HW1 P1 Let S, T be sets. We define the set-theoretic difference of the ordered pairs (S,T) to be

$$S\backslash T = \{x \in S | x \notin T\}.$$

(a) Prove that $T \cap (S\backslash T) = \emptyset$.
(b) Prove that $(S\backslash T) \cup (S \cap T) = S$.

Proof. (a) Let $x \in T \cap (S\backslash T)$, then $x \in T$ and $x \notin T$, a contradiction. Thus, no element in the set $T \cap (S\backslash T)$, therefore $T \cap (S\backslash T) = \emptyset$.

(b) $(S\backslash T) \cup (S \cap T) \supseteq S$:
Let $x \in S$, if $x \in T$ then $x \in (S \cap T) \subseteq (S\backslash T) \cup (S \cap T)$; if $x \notin T$ then $x \in (S\backslash T) \subseteq (S\backslash T) \cup (S \cap T)$.
$(S\backslash T) \cup (S \cap T) \subseteq S$:
Since $(S\backslash T) \subseteq S$ and $(S \cap T) \subseteq S$, thus $(S\backslash T) \cup (S \cap T) \subseteq S$.
Therefore $(S\backslash T) \cup (S \cap T) = S$.

□

HW1 P5 The Fibonacci sequence f_n is defined by $f_1 = f_2 = 1$ and

$$f_n = f_{n-1} + f_{n-2}$$

for all integers $n \geq 3$. Prove that for every integer $k \geq 1$, the Fibonacci number f_{5k} is divisible by 5.

Proof. By induction
If $k = 1$, $f_5 = f_4 + f_3 = f_3 + f_2 + f_3 = 2f_3 + f_2 = 2(f_2 + f_1) + f_2 = 3f_2 + 2f_1 = 3 + 2 = 5$, thus f_5 is divisible by 5.
Suppose that f_{5k} is divisible by 5, consider

$$\begin{aligned} f_{5(k+1)} = f_{5k+4} + f_{5k+3} &= f_{5k+3} + f_{5k+2} + f_{5k+3} = 2f_{5k+3} + f_{5k+2} \\ &= 2(f_{5k+2} + f_{5k+1}) + (f_{5k+1} + f_{5k}) \\ &= 2f_{5k+2} + 3f_{5k+1} + f_{5k} \\ &= 2(f_{5k+1} + f_{5k}) + 3f_{5k+1} + f_{5k} \\ &= 5f_{5k+1} + 2f_{5k} \end{aligned}$$

Since $2f_{5k}$ is divisible by 5, so is $f_{5(k+1)}$.
Therefore, for all $k \geq 1$, f_{5k} is divisible by 5.

□

HW2 P2 Let G be the set of all 2×2 matrices

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

where $a, b \in \mathbb{R}$ and $a^2 + b^2 \neq 0$. Prove that G forms a group with the usual matrix multiplicative. You may freely use basic facts from linear algebra without proof.

Proof. 0° Matrix multiplicative is a binary operation on G:

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -b_1a_2 - a_1b_2 & -b_1b_2 + a_1a_2 \end{pmatrix} \in G$$

where $a_1^2 + a_2^2, b_1^2 + b_2^2 \neq 0$, thus $(a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2 = (a_1^2 + a_2^2)(b_1^2 + b_2^2) \neq 0$.

1° Associative law:
G inherit associativity from usual matrix multiplication.

2° Identity exist:
$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity of G, $eA = Ae = A$ for any $A \in G$.

3° Inverse exist:
$\forall A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G$, $A^{-1} = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in G$, where $(\frac{a}{a^2+b^2})^2 + (\frac{-b}{a^2+b^2})^2 = \frac{1}{a^2+b^2} \neq 0$.

□

HW2 P4 Let $(G, *)$ be a group such that $x * x = e$ for all $x \in G$. Prove that G is abelian.

Proof. $\forall z \in G$, since $z * z = e$, thus $z = z^{-1}$. Let $x, y \in G$, $x * y = (x * y)^{-1} = y^{-1} * x^{-1} = y * x$, therefore G is abelian. □

HW2 P5 In class, we defined a binary operation $\bigoplus$ on $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$. We now define a binary operation $\bigodot$ on $\mathbb{Z}_n$ by setting $\overline{a} \bigodot \overline{b} := \overline{a \cdot b}$.

(a) Prove that $\bigodot$ is associative.
(b) Does $\mathbb{Z}_4 \backslash \{\overline{0}\}$ form a group with $\bigodot$? Prove your answer.
(c) Does $\mathbb{Z}_5 \backslash \{\overline{0}\}$ form a group with $\bigodot$? Prove your answer.

Proof. (a)

$$(\overline{a} \bigodot \overline{b}) \bigodot \overline{c} = \overline{a \cdot b} \bigodot \overline{c} = \overline{(a \cdot b) \cdot c}$$
$$\overline{a} \bigodot (\overline{b} \bigodot \overline{c}) = \overline{a} \bigodot \overline{b \cdot c} = \overline{(a \cdot b) \cdot c}$$

$(a \cdot b) \cdot c = (a \cdot b) \cdot c$ implies $(\overline{a} \bigodot \overline{b}) \bigodot \overline{c} = \overline{a} \bigodot (\overline{b} \bigodot \overline{c})$, where $a, b, c \in \mathbb{Z}$.

(b) No, it is not a group. Since $\overline{0} \neq \overline{2} \in \mathbb{Z}_4 \backslash \{0\}$ but $\overline{2} \bigodot \overline{2} = \overline{2 \cdot 2} = \overline{0} \notin \mathbb{Z}_4 \backslash \{\overline{0}\}$, it is not closed under $\bigodot$.

(c) The table under $\bigodot$

$\bigodot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\overline{1}$ is the identity in $\mathbb{Z}_5\backslash\{\overline{0}\}$; every element has inverse in $\mathbb{Z}_5\backslash\{\overline{0}\}$. Therefore, $\mathbb{Z}_5\backslash\{\overline{0}\}$ is a group.

□

HW3 P2 Let G be a nonempty set and let $*$ be an associative binary operation on G. Assume that for any elements $a, b \in G$, we can find $x \in G$ such that $a * x = b$, and we can find $y \in G$ such that $y * a = b$. Prove that G is a group. Carefully write the proof in your own words.

Proof. Choose $a \in G$, we can find $x, y \in G$, such that $a * x = a$ and $y * a = a$.
x is the right inverse of G and y is the left inverse of G:
$\forall z \in G$, there exists $z' \in G$, such that $z = z' * a$, then $z * x = (z' * a) * x = z' * (a * x) = z' * a = z$. Similarly, $y * z = z$. Define $e = x = xy = y$, thus e is the identity in G.
$\forall z \in G$, there exists z_l^{-1} and z_r^{-1} in G, such that $z_l^{-1} * z = z * z_r^{-1} = e$. And then $z_l^{-1} = z_l^{-1} * e = z_l^{-1} * (z * z_r^{-1}) = (z_l^{-1} * z) * z_r^{-1} = e * z_r^{-1} = z_r^{-1}$.
Thus, $z^{-1} = z_l^{-1} = z_r^{-1}$ is the inverse of z.
Therefore, $(G, *)$ is a group. □

HW3 P5 Let G be a group. Let $x, y \in G$. Assume that $y \neq e$, $o(x) = 2$, and $xyx^{-1} = y^2$. Determine $o(y)$.

Proof. (1) $y^2 \neq e$:
BWOC, if $y^2 = e$, thus $e = y^2 = xyx^{-1}$, so $e = x^{-1}ex = x^{-1}xyx^{-1}x = eye = y$, contradiction to $y \neq e$.
(2) $y^3 = e$:
Since $o(x) = 2$, then $x^2 = x^{-2} = e$, thus

$$\begin{aligned} y^4 &= (y^2)(y^2) = xyx^{-1}xyx^{-1} = xy^2x^{-1} \\ &= x(xyx^{-1})x^{-1} = x^2yx^{-2} = eye = y \end{aligned}$$

So, $y^4 = y \Rightarrow y^3 = e$, therefore $o(y) = 3$. □

HW4 P3 Let H, K be subgroups of a group G.
(a) Prove that $H \cap K$ is a subgroup of G.
(b) Prove that $H \cup K$ is a subgroup of G iff $H \subseteq K$ or $K \subseteq H$.

Proof. (a) $e \in H, K$ implies $e \in H \cap K$; $\forall x \in H \cap K$, H and K are subgroups of G, thus $x^{-1} \in H$ and K, therefore $x^{-1} \in H \cap K$.
(b) $\Rightarrow$ BWOC
Suppose that $H \not\subset K$ and $K \not\subset H$. Choose $h \in H\backslash K$ and $k \in K\backslash H$, since $H \cup K$ is a subgroup of G and $h, k \in H \cup K$, then $hk \in H \cup K$. Without lose of generality, suppose $hk \in H$, then $k = h^{-1}hk \in H$, contradiction to $k \notin H$. Therefore $hk \in K \Rightarrow h = hkk^{-1} \in K$, also

contradiction to $h \notin K$. So $H \subseteq K$ or $K \subseteq H$.
$\Leftarrow$ easy to verify.

□

HW5 P3 Let $f : A \to B$ and $g : B \to C$ be functions.

(a) Assume that $g \circ f$ is injective. Does this imply that both f and g are injective? Prove your answer.
(b) Assume that $g \circ f$ is surjective. Does this imply that both f and g are surjective? Prove your answer.

Proof. (a) $g \circ f$ is injective implies f is injective:
Let $x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $(g \circ f)(x_1) = (g \circ f)(x_2)$. Since $g \circ f$ is injective, thus $x_1 = x_2$. Therefore, f is injective.
But, g needn't be injective.

(b) $g \circ f$ is surjective implies g is surjective:
$\forall c \in C$, since $g \circ f$ is surjective, there exists $x \in A$, such that $(g \circ f)(x) = c$, i.e. $g(f(x)) = c$ with $f(x) \in B$. Therefore, g is surjective.
f needn't be surjective.

□

HW6 P4 Let p, q be two prime numbers, and let G be a group of order pq. Show that every subgroup H of G with $H \neq G$ is cyclic.

Proof. By Lagrange's Theorem, $\sharp H$ divides $\sharp G = pq$, thus $\sharp H$ equal to 1, p or q ($\sharp H \neq pq$, since $H \neq G$). Since p and q are prime numbers, then H is cyclic. □

HW6 P5 Let G be a group of order p^2, where p is a prime. Prove that G must have a subgroup of order p.

Proof. Let $e \neq x \in G$ (since $G \neq \{e\}$), by Lagrange's theorem, $o(x) = \sharp\langle x\rangle$ divides $\sharp G = p^2$, thus $o(x)$ equal to p or p^2 ($o(x) \neq 1$, since $x \neq e$). If $o(x) = p$, then $\sharp\langle x\rangle = p$; if $o(x) = p^2$, then $\langle x^p\rangle = o(x^p) = p$. □

HW6 P6 Let G be a group. Let H, K be subgroups of G. Assume that $\sharp H = 12$ and $\sharp K = 17$. Prove that $H \cap K = \{e\}$.

Proof. Since H and K are subgroups of G, so is $H \cap K$. Thus $H \cap K$ also subgroup of H and K ($H \cap K \subseteq H, K$). By Lagrange's Theorem, $\sharp(H \cap K)$ divides $\sharp H$ and $\sharp K$, thus $\sharp(H \cap K) \mid gcd(12, 17) = 1$. Therefore, $\sharp(H \cap K) = 1$ i.e. $H \cap K = \{e\}$. □

HW7 P5 Let G be a group and let N a normal subgroup of G. Let H be a subgroup of G. Set $NH = \{nh | n \in N, h \in H\}$. Prove that NH is a subgroup of G.

Proof. 0° NH is closed under group multiplicative:

Let $n_1, n_2 \in N$ and $h_1, h_2 \in H$, $n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2$. N is a normal subgroup of G, implies $h_1n_2h_1^{-1} \in N$, thus $n_1(h_1n_2h_1^{-1}) \in N$. H is a subgroup of G, implies $h_1h_2 \in H$. Therefore $n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2 \in NH$.

1° $e \in NH$: $e = ee \in NH$.

2° NH is closed under inverses:

Let $n \in N$ and $h \in H$, $(nh)^{-1} = h^{-1}n^{-1} = h^{-1}n^{-1}hh^{-1}$. Since N is a normal subgroup of G, thus $h^{-1}n^{-1}h \in N$. Therefore, $(nh)^{-1} = h^{-1}n^{-1} = h^{-1}n^{-1}hh^{-1} \in NH$.

Therefore, NH is a subgroup of G. □

HW7 P6 Let G be a group and let H a normal subgroup of G such that $[G : H] = 20$ and $\sharp H = 7$. Suppose $x \in G$ and $x^7 = e$. Prove that $x \in H$.

Proof. Since H is a normal subgroup of G, thus G/H is a group under natural multiplicative. $\sharp(G/H) = [G : H] = 20$ and $xH \in G/H$, implies $x^{20}H = (xH)^{20} = H \in G/H$, i.e. $x^{20} \in H$. 7 coprime with 20, we can find $7 \times 3 - 20 = 1$, $x = x^{7\times3-20} = (x^7)^3x^{-20} = e^3x^{-20} = x^{-20} \in H$. □