

Abstract algebra I Homework 2

B13902022 賴昱錡

Due: 24th September 2025

1)

(a)

Take the sum of 14 and 13, and it's 27 modulo 30, $27 \notin G_1$ thus, G_1 is not a subgroup of G .

(b)

We can check some necessary properties a subgroup must follow:

- All elements of G_2 are also in G , $G_2 \in G$
- $\exists e$ such that $\forall g \in G_2, g + e = e + g = g$. There $e = 0$.
- $0 + 0 \equiv 0 \pmod{30}$, thus, $g^{-1} = 0$ when $g = 0$. All the other non-zero elements $\in G_2$ can be written as the form $2k, k \in [1, 14], k \in \mathbb{N}$. Assume $g = 2k$, then there must exists an element $h = 2(15 - k) \in G_2$ such that $g + k \equiv 0 \pmod{30}$. Thus, every element in G_2 has an inverse element.

(c)

Take the sum of 1 and 29, and it's 0 modulo 30, $0 \notin G_3$ thus, G_3 is not a subgroup of G .

2)

(i)

Proof. Since H is not empty, we can choose $x, y \in G$.

By the closedness of inverse, the inverse of x exists and belongs to the H , let $y = x^{-1}$.

By the closedness of $*$, $x * x^{-1} = e \in H$, where e is the identity element of H . Thus, the identity of H exists.

Since H is closed under products, and inverse for each element exists, and the identity for H exists. It's a group and $H \subset G$, so H is a subgroup of G . \square

(ii)

For simplicity, I denote the determinant of a n by n matrix A as $|A|$.

Since the determinant of an identity matrix I_n is 1, $SL_n(\mathbb{R}) \neq \emptyset$.

For any matrices $a, b \in SL_n(\mathbb{R})$, suppose $c = ab$, then c must be a real matrix (all entries are real), also, $|c| = |a||b| = 1 * 1 = 1$, the determinant of c is also 1. Thus, $c \in SL_n(\mathbb{R})$. Here proves the closedness of matrix multiplication.

Claim 1: Real $n \times n$ matrix A is invertible if and only if $|A| \neq 0$

Proof. Suppose A is invertible, then there exists a matrix B such that $AB = I$. $|I| = |A||B| = 1$, $|A|$ can't be zero.

Assume $|A| \neq 0$, then $B = \frac{1}{|A|} \text{adj}(A)$ (B is also a real $n \times n$ matrix) satisfies $AB = BA = I$ where $\text{adj}(A)$ is the classical adjoint matrix of A and I is the identity matrix.

Thus, $|A| \neq 0$ is necessary and sufficient. \square

By claim 1, every element in $SL_n(\mathbb{R})$ has its inverse due to their non-zero determinant. Suppose A is any matrix in $SL_n(\mathbb{R})$, and its inverse is A^{-1} , then $AA^{-1} = A^{-1}A = I$, $|A||A^{-1}| = |I| = 1$, thus, $|A^{-1}| = 1$.

Hence, the inverse of A , i.e., A^{-1} is also in $SL_n(\mathbb{R})$. Here the closedness of inverse is proved. By the subgroup criterion proved in 2(i), $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

3)**(a)**

Proof. Let's call the two sets A and B . $A = \{1, 2, \dots, n\}$, $B = \{1, 2, \dots, n\}$. And A is mapped to B .

Since the map is bijective, for 1 in A , there are n choices to be mapped, after 1 is mapped, 2 in A has $n - 1$ choices to be mapped, and so on.

Thus, there are $n(n - 1)(n - 1) \dots 1 = n!$ types of bijection, i.e., the order of S_n is $n!$. \square

(b)**(c)**

The identity element in the group for matrices multiplication is the identity matrix $I_{2 \times 2}$.

For a , $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $a^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $a^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_{2 \times 2}$. Thus, $o(a) = 4$. For b , $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, $b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_{2 \times 2}$, thus, $o(b) = 3$.

4)

(a)

Theorem 1. Bézout's identity

Let $a, b \in \mathbb{Z}, ab \neq 0$

$d = \gcd(a, b)$ be the greatest common divisor of a and b .

Then $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$. Also, d is the smallest positive integer combination of a and b .

Proof. Given any two non-zero integer a, b , Let set $S = \{ax + by : x, y \in \mathbb{Z} \wedge ax + by > 0\}$

It's trivial that S is not an empty set (For example, $a > 0, x = 1, y = 0$ or $a < 0, x = 1, y = 0$, $ax + by \in S$, thus, S is not an empty set). Since all elements in S are positive integers, by well ordering principle, S contains a least element d . And write it as the form $d = au + bv$, where u and v are integers.

Consider a 's euclidean division: $a = qd + r, q \in \mathbb{Z}, 0 \leq r < d$, we have:

$$r = a - qd = a - q(au + bv) = a(1 - qu) - bq v$$

Because both $1 - qu$ and qv are integers, $r \in S \cup \{0\}$ (because $0 \leq r < d$). Also, d is the least element in S , this implies that r is not belonging to S , it must be 0. Thus, $d|a$. Similarly, $d|b$.

Consider arbitrary common divisor c of a, b , $\exists s, t$ such that $a = cs, b = ct$. So, $d = au + bv = c(us + vt)$, because $us + vt \in \mathbb{Z}$, we know $c|d \wedge c \leq d$.

Since d is greater than all divisors, $d = \gcd(a, b)$, it's also the least element in S by previous definition. \square

Claim 2: If x is the generator of cyclic group H , then the order of H is the same as $|x|$ (If one side of this equality is infinite, so is the other).

Proof. Let $|x| = n$ and first consider the case when $n < \infty$. The elements $1, x, x^2, \dots, x^{n-1}$ are distinct since if $x^a = x^b, 0 \leq a < b < n$ then $x^{b-a} = 1$, which contradict n being the smallest positive power give the identity. Also, we can write any integer power t as the form $t = ns + r, 0 \leq r < n$. Hence, $x^t = x^{ns+r} = (x^n)^s x^r = x^r \in \{1, x, \dots, x^{n-1}\}$, x can generate all elements in H .

Suppose $|x| = \infty$ so no power of x is the identity, If $x^a = x^b$ for some a and b , with $a < b$, then $x^{b-a} = 1$ induced a contradiction. Distinct power of x are distinct elements of $|H|$, so $|H| = \infty$ is true. \square

Claim 3: Let G be an arbitrary group, $x \in G$ and let $m, n, n\mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m .

Proof. By Theorem 1 there exists integers a and b such that $d = an + bm, d = (m, n)$. Thus, $x^d = x^{an+bm} = (x^n)^a (x^m)^b = 1$, this proves the first assertion.

If $x^m = 1$, let $n = |x|$. If $m = 0$, $n|m$ is trivially true. Assume m is not zero, by preceding result, $x^d = 1, d = (m, n)$. Since $0 < d \leq n$ and n is the smallest positive power of x which gives the identity, we must have $d = n$, that is $n|m$ as the claim said. \square

Claim 4: Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$, if $o(x) = n < \infty$, then $o(x^a) = \frac{n}{(n,a)}$.

Claim 5: Let $H = \langle x \rangle$. Assume $o(x) = n < \infty$. Then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$.

(b)

(c)

5)**(a)***Proof.*

□

(b)**(c)**

Since elements in the abelian group $(G, *)$ are commutative, i.e., for any $a, b \in G$, we have $a * b = b * a$.

Let's choose one arbitrary elements g , consider the subgroup as $B = \{a_1, a_2, \dots, a_m\}$. Then $gB = \{g * a_1, g * a_2, \dots, g * a_m\}$, and $Bg = \{a_1 * g, a_2 * g, \dots, a_m * g\}$. since $g * a_i = a_i * g$ for all i , we have $gB = Bg$.

Hence, by the definition, every subgroup of an abelian group is normal.

(d)