Abstract Algebra hw2

Chengyu Hsieh, B13201053

1) The identity element of G is 0. We assume 2) is proven(the proof is given below at 2)).

   (a) $1, 14 \in G_1$, but $1 + 14 = 15 \notin G_1$, so it is not close under addition $\Rightarrow$ not a subgroup.

   (b) G_2 is non empty. For any $g_1, g_2 \in G_2$, $g_1 = 2a$, $g_2 = 2b$, we have $g_1 + g_2 = 2(a + b) \in G_2$, so G_2 is closed under addition.
   For any $g_1 = 2a \in G_2$, $0 \leq a \leq 14$, we have $g_1 + 2(15 - a) = 0$. Note $2(15 - a) \in G_2$, hence it is $-g \in G_2$.
   Hence by 2) G_2 is a subgroup of G.

   (c) The identity element $0 \notin G_3$, so it is not a subgroup of G.

2) (i) For any $a \in H$, since $a^{-1} \in H$ and H is closed under $*$, we have $e = a * a^{-1} \in H$. Combined with the given criterion and that $H \subset G$, we have the required properties for a group. Hence $H \leq G$.

   (ii) Note we have $det(AB) = (detA)(detB)$. The identity matrix has determinant 1 so $SL_n(\mathbb{R})$ is non empty. For any A, $B \in SL_n(\mathbb{R})$, $det(AB) = 1 \times 1 = 1$, so $SL_n(\mathbb{R})$ is closed. For any $A \in SL_n$, since A^{-1} exists and $det(A^{-1}) = \frac{1}{det(A)} = 1$ so $A^{-1} \in SL_n$. By the criterions in (i), we know $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

3) (a) Composites of bijections are clearly bijections. Also the composition of functions satisfy associativity. The identity mapping is $I(x) = x\, \forall x \in G$. For any mapping $f(x) \in S_n$, since f is bijective, $\exists f^{-1}(x) \in S_n$, the inverse mapping of f, is the inverse of f in S_n, satisfying $f(f^{-1}(x)) = I(x)$. Hence S_n is a group. For its order, $f(1)$ has n possible values. After assigning $f(1)$, $f(2)$ has $n - 1$ possible values, etc. Hence there are $n(n-1)\ldots(2)(1) = n!$ elements in S_n.

   (b) The closure is trivial. The inverse is just the inverse mapping. Hence $S := \{\sigma \in S_4 | \sigma(1) = 1\}$ is a subgroup of S_4.

   (c) The identity of the given group is $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. By calculation we find $a^4 = I$ and $b^3 = I$. Hence a has order 4 and b has order 3.

4)

Claim 1. For any $x \in G$, $g \in G$ a generator of G, we have $x = xg^{bn}$ for any $b \in \mathbb{Z}$.

Proof. $g^n = e$, so $g^b n = (g^n)^b = e^b = e$ for any $b \in \mathbb{Z}$.

Claim 2. Let $a, b \in \mathbb{Z}$, $a, b > 0$. If $\exists c, d \in \mathbb{Z}$ such that $ca + db = 1$, then$(a, b) = 1$.

Proof. Suppose $(a,b) = k > 1$. Let $a = k\alpha$, $b = k\beta$. Let c, d be integers such that $ca + db = 1$. Subsitute in $k\alpha$ and $k\beta$ we obtain '

$$k(c\alpha + d\beta) = 1$$

Since k and $c\alpha + d\beta$ are integers, we have $(k = 1 \wedge c\alpha + d\beta = 1) \vee (k = -1 \wedge c\alpha + d\beta = -1)$. But we assumed that $k > 1$ and so we arrived at an contradiction. Hence $(a,b) = 1$.

Claim 3. Let $a, b \in \mathbb{Z}$, $a, b > 0$. If $(a,b) = m$, then exists $c, d \in \mathbb{Z}$ such that $ca + db = m$.

Proof. First note that if $d|a \wedge d|b$, then $d|m$. Now let $M = \{ca + db | c, d \in \mathbb{Z}\}$. $1a + 0b = a > 0$, so M has positive integers. Let $M^+ = \{ca + db > 0 | c, d \in \mathbb{Z}\}$, which is non empty. Clearly $\min M^+$ exist. Let $m' = \min M^+$. Then $m' = c'a + d'b$ for some $c', d' \in \mathbb{Z}$. Now for any $x = ca + db \in M$, let $x = m'q + r$ with $0 \leq r < m'$.

$$r = x - m'q = (c - c'q)a + (d - d'b)b \in M$$

Since we have $0 \leq r < m'$, we have $r = 0$. (Otherwise $m' \neq \min(M^+)$).) Therefore $m'|x\ \forall x \in M$. Note that $a, b \in M \Rightarrow m'|a \wedge m'|b$. Also, for any d such that $d|a \wedge d|b$ we have $d|c'a + d'b$, so $d|m'$. Hence $m' = (a,b) = m$. We conclude that $\exists c, d \in \mathbb{Z}$ such that $ca + db = m$.

(a) If $n = 1$ then $g^k = e$ is always a generator, also $gcd(k,n) = 1$ for any k. We then consider $n \geq 2$
Sufficiency:
Suppose g^k is a generator of G. Since g^k is a generator, $g = (g^k)a$ for some a. Let $ka = bn + m$, $1 \leq m \leq n - 1$(m cannot be zero as that leeds to $g = e$ which cannot be true for $n \geq 2$.) Then by Claim 1, $g = (g^k)^a = g^{ak-bn} = g^m$. Applying g^{-1} to both sides, we obtain $g^{m-1} = e$. If $m - 1 \neq 0$ then we found $n' = m - 1 < n$ such that $g^{n'} = e$, contradicting the fact that g is a generator of G. Hence $m = 1$. Then by Claim 2, $\exists a,\ b \in \mathbb{Z}$ such that $ak + (-b)n = 1$, so $gcd(n,k) = 1$.
Necessity:
Suppose $gcd(k,n) = 1$. Then by Claim 3, $\exists a,\ b \in \mathbb{Z}$ such that $ak + bn = 1$. So $(g^k)^a = g^{ak} = g^{1-bn} = g^1 = g$. Clearly this leads to g^k also being a generator.

(b) Let $n = ma$. Consider $S = \{g^a,\ g^{2a},\ \ldots, g^{ma}\}$. Note that $0 < a < 2a < \cdots < (m-1)a < ma = n$, so $|S| = m$. For any $g^{\gamma a} \in S$, see that $g^{\gamma a} g^{(m-\gamma)a} = e$ and $g^{(m-\gamma)a}$ is clearly in S. Also S is clearly closed. Thus $S \leq G$ and we have found a subgroup of order m.
Now suppose we find $H \leq G$ with $|H| = m$. Let c be the smallest positive integer such that $g^c \in H$. If $\exists g^x \in H$ with $x = yc + z$, $1 \leq z \leq c - 1$, we have $g^z = g^x G^{-yc} \in H$. But $z < c$ so we have arrived at a contradiction. Hence $\forall g^x \in H$, we have $g^x = (g^c)^y$ for some y, and so g^c generates H. Now, $g^{mc} = g^n$ so $mc = bn = bam$ for some b. Hence $c = ab$. This gives us $g^c = (g^a)^b \in H$. But c is the smallest positive integer such that $g^c \in H$. So $a = c$ and $H = S$.
We conclude that G has exactly one subgroup of order m.

(c) $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ has order 6. Order of (1) is $1 < 6$, order of $(12), (13), (23)$ are all $2 < 6$, order of $(123), (132)$ are both $3 < 6$. Hence no elements of S_3 g can generate the entire group, so S_3 is not cyclic.

5) (a) For any $g_1N, g_2N \in G/N$, since $g_1 * g_2 \in G$, we have $g_1N \cdot g_2N \in G/N$. For $g_1N, g_2N, g_3N \in G/N$, $(g_1N \cdot g_2N) \cdot g_3N = (g_1 * g_2)N \cdot g_3N = (g_1 * g_2 * g_3)N = g_1N \cdot (g_2 * g_3)N = g_1N \cdot (g_2N \cdot g_3N)$, thus associativity holds. $N = eN \in G/N$ is clearly the identity. For any $gN \in G/N$, $g^{-1}N$ is clearly in G/N and is the inverse of gN.

(b) $(13)H = \{(13), (123)\}$, $H(13) = \{(13), (132)\} \neq (13)H$. Thus H is not a normal subgroup of S_3.

(c) Let $H \leq G$. $\forall h \in H,\ g \in G$, we have $g * h = h * g$ so $gH = \{g * h | h \in H,\ g \in G\} = \{h * g | h \in H,\ g \in G\} = Hg$. So any subgroup of an abelian group G is normal.

(d) Consider the quaterion group $Q_4 = \pm 1, \pm i, \pm j, \pm k$ with $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. This group satisfies the required conditions.