.2. The symmetric group.

(1) Notation

(a) $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$, $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 5 & 2 & 4 & 1 \end{pmatrix}$, $\sigma^{-1} = \begin{pmatrix} 5 & 2 & 4 & 1 & 3 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 3 & 1 & 6 \end{pmatrix}$, $\tau^{-1} = \begin{pmatrix} 2 & 3 & 4 & 5 & 6 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$, $\sigma\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 1 & 2 & 5 \end{pmatrix}$.

(b) $\sigma = (1534)(2)(6)$, $\tau = (123456)$, $\sigma\tau = (1243)(56)$, $\tau\sigma = (16)(2354)$, $\sigma^{-1} = (4351)(2)(6)$, $\tau^{-1} = (654321)$, $\sigma\tau\sigma^{-1} = (136524)$.

(2)

(a) $\sigma = (154)(237)(68)$.

(b) $\tau\sigma = (154237)(68)$ and the two 3-cycles merged. $\tau(\tau\sigma) = \sigma$ and the 6-cycle 154237 breaks up to two 3-cycles.

(c) $\rho\sigma\rho^{-1} = (137)(248)(65)$.

2. Groups

2.1. Definitions.

(1) Which are groups?

(a) $\frac{1}{2}\mathbb{Z}$ is a group: $\left(\frac{a}{2}+\frac{b}{2}\right)+\frac{c}{2} = \frac{a+b+c}{2} = \frac{a}{2}+\left(\frac{b}{2}+\frac{c}{2}\right)$, $\frac{0}{2}+\frac{a}{2} = \frac{a}{2}$ and $\frac{-a}{2}+\frac{a}{2} = \frac{0}{2}$.

(b) $\mathbb{Z}\left[\frac{1}{2}\right]$ is a group.

(c) In $\mathbb{Z}[\frac{1}{2}] \setminus \{0\}$ note that $1\cdot x = x$ for all x, so if this was a group the identity element would be 1. Now consider $3 = \frac{3}{1}$; if this was a group there would be x such that $3x = 1$ so that $x = \frac{1}{3}$. But by unique factorization there is no way to write $\frac{1}{3}$ in the form $\frac{a}{2^k}$ where $k \geq 0$ – if $\frac{1}{3} = \frac{a}{b}$ then $b = 3a$ so b is divisible by 3.

(2)

(a) F is a non-empty subset of $\mathbb{R}$ closed under addition and subtraction, hence a subgroup.

(b) $1 = 1 + 0\sqrt{2} \in F \setminus \{0\} \subset \mathbb{R}^\times$ so it's enough to show closure. If $a + b\sqrt{2}, c + d\sqrt{2} \neq 0$ then $\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = (ac + 2bd) + (ad + bc)\sqrt{2} \in F$ and the product is non-zero since $\mathbb{R}$ is a field. Also $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{\left(a+b\sqrt{2}\right)\left(c-d\sqrt{2}\right)}{c^2-2d^2} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2} \in F \setminus \{0\}$ since the denominator is a non-zero rational number (were $c^2 - 2d^2 = 0$ it would mean $c^2 = 2d^2$ and this violates unique factorization since the number of factors of 2 of this number is odd on the right, even on the left).

2.2. Cyclic groups.

(1) $\kappa^2 = (135)(246)$, $\kappa^3 = (14)(25)(36)$, $\kappa^4 = (153)(264)$, $\kappa^5 = (165432)$ and $\kappa^6 = \mathrm{id}$ so $\langle\kappa\rangle = \{\mathrm{id}, (135)(246), (14)(25)(36), (153)(264), (165432)\}$.

(2) In the first class we shows that $\langle n\rangle = n\mathbb{Z}$.

(3) Only one representative from each cycle structure is given. $\langle \mathrm{id}\rangle = \{\mathrm{id}\}$, $\langle(12)\rangle = \{\mathrm{id}, (12)\}$, $\langle(123)\rangle = \{\mathrm{id}, (123), (132)\}$, $\langle(1234)\rangle = \{\mathrm{id}, (1234), (13)(24), (1432)\}$, $\langle(12)(34)\rangle = \{\mathrm{id}, (12)(34)\}$.

(4) The matrix g is real and has characteristic polynomial $z^2 - (\operatorname{tr} g)z + (\det g) = z^2 - (\zeta + \bar\zeta)z + 1 = (z - \zeta)(z - \bar\zeta)$ since $\zeta\bar\zeta = 1$. We conclude that there is $S \in \mathrm{GL}_2(\mathbb{C})$ such that $g = S\begin{pmatrix}\zeta & \\ & \zeta^{-1}\end{pmatrix}S^{-1}$ ($\zeta^{-1} = \bar\zeta$). We show by induction that $g^k = S\begin{pmatrix}\zeta^k & \\ & \zeta^{-k}\end{pmatrix}S^{-1}$: for $k = 0$ this is clear, and if true for k then

$$\begin{aligned} g^{k+1} &= g^k \cdot g = S\begin{pmatrix}\zeta^k & \\ & \zeta^{-k}\end{pmatrix}S^{-1}S\begin{pmatrix}\zeta & \\ & \zeta\end{pmatrix}S^{-1} \\ &= S\begin{pmatrix}\zeta^k & \\ & \zeta^{-k}\end{pmatrix}\begin{pmatrix}\zeta & \\ & \zeta\end{pmatrix}S^{-1} = S\begin{pmatrix}\zeta^{k+1} & \\ & \zeta^{-k-1}\end{pmatrix}S^{-1}. \end{aligned}$$

Thus, when $k < n$ g^k has eigenvalues $\zeta^k, \zeta^{-k} \neq 1$ so isn't the identity matrix while $g^n = S\begin{pmatrix}1 & \\ & 1\end{pmatrix}S^{-1} = I$. It follows that g has order n exactly.

2.3. The dihedral group.

(1) Let $D_{2n} = \left\{c^\epsilon r^i \mid \epsilon \in \mathbb{Z}/2\mathbb{Z}, i \in \mathbb{Z}/n\mathbb{Z}\right\}$ and define $\left(c^\epsilon r^i\right) \cdot \left(c^\delta r^j\right) = c^{\epsilon+\delta} r^{\delta(i)+j}$ where

$$\delta(i) = \begin{cases} i & \delta = [0]_2 \\ -i & \delta = [1]_2 \end{cases}.$$

(a) For associativity, we start by noting that $\delta(a+b) = \delta(a)+\delta(b)$ for any $a, b \in \mathbb{Z}/n\mathbb{Z}$ and regardless of the value of δ, and that $(\delta + \eta)(i) = \delta(\eta(i))$ f or any $\delta, \eta \in \mathbb{Z}/2\mathbb{Z}$ and $i \in \mathbb{Z}/n\mathbb{Z}$. We thus have:

$$\begin{aligned} \left(\left(c^\epsilon r^i\right)\cdot\left(c^\delta r^j\right)\right)\cdot\left(c^\eta r^k\right) &= \left(c^{\epsilon+\delta} r^{\delta(i)+j}\right)\cdot\left(c^\eta r^k\right) \\ &= c^{(\epsilon+\delta)+\eta} r^{\eta(\delta(i)+j)+k} \\ &= c^{\epsilon+\delta+\eta} r^{\eta(\delta(i))+\eta(j)+k} \end{aligned}$$

and

$$\begin{aligned} \left(c^\epsilon r^i\right)\cdot\left(\left(c^\delta r^j\right)\cdot\left(c^\eta r^k\right)\right) &= \left(c^\epsilon r^i\right)\cdot\left(c^{\delta+\eta} r^{\eta(j)+k}\right) \\ &= c^{\epsilon+(\delta+\eta)} r^{(\delta+\eta)(i)+\eta(j)+k} \\ &= c^{\epsilon+\delta+\eta} r^{\eta(\delta(i))+\eta(j)+k}. \end{aligned}$$

For identity, $\left(c^{[0]}r^{[0]}\right)\cdot\left(c^\delta r^j\right) = c^{[0]+\delta} r^{\delta(0)+j} = \left(c^\delta r^j\right)$. To invert $\left(c^\delta r^j\right)$, if $\delta = [0]$ them $\left(c^{[0]}r^{-j}\right)\cdot\left(c^{[0]}r^j\right) = c^{[0]}r^{-j+j} = c^{[0]}r^{[0]}$ while if $\delta = [1]$ then

$$\left(c^{[1]}r^j\right)\cdot\left(c^{[1]}r^j\right) = c^{[1]+[1]}r^{-j+j} = c^{[0]}r^{[0]}.$$

(b) We show by induction that $(r')^k = c^{[0]_2} r^{[k]_n}$ for all $k \geq 0$. This is clear for $k = 0$, and if true for k then

$$(r')^{k+1} = \left(c^{[0]_2} r^{[k]_n}\right) \cdot \left(c^{[0]_2} r^{[1]_n}\right) = \left(c^{[0]_2+[0]_2} r^{[k]_n+[1]_n}\right) = \left(c^{[0]_2} r^{[k+1]_n}\right) .$$

In particular, we see that $(r')^k \neq e$ for $0 < k < n$ while $(r')^n = e$. Thus r' has order n. Finally,

$$(c')^{\epsilon} (r')^k = \left(c^{\epsilon} r^{[0]}\right) \cdot \left(c^{[0]_2} r^{[k]_n}\right) = c^{\epsilon} r^{[0]+[k]} = \left(c^{\epsilon} r^{[k]}\right) .$$

(c) By the formula for multiplicatio, $rc = cr^{[-1]_n} \neq cr$ (if $n > 2$).
(d) This is part (b)
(e) By definition of multiplication in D_{2n}, the map $i \to \left(c^{[0]} r^i\right)$ is a bijective group homomorphism.
(f) The subgroup H is commutative, so if $g \in H$ we have $ghg^{-1} = gg^{-1}h = h$. Otherwise, $g = cr^j$ for some j and then for $h = r^i$ we have

$$\begin{aligned} ghg^{-1} &= cr^j r^i r^{-j} c \\ &= cr^j cr^0 = r^{-j} = h^{-1} \end{aligned}$$

by definition of multiplication in D_{2n}. We conclude that if $g \notin H$ then the map $h \mapsto ghg^{-1}$ is the map $h \mapsto h^{-1}$ which exchanges elements and their inverses, so preserves H since subgroups are closed under taking inverses.

2.4. **Cosets and the index.**

(1) $S_3/H = \{\{\mathrm{id}, (12)\}, \{(23), (132)\}, \{(13), (123)\}\}$, $H\backslash S_3 = \{\{\mathrm{id}, (12)\}, \{(23), (123)\}, \{(13), (132)\}\}$. $S_3/K = K\backslash S_3 = \{\{\mathrm{id}, (123), (132)\}, \{(12), (23), (13)\}\}$.
(2) By assumption G/H consists of two cosets. Since H itself is one of them and the cosets cover G, it follows that $G - H$ is the other left coset. But $H\backslash G$ is also of size 2, and it also follows that $G - H$ is also the other right coset. Now let $g \in G$. If $g \in H$ then H is the left coset g belongs to, so $gH = H$. Also $g^{-1} \in H$ and H is the right coset g^{-1} belongs to, so $gHg^{-1} = (gH)g^{-1} = Hg^{-1} = H$. Otherwise, $g \notin H$ and then $gH = G - H$ and $Hg = G - H$ so $gH = Hg$. Multiplying on the right by g^{-1} we find

$$gHg^{-1} = Hgg^{-1} = H .$$

(3) Since H is closed under multiplication, $XH \subset H$. Conversely fix $x \in X$. Then for any $h \in H$ we have $x^{-1}h \in H$ and hence $h = x(x^{-1}h) \in XH$, so that $H \subset XH$.
(4) We have $[G : K] = \frac{\#G}{\#K} = \frac{\#G}{\#H} \cdot \frac{\#H}{\#K} = [G : H]\,[H : K]$.

2.5. **Direct and semidirect products.**

(1)

(a) Let $f \colon \mathbb{R}^+ \to \mathrm{GL}_2(\mathbb{R})$ be the map $f(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. This is evidently injective. It is also a group homomorphism $\mathbb{R}^+ \to \mathrm{GL}_2(\mathbb{R})$:

$$f\left(b_1 + b'\right) = \begin{pmatrix} 1 & b + b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = f(b) f(b')$$

so its image N is a subgroup, isomorphic to $\mathbb{R}^+$. Similarly, let $g \colon \left(\mathbb{R}^\times\right)^2 \to \mathrm{GL}_2(\mathbb{R})$ be given by $g(a, d) = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. This is evidently injective (so a bijection on its image) and easily verified to be a group homomorphism. It follows that the image A is a subgroup isomorphism to $\left(\mathbb{R}^\times\right)^2$. That B is a subgroup will follow from (b) and 2(b).

(b) By problem 2 it is enough to check that A normalizes N and that $A \cap N = \{I\}$. The last one is clear: if for $x \in \mathrm{GL}_2(\mathbb{R})$ there are a, b, d such that $x = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ then $b = 0$,

$a = d = 1$ and $x = I_2$. For the other claim, let $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in N$ and $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in A$. Then $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} a & ab \\ 0 & d \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix} = \begin{pmatrix} 1 & abd^{-1} \\ 0 & 1 \end{pmatrix} \in N$, so A normalizes N.

(c) Set $X = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid b \in \mathbb{R} \right\}$. Then for any $b \in \mathbb{R}$ we have $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ab \\ 0 & d \end{pmatrix} \in X$ so $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} N \subset X$. Conversely, we have $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix} \in \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} N$ so $X \subset \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} N$.

3. Group actions

3.1. **Basic definitions.**

(1) Say the elements are e, a, b, ab, numbered $1, 2, 3, 4$. Then e corresponds to the identity, a corresponds to $(12)(34)$, b corresponds to $(13)(24)$ and ab to $(14)(23)$.

(2) Number the elements 1 to 6 along $\mathrm{id}, (12), (23), (31), (123), (132)$. Then $\mathrm{id} \mapsto \mathrm{id}$, $(12) \mapsto (34)(56)$, $(23) \mapsto (24)(56)$, $(13) \mapsto (23)(56)$, $(123) \mapsto (234)$, $(132) \mapsto (243)$.

(3) We consider the classes of r^i and cr^i sepatately.

(a) In the first case, since $\langle r \rangle$ is commutative, there is no point in conjugating by r^j and it's enough to find

$$\left(cr^j\right) r^i \left(cr^j\right)^{-1} = cr^i c^{-1} = r^{-i} .$$

We conclude that the conjugacy class of r^i is $\left\{r^i, r^{-i}\right\}$. This has size 2 unless $i = -i$, which happens when $i = [0]$ or when $i = \left[\frac{n}{2}\right]$ (the latter only when n is even).

(b) We know that any conjugate of cr^i is of the form cr^k for some k since we know the conjugates of the elements of the form r^k. Next,

$$r^j cr^i r^{-j} = cr^{i-2j}$$

so we see that the conjugacy class of cr^i includes at least all cr^k where $k - i \in 2\mathbb{Z}/n\mathbb{Z}$. When n is odd, 2 is invertible so every k is of this form and $\left\{cr^i\right\}_{i \in \mathbb{Z}/n\mathbb{Z}}$ are all one class. When n is even, we note that

$$\left(cr^j\right)\left(cr^i\right)\left(r^{-j}\right) = cr^{-i-2j}$$

but $i - (-i - 2j) = 2i + 2j$ is a multiple of 2, so we don't get any new conjugate. We conclude that when n is even we have the two classes

$$\left\{cr^{2i}\right\}_{i \in \mathbb{Z}/n\mathbb{Z}}, \left\{cr^{[1]+2i}\right\}_{i \in \mathbb{Z}/2\mathbb{Z}} .$$

(4) S_4 has order 24, so its subgroups can have orders $1, 2, 3, 4, 6, 8, 12, 24$.

(a) At orders $1, 24$ there can be only one subgroup.

(b) A subgroup of order 2 must contain a unique element of order 2, which can have the cycle structure (12) or $(12)(34)$ and these aren't conjugate, so there are two conjugacy classes, represented by $\langle (12) \rangle$, $\langle (12)(34) \rangle$.

(c) A subgruop of order 3 is generated by an element of order 3, which must have cycle structure (123) so there is one conjugacy class, represented by $\langle (123) \rangle$.

(d) A subgroup of order 4 is either isomorphic to C_4, in which case it has a generator of order 4, conjugate to (1234) or isomorphic to V, in which case every element has order 2. If we contain (12) then the only elements of order 2 which commute with it are (34), and $(12)(34)$, so this must be the group. Otherwise we note that $N = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ form a subgroup isomorphic to V, so the classes are the one reprented by $\{\mathrm{id}, (12), (34), (12)(34)\}$ and the only consisting of the normal subgroup N.

(e) By Cauchy's Theorem, a subgroup of order 6 will contain an element of order 3, so up to conjugacy contains $\{\mathrm{id}, (123), (132)\}$. It will also contain an element of order 2. Adding $(12), (13)$ or (23) gives $S_{\{1,2,3\}} \simeq S_3$ and this is clearly one conjugacy class. Adding $(14), (24), (34)$ (they are all conjugacy by (123)) gives all of S_4 so this isn't possible. The elements $(12)(34), (13)(24), (23)(14)$

are all conjguate by (123) and adding them will give a copy of V so order divisible by 4. We conclude that $\{S_{\{1,2,3\}}, S_{\{1,2,4\}}, S_{\{1,3,4\}}, S_{\{2,3,4\}}\}$ is the conjugacy class at order 6.

(f) There is no subgroup of order 8.

(g) By the reasoning of part (e), at order 12 we have exactly A_4 generated by (123) and (12) (34).

(5) Suppose the group G acts on sets X, Y.

(a) Define $g \cdot (x, y) = (g \cdot x, g \cdot y)$. Then $e \cdot (x, y) = (e \cdot x, e \cdot y) = (x, y)$ and

$$g \cdot (h \cdot (x, y)) = g \cdot (h \cdot x, h \cdot y) = (g \cdot (h \cdot x), g \cdot (h \cdot y)) = ((gh) \cdot x, (gh) \cdot y) = (gh) \cdot (x, y) \,.$$

(b) We have $\sigma \cdot (x, x) = (\sigma(x), \sigma(x))$. Since for all $x, x' \in X$ there is σ with $\sigma(x) = x'$, we conclude that one orbit is the *diagonal* $\{(x, x) \mid x \in X\}$. The key idea is to see that we can extent partial permutations: if $x \neq y$, $x' \neq y'$ then there is σ with $\sigma(x) = x'$, $\sigma(y) = y'$.

4. p-groups and Sylow's Theorems

4.1. p-groups.

(1) For a field F let $H = \left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \mid x, y, z \in F \right\}$ is called the *Heisenberg group* over F.

(a) We have $\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & z' \\ & 1 & y' \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + x' & z + z' + xy' \\ & 1 & y + y' \\ & & 1 \end{pmatrix}$ (so this is closed under matrix multiplication). In particular, $\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & -x & xy - z \\ & 1 & -y \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$ so each element of $H(F)$ is invertible (hence $H(F) \subset \mathrm{GL}_3(F)$), and the inverse belongs to $H(F)$. $H(F)$ contains the identity matrix (let $x = y = z = 0$) so it is non-empty.

(b) $\begin{pmatrix} 1 & x' & z' \\ & 1 & y' \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + x' & z + z' + x'y \\ & 1 & y + y' \\ & & 1 \end{pmatrix}$. Fixing x, y, z we see that

$$\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & z' \\ & 1 & y' \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & x' & z' \\ & 1 & y' \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}$$

for all x', y', z' iff $x'y = xy'$ for all x', y'. If $x = y = 0$ this is of course an identity, but if one of x, y is non-zero then choosing one of x', y' to be zero and the other 1 makes one of $x'y, xy'$ zero and the other non-zero, showing that $\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}$ is non-central. To see that $Z(H) \simeq F^+$ check that the bijection $z \mapsto \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix}$ is a group homomorphism.

(c) Consider the map $f\left(\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}\right) = (x, y)$. The first calculation of (a) shows that

$$\begin{aligned} f\left(\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & z' \\ & 1 & y' \\ & & 1 \end{pmatrix}\right) &= f\left(\begin{pmatrix} 1 & x + x' & z + z' + xy' \\ & 1 & y + y' \\ & & 1 \end{pmatrix}\right) \\ &= (x + x', y + y') = (x, y) + (x', y') \\ &= f\left(\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}\right) + f\left(\begin{pmatrix} 1 & x' & z' \\ & 1 & y' \\ & & 1 \end{pmatrix}\right), \end{aligned}$$

that is that f is a group homomorphism $H(F) \to (F^+)^2$. The kernel is exactly the set of elements such that $x = y = 0$, that is the center. The first isomorhpism theorem then says that f induces an isomorphism between $H/\operatorname{Ker}(f) = H/Z(H)$ and its image. But since all x, y are possible, f is surjective and the claim follows.

(d) We saw that $Z(H) \neq H$.

(e) We show by that for $k \geq 0$, $\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & kx & kz + \binom{k}{2}xy \\ & 1 & ky \\ & & 1 \end{pmatrix}$. This is clear for $k = 0$ (both sides are the identity). We continue by induction:

$$\begin{aligned}
\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}^{k+1} &= \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}^k \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}^1 \\
&= \begin{pmatrix} 1 & kx & kz + \binom{k}{2}xy \\ & 1 & ky \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & (k+1)x & kz + \binom{k}{2}xy + kxy \\ & 1 & (k+1)y \\ & & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & (k+1)x & kz + \binom{k+1}{2}xy \\ & 1 & (k+1)y \\ & & 1 \end{pmatrix}
\end{aligned}$$

since $\binom{k}{2} + k = \binom{k}{2} + \binom{k}{1} = \binom{k+1}{2}$. In particular, for $k = p$ we get

$$\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & px & pz + p\frac{p+1}{2}xy \\ & 1 & py \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}.$$