1. Let A be a set. $+_A : P(A) \times P(A) \to P(A)$ defined as $(B, C) \mapsto (B \cup C)\setminus(B \cap C)$. Then:

   (a) Show that $(P(A), +_A)$ is an abelian group.

   (b) Let $A' \subseteq A$, show that $B \mapsto B \cap A'$ is a homomorphism from $(P(A), +_A)$ to $(P(A'), +_{A'})$.

   (c) Let $F = \{B \in P(A) : B \text{ is finite or } A\setminus B \text{ is finite}\}$. Show that F is a subgroup of $(P(A), +_A)$.

(a). Pf.

associativity. given $R.\ S.\ T \in P(A)$

denote $A\setminus R.\ A\setminus S.\ A\setminus T$ by $\bar{R}.\ \bar{S}.\ \bar{T}$. respectively

$$(R+_A S)+_A T = ((R\cup S)\setminus(R\cap S))+_A T$$

$$=((R\cup S)\cap(\bar{R}\cup\bar{S}))+_A T \quad \text{(de Morgan)}$$

$$=((R\cap\bar{R})\cup(S\cap\bar{R})\cup(\bar{S}\cap R)\cup(S\cap\bar{S}))+_A T$$

$$=((S\cap\bar{R})\cup(R\cap\bar{S}))+_A T$$

$$=(((\bar{R}\cap S)\cup(R\cap\bar{S}))\cap\bar{T})\cup(((R\cup\bar{S})\cap(\bar{R}\cup S))\cap T)$$

$$=(\bar{R}\cap S\cap\bar{T})\cup(R\cap\bar{S}\cap\bar{T})\cup(\bar{R}\cap\bar{S}\cap T)\cup(R\cap S\cap T)$$

$$R+_A(S+_A T) = R+_A((S\cap\bar{T})\cup(\bar{S}\cap T))$$

$$=(R\cap((\bar{S}\cup T)\cap(S\cup\bar{T})))\cup(\bar{R}\cap((S\cap\bar{T})\cup(\bar{S}\cap T)))$$

$$=(R\cap S\cap T)\cup(R\cap\bar{S}\cap\bar{T})\cup(\bar{R}\cap S\cap\bar{T})\cup(\bar{R}\cap\bar{S}\cap T)$$

$$=(R+_A S)+_A T$$

identity. it can be checked that $e_{P(A)} = \phi \in P(A)$

$$\forall S \in P(A) \quad S +_A \phi = (S \cup \phi) \setminus (S \cap \phi)$$
$$= (\phi \cup S) \setminus (\phi \cap S)$$
$$= \phi +_A S$$
$$= S.$$

so ϕ is the identity in $(P(A), +_A)$

inverse. it can be checked that S is an inverse of itself for all $S \in P(A)$.

$$S +_A S = (S \cup S) \setminus (S \cap S) = \phi = e_{P(A)}$$

abelian. $\forall S, T \in P(A)$

$$S +_A T = (S \cup T) \setminus (S \cap T)$$
$$= (T \cup S) \setminus (T \cap S)$$
$$= T +_A S$$

so by definition. $(P(A), +_A)$ is an abelian group. $\square$.

(b). Pf. denote this function by $f: B \to A' \cap B$

Firstly I'll show that $(P(A'), +_{A'})$ is a group.

This instantly follows from the fact that A is arbitrary.

$\forall B, C \in \mathcal{P}(A)$

$$
\begin{aligned}
f(B +_A C) &= (B +_A C) \cap A' \\
&= \big((B \cap (A \setminus C)) \cup ((A \setminus B) \cap C)\big) \cap A' \\
&= \big((A' \cap B) \cap (A' \setminus C)\big) \cup \big((A' \setminus B) \cap (A' \cap C)\big) \\
&= \big((A' \cap B) \cap (A' \setminus (A' \cap C))\big) \cup \big((A' \setminus (A' \cap B)) \cap (A' \cap C)\big) \\
&= (A' \cap B) +_{A'} (A' \cap C) \\
&= f(B) +_{A'} f(C)
\end{aligned}
$$

So $B \mapsto B \cap A'$ is a homomorphism from $(\mathcal{P}(A), +_A)$ to $(\mathcal{P}(A'), +_{A'})$

$\square$

(c). Pf.

(i) identity. $e_{\mathcal{P}(A)} = \phi \in F$ by definition.

(ii) closed under operator. $\forall S, T \in F$

$$
\begin{aligned}
S +_A T &= (S \cup T) \setminus (S \cap T) \qquad \text{let } \bar{S} := A \setminus S,\ \bar{T} := A \setminus T \\
&= (S \cap \bar{T}) \cup (\bar{S} \cap T)
\end{aligned}
$$

observe that $|S \cap \bar{T}| \leq |S|$ $|\bar{S} \cap T| \leq |T|$

so $|S +_A T| \leq |S| + |T| < \infty$

$\Rightarrow S +_A T \in F$

(iii) existence of inverse.

$\forall s \in F$. s itself is the inverse.

$$s +_A s = \phi = e_{P(A)} = e_F.$$

by definition of subgroup. $F \leqslant P(A)$ $\square$.

2. Let G be a group, H_1, H_2 be two subgroups.

   (a) Show that $H_1 \cap H_2 \leq G$.

   (b) Show that $H_1 \cup H_2 \leq G$ iff $H_1 \leq H_2$ or $H_2 \leq H_1$.

   (c) Let G be the group of integers and the group operation is addition. Write down two subgroups whose union is no longer a subgroup.

(a). Pf. suppose a group operator of G is $*$. $(G, *)$ is a group.

identity: since $H_1 \leqslant G$. $H_2 \leqslant G$. denote identity of G by e_G.

$e_G \in H_1$. $e_G \in H_2$

So $e_G \in H_1 \cap H_2$

closed under $*$:

for $i = 1.2$. $\forall x.y \in H_i$ $x * y \in H_i$

so take $\forall x.y \in H_1 \cap H_2$.

$$\left.\begin{array}{l} x \in H_1 .\ y \in H_1 \Rightarrow x * y \in H_1 \\ x \in H_2 .\ y \in H_2 \Rightarrow x * y \in H_2 \end{array}\right\} \Rightarrow x * y \in H_1 \cap H_2$$

existence of inverse.

$\forall x \in H_1 \cap H_2 \subset G$

$H_1 \leq G \Rightarrow x^{-1} \in H_1$

$H_2 \leq G \Rightarrow x^{-1} \in H_2$

since $x \in G$. x^{-1} is unique.

so $x^{-1} \in H_1 \cap H_2$.

so $H_1 \cap H_2 \leq G$. $\square$

(b). pf. Suppose $H_1 \leq H_2$.

by definition $H_1 \subset H_2$. $H_1 \cup H_2 = H_2 \leq G$.

Suppose $H_1 \cup H_2 \leq G$.

by definition (i). $e_G \in H_1 \cup H_2$

(ii) $\forall x, y \in H_1 \cup H_2$. $x * y \in H_1 \cup H_2$

(iii) $\forall x \in H_1 \cup H_2$. $x^{-1} \in H_1 \cup H_2$

If $H_1 = H_2$ then the proof is done

If $H_1 \neq H_2$. W.L.O.G suppose $H_2 \setminus H_1 \neq \phi$.

I'll show that under this condition, $H_1 \setminus H_2 = \phi$

if $H_1 \setminus H_2 \neq \phi$ (this is my assumption)

pick $x_1 \in H_1 \setminus H_2 \subset H_1 \cup H_2$.

if $x_1^{-1} \in H_2$. since H_2 is a group . $H_2 \leq G$

$x_1 = (x_1^{-1})^{-1} \in H_2$ contradiction

so $x_1^{-1} \in H_1 \setminus H_2$. (I)

similarly $\forall x_2 \in H_2 \setminus H_1$ $x_2^{-1} \in H_2 \setminus H_1$

pick $x_1 \in H_1 \setminus H_2$. $x_2 \in H_2 \setminus H_1$

since $x_1 . x_2 \in H_1 \cup H_2 \leq G$ $x_1 * x_2 \in H_1 \cup H_2$

if $x_1 * x_2 = y \in H_1$

$x_1^{-1} * x_1 * x_2 = x_2 = x_1^{-1} * y \in H_1$ (by I)

but by assumption $x_2 \in H_2 \setminus H_1$. contradiction.

so $x_1 * x_2 \notin H_1$ similarly $x_1 * x_2 \notin H_2$

so $H_1 \cup H_2$ is not closed under $*$. thus not a group.

Contradiction.

so my assumption is false. i.e. $H_1 \setminus H_2 = \phi$.

Next I'll show that at this time $H_1 \leq H_2$

since $H_1 \setminus H_2 = \phi$ $H_2 \setminus H_1 \neq \phi$

$H_1 \subset H_1 \cup H_2 = H_2$

consider $x \in H_1$. $x * e_{H_1} = x = x * e_{H_2}$

by cancellation law. $e_{H_1} = e_{H_2}$

since H_1 itself is a group. the other two rules are automatically satisfied.

so $H_1 \leq H_2$ (or $H_2 \leq H_1$)

$\square$

(c). Solution. $\langle 2\rangle, \langle 3\rangle$ are subgroups of $(\mathbb{Z},+)$ respectively.

but $2 \in \langle 2\rangle$. $3 \in \langle 3\rangle$

$$2+3=5 \notin (\langle 2\rangle \cup \langle 3\rangle).$$

3. Show that the set of $n \times n$ matrices with integer entries and determinant 1 form a group under matrix multiplication. (These groups are denoted as $SL(n,\mathbb{Z})$).

Pf. $\forall A.B \in SL(n.\mathbb{Z})$ with determinant 1.

$$|AB| = |A|\cdot|B| = 1\times 1 = 1$$

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj} \in \mathbb{Z} \text{ is obvions.}$$

So $SL(n.\mathbb{Z})$ is closed under matrix multiplication.

(i). Identity. $I=\mathrm{diag}(\underbrace{1,1,\cdots,1}_{n}) \in SL(n.\mathbb{Z})$ is the identity.

$\forall M \in SL(n.\mathbb{Z})$. $M\cdot I = I\cdot M = M$

(ii). Associativity. $\forall M.N.P \in SL(n.\mathbb{Z})$.

$$(M\cdot N)\cdot P = M\cdot(N\cdot P)$$

follows from the definition of matrix multiplication.

(iii). Inverse.

$\forall A \in SL(n.\mathbb{Z})$. $A\cdot A^* = A^*\cdot A = |A|\cdot I = I$

by definition $A^*_{ij} = (-1)^{i+j} M_{ij}$

where M_{ij} is the (i,j)-minor of A

by definition $M_{ij} \in \mathbb{Z}$

also $|A| \cdot |A^*| = |I| = 1 \Rightarrow |A^*| = 1$.

so A^* is the inverse of A in $SL(n. \mathbb{Z})$.

By definition $SL(n. \mathbb{Z})$ is a group under matrix multiplication.

$\square$

4. Let G be a group, show that G has only the identity element iff for any group H, $Hom(H, G)$ has exactly one element.

Pf. if G is trivial. obviously the only possible map should be

$$f: H \to G$$
$$x \mapsto e$$

if $|Hom(H. G)| = 1$.

If G has more than 1 element,

pick $g \in G$ where g is not the identity. Let $H = (\mathbb{Z}, +)$

$f_1: x \mapsto e$ (trivial homomorphism) and $f_2: n \mapsto g^n$

are two different mappings when $|G| \neq 1$.

$f_2(n_1 + n_2) = g^{n_1+n_2} = g^{n_1} * g^{n_2} = f_2(n_1) * f_2(n_2)$

so $\left| \mathrm{Hom}(G, G) \right| \geq 2$ contradiction.

so G has only one element. and it has to be the identity. $\square$

5. Show that for any group G, any $g \in G$, there is a unique group homomorphism from $(\mathbb{Z}, +)$ to G, sending 1 to g.

Pf. Denote group G by $(G, *)$

let $f \in \mathrm{Hom}(\mathbb{Z}, G)$ with $f(1)=g$, $\forall x.y \in \mathbb{Z}$ $f(x+y) = f(x) * f(y)$

let $y=1$ $f(x+1) = f(x) * f(1) = f(x) * g$

If $g = e_G$ $\forall x \in \mathbb{Z}$ $f(x+1) = f(x)$

so $f: \mathbb{Z} \to G$ is unique (and obviously exists).
$x \mapsto e_G$

If $g \neq e_G$. $\forall x \in \mathbb{Z}. f(x+1) = f(x) * g$

so $f(n) = g^n$ $(n \in \mathbb{Z})$ is such a homomorphism

if in this case $\exists h \in \mathrm{Hom}(\mathbb{Z}, G)$ s.t. $h(x+1) = h(x) * g$
$(\forall x \in \mathbb{Z})$

let $x=0$ $f(0) = h(0) = g$

It can be easily shown by induction that $f = h$.

(Note. $\forall m \in \mathbb{N}$. $g^m := g * g * \cdots * g$ (m times)

$g^{-m} := g^{-1} * g^{-1} * \cdots * g^{-1}$ (m times)).

$\square$.

6. Let M be a set, $* : M \times M \to M$ be a function, such that for any $a, b, c \in M$, $*(a, *(b, c)) = *(*(a, b), c)$, $*(a, b) = *(b, a)$, and there is an element $e \in M$ such that for any $a \in M$, $*(e, a) = *(a, e) = a$. Let $\cdot : (M \times M) \times (M \times M) \to M \times M$ be $((a, b), (c, d)) \mapsto (*(a, c), *(b, d))$, $\sim$ a relation on $M \times M$ defined as $\sim = \{((a, b), (c, d)) \in (M \times M) \times (M \times M) :$ there exists $k \in M, *(*(a, d), k) = *(*(b, c), k)\}$

   (a) Show that $\sim$ is an equivalence relation.

   (b) Let $G = (M \times M)/\sim$. Show that $([a], [b]) \mapsto [\cdot(a, b)]$ is a function from $G \times G$ to G. Denote it as $\cdot'$.

(a) Pf. Denote $*(x.y)$ by $x * y$

$(a.b) \sim (c.d)$ iff $\exists k \in M \quad (a*d)*k = (b*c)*k$

reflexity. $\forall (x.y) \in M \times M$. take $k = e$

$$(x*y)*e = (x*y)*e \Rightarrow (x.y) \sim (x.y)$$

symmetry. $\forall (x_1.y_1).(x_2.y_2) \in M \times M$

$$\begin{aligned}(x_1.y_1) \sim (x_2.y_2) &\Leftrightarrow (x_1 * y_2) * e = (x_2 * y_1) * e \\ &\Leftrightarrow (x_2 * y_1) * e = (x_1 * y_2) * e \\ &\Leftrightarrow (x_2.y_2) \sim (x_1.y_1)\end{aligned}$$

transitivity. $\forall (x_1.y_1)\ (x_2.y_2)\ (x_3.y_3) \in M \times M$

$$(x_1.y_1) \sim (x_2.y_2) \wedge (x_2.y_2) \sim (x_3.y_3)$$

$\Leftrightarrow (x_1 * y_2) * e = (x_2 * y_1) * e. \quad (x_2 * y_3) * e = (x_3 * y_2) * e.$

$\Rightarrow y_3 * (x_1 * y_2) * e = y_3 * (x_2 * y_1) * e$

$$\Rightarrow \quad y_3 * (x_1 * y_2) = y_3 * (x_2 * y_1)$$
$$= (x_2 * y_3) * y_1$$
$$= (x_3 * y_2) * y_1$$
$$(y_3 * x_1) * y_2 = (x_3 * y_1) * y_2$$
$$\Leftrightarrow \quad (x_1, y_1) \sim (x_3, y_3)$$

$\square$

(b). Pf. Given $A = [a] \in G$. $B = [b] \in G$.

$$\cdot'(A, B) = [\cdot(a, b)] = [(x_a * x_b, y_a * y_b)]$$
$$= \{(x, y) \in M \times M \mid \exists k \in M.\ x_a * x_b * y * k = x * y_a * y_b * k\}$$

We only need to show that "$\cdot'$" is well-defined.

If $A_1 = [a_1] = [a_2] = A_2 \in G$. $B_1 = [b_1] = [b_2] = B_2 \in G$.

$A_1 \cdot' B_1 = \{(x, y) \in M \times M \mid (x, y) \sim (x_{a_1} * x_{b_1}, y_{a_1} * y_{b_1})\}$

$A_2 \cdot' B_2 = \{(x, y) \in M \times M \mid (x, y) \sim (x_{a_2} * x_{b_2}, y_{a_2} * y_{b_2})\}$

We then only need to show that $(x_{a_1}, y_{a_1}) \cdot (x_{b_1}, y_{b_1}) \sim (x_{a_2}, y_{a_2}) \cdot (x_{b_2}, y_{b_2})$

$(x_{a_1}, y_{a_1}) \cdot (x_{b_1}, y_{b_1}) \sim (x_{a_2}, y_{a_2}) \cdot (x_{b_2}, y_{b_2})$

$$\Leftrightarrow \exists k \in M.\ x_{a_1} * x_{b_1} * y_{a_2} * y_{b_2} * k = y_{a_1} * y_{b_1} * x_{a_2} * x_{b_2} * k \quad (\mathrm{I})$$

Since $\exists k_1 \in M.\ x_{a_1} * y_{a_2} * k_1 = x_{a_2} * y_{a_1} * k_1$

$\exists k_2 \in M \quad x_{b_1} * y_{b_2} * k_2 = x_{b_2} * y_{b_1} * k_2$

using the commutative rule and let $k = k_1 * k_2$

(I) follows instantly. $\square$