

9.1 关系及性质

6. Determine whether the relation R on the set of all real numbers is reflexive, symmetric, antisymmetric, and/or transitive, where $(x, y) \in R$ if and only if

c) $x - y$ is a rational number.

d) $x = 2y$.

e) $xy \geq 0$.

g) $x = 1$.

h) $x = 1$ or $y = 1$.

答: c) 自反、对称、非 反对称、传递。

d) 非 自反、非 对称、反对称、非 传递。

e) 自反、对称、非 反对称、非 传递 (因 $(1,0)$ and $(0,-2)$ not imply $(1,-2)$)

g) 非 自反、非 对称、反对称、传递。

h) 非 自反、对称、非 反对称、非 传递 (因 $(2,1)$ and $(1,2)$ not imply $(2, 2)$)。

33. Let R be the relation on the set of people consisting of pairs (a, b) , where a is a parent of b . Let S be the relation on the set of people consisting of pairs (a, b) , where a and b are siblings (brothers or sisters). What are $S \circ R$ and $R \circ S$?

答: $S \circ R = \{(a, b) \mid a \text{ is a parent of } b \text{ and } b \text{ has a sibling}\}$,

$R \circ S = \{(a, b) \mid a \text{ is an aunt or uncle of } b\}$

9.3 关系的表示及关系运算

14. Let R_1 and R_2 be relations on a set A represented by the matrices

$$\mathbf{M}_{R_1} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \mathbf{M}_{R_2} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Find the matrices that represent

- a) $R_1 \cup R_2$. b) $R_1 \cap R_2$. c) $R_2 \circ R_1$.
d) $R_1 \circ R_1$. e) $R_1 \oplus R_2$.

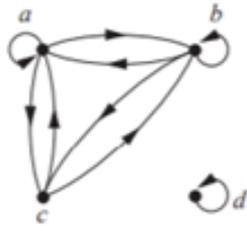
c) The matrix is the Boolean product $M_{R_1} \odot M_{R_2} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

d) The matrix is the Boolean product $M_{R_1} \odot M_{R_1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

答:

32. Determine whether the relations represented by the directed graphs shown in Exercises 26–28 are reflexive, irreflexive, symmetric, antisymmetric, asymmetric, and/or transitive.

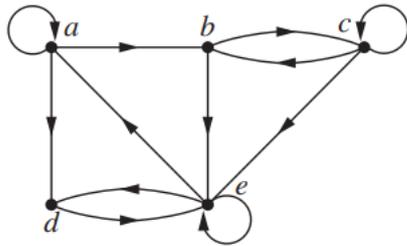
27.



答: 仅满足 对称, 其它性质都不满足, 非 传递((c,a)and(a,c),但没有(c,c))。

9.4 关系闭包运算

17. Find all circuits of length three in the directed graph in Exercise 16.



答: a, a, a, a; a, b, e, a; a, d, e, a; b, c, c, b; b, e, a, b; c, b, c, c;
 c, c, b, c; c, c, c, c; d, e, a, d; d, e, e, d; e, a, b, e; e, a, d, e;
 e, d, e, e; e, e, d, e; e, e, e, e;

写不全的原因是没有使用 R^3 的算法。

26. Use Algorithm 1 to find the transitive closures of these relations on $\{a, b, c, d, e\}$.

- a) $\{(a, c), (b, d), (c, a), (d, b), (e, d)\}$
- b) $\{(b, c), (b, e), (c, e), (d, a), (e, b), (e, c)\}$
- c) $\{(a, b), (a, c), (a, e), (b, a), (b, c), (c, a), (c, b), (d, a), (e, d)\}$
- d) $\{(a, e), (b, a), (b, d), (c, d), (d, a), (d, c), (e, a), (e, b), (e, c), (e, e)\}$

答

b) For this and the remaining parts we just exhibit the matrices that arise.

$$\begin{aligned}
 \mathbf{A} &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} & \mathbf{A}^{[2]} &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} & \mathbf{A}^{[3]} &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} \\
 \mathbf{A}^{[4]} &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} = \mathbf{A}^{[5]} & \mathbf{B} &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}
 \end{aligned}$$

29. Find the smallest relation containing the relation $\{(1, 2), (1, 4), (3, 3), (4, 1)\}$ that is

- a) reflexive and transitive.
- b) symmetric and transitive.
- c) reflexive, symmetric, and transitive.

答: b)要算 $ts(R)$, c)要算 $tsr(R)$.

- b) $\{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (2, 4), (3, 3), (4, 1), (4, 2), (4, 4)\}$
- c) $\{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (2, 4), (3, 3), (4, 1), (4, 2), (4, 4)\}$

9.5 等价关系

8. Let R be the relation on the set of all sets of real numbers such that SRT if and only if S and T have the same cardinality. Show that R is an equivalence relation. What are the equivalence classes of the sets $\{0, 1, 2\}$ and \mathbb{Z} ?

Proof: show that R is reflexive, symmetric, and transitive.

- (1) Every set has the same cardinality as itself, so SRS , R is reflexive.
- (2) If SRT , $|S| = |T|$, then $|T| = |S|$, TRS , so R is symmetric.
- (3) If SRT and TRW , then $|S| = |T|$, $|T| = |W|$, so $|S| = |W|$, R is transitive.

16. Let R be the relation on the set of ordered pairs of positive integers such that $((a, b), (c, d)) \in R$ if and only if $ad = bc$. Show that R is an equivalence relation.

Proof: show that R is reflexive, symmetric, and transitive.

- (1) $((a, b), (c, d)) \in R$ if and only if $ad = bc$.
 $(a, b), (a, b) \in R$ because $a \cdot b = b \cdot a$, R is reflexive.

(2) If $((a, b), (c, d)) \in R$, then $ad = bc$, so $cb=da$, $((c, d), (a, b)) \in R$, thus R is symmetric.

(3) If $((a, b), (c, d)) \in R$ and $((c, d), (e, f)) \in R$,

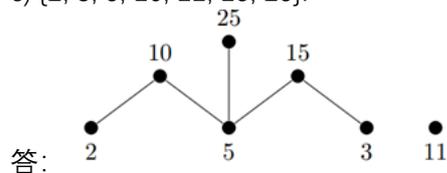
Then $ad=bc$, $cf=de$. $adcf=bcde$, because cd is nonzero, so $af=be$.

$((a, b), (e, f)) \in R$, thus R is transitive.

9.6 偏序关系

22. Draw the Hasse diagram for divisibility on the set

$c) \{2, 3, 5, 10, 11, 15, 25\}$.



35. Answer these questions for the poset $(\{\{1\}, \{2\}, \{4\}, \{1, 2\}, \{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}, \subseteq)$.

a) Find the maximal elements.

答: a) $\{1, 2\}, \{1, 3, 4\}, \{2, 3, 4\}$

44. Determine whether these posets are lattices.

c) (\mathbb{Z}, \geq)

答: this is a lattice because it is a linear order. The least upper bound of two numbers in the list is the smaller number (since here "greater" really means "less"!), and the greatest lower bound is the larger of the two numbers.

补充 9.1 抽象代数与二元运算

20. Consider the binary operation $*$ defined on the set $A = \{a, b, c\}$ by the following table.

$*$	a	b	c
a	b	c	b
b	a	b	c
c	c	a	b

(a) Is $*$ a commutative operation?

(b) Compute $a * (b * c)$ and $(a * b) * c$.

(c) Is $*$ an associative operation?

答: (b) $a*(b*c)=a*c=b$, $(a*b)*c=c*c=b$.

(c) not associative, $(c*c)*c=b*c=c \neq a=c*b=c*(c*c)$.

24. Let A be a set with n elements. How many binary operations can be defined on A ?

Solution: n^{n^2} , 不是 2^{nn}

28. Let $*$ be a binary operation on a set A , and suppose that $*$ satisfies the idempotent, commutative, and associative properties, as discussed in Example 16. Define a relation \leq on A by $a \leq b$ if and only if $b = a * b$. Show that (A, \leq) is a poset and, for all a and b , $\text{LUB}(a, b) = a * b$.

Proof:

1. \leq is reflexive

Since idempotent, $a = a * a$, $a \leq a$ for all a in A .

2. \leq is antisymmetric

suppose that $a \leq b$ and $b \leq a$.

Then, $b = a * b$, and $a = b * a$, because commutative, $a * b = b * a$, so $a = b$.

3. \leq is transitive

If $a \leq b$ and $b \leq c$, then $c = b * c = (a * b) * c = a * (b * c) = a * c$, so $a \leq c$.

4. show $a * b = a \vee b$, for all a and b in A

(1) $a * b = a * (b * b) = (a * b) * b = b * (a * b)$, so $b \leq a * b$.

In a similar way, $a * b = (a * a) * b = a * (a * b)$, so $a \leq a * b$.

so $a * b$ is an upper bound for a and b .

(2) if $a \leq c$ and $b \leq c$. then $c = a * c$ and $c = b * c$ by definition.

Thus $c = a * (b * c) = (a * b) * c$. so $a * b \leq c$.

This shows that $a * b$ is the leastest upper bound of a and b .

补充 9.2 半群与群

12. Let $S = \{x \mid x \text{ is a real number and } x \neq 0, x \neq -1\}$. Consider the following functions $f_i: S \rightarrow S, i = 1, 2, \dots, 6$:

$$f_1(x) = x, \quad f_2(x) = 1 - x, \quad f_3(x) = \frac{1}{x}$$

$$f_4(x) = \frac{1}{1-x}, \quad f_5(x) = 1 - \frac{1}{x}, \quad f_6(x) = \frac{x}{x-1}.$$

Show that $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ is a group under the operation of composition. Give the multiplication table of G .

Proof: (1) show composition is closure. 从运算表自然可知.

°	f1	f2	f3	f4	f5	f6
f1	f1	f2	f3	f4	f5	f6
f2	f2	f1	f5	f6	f3	f4
f3	f3	f4	f1	f2	f6	f5
f4	f4	f3	f6	f5	f1	f2
f5	f5	f6	f2	f1	f4	f3
f6	f6	f5	f4	f3	f2	f1

(2) identity e is f_1 ;

(3) show every element exist reverse.

$$f_2^{-1}=f_2, \quad f_3^{-1}=f_3, \quad f_4^{-1}=f_5, \quad f_6^{-1}=f_6.$$

(4) show associate.

because \circ is associate.

16. Let G be a group with identity e . Show that if $a^2 = e$ for all a in G , then G is Abelian.

Proof: If $a*a=e, \forall a \in G$. show commutative.

(1) group propertise $(a*b)^{-1}=b^{-1}*a^{-1}$

because $a*a=e=a*a^{-1}$ so, $b^{-1}*a^{-1}=b*a$,

(2) $(a*b)*(a*b)=e \Rightarrow (a*b)^{-1}=a*b$,

reverse be only one in Group. so $b*a=a*b$.

补充 9.3 子代数与商代数

22. Prove or disprove that the intersection of two subsemigroups of a semigroup $(S, *)$ is a subsemigroup of $(S, *)$

proof: closure;

$$\forall a, b \in S_1 \cap S_2, \text{ then } a*b \in S_1, a*b \in S_2, \text{ so } a*b \in S_1 \cap S_2.$$

if $S_1 \cap S_2 = \emptyset$, still be subsemigroup.

2. Let $(S, *)$ and $(T, *')$ be monoids. Show that $S \times T$ is also a monoid. Show that the identity of $S \times T$ is (e_S, e_T) .

Proof:

(1) show $(S \times T, *'')$ is a binary operation.

Let $(s_1, t_1), (s_2, t_2) \in S \times T$.

$$\text{then } (s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2, t_1 *' t_2)$$

so $*''$ is a binary operation.

(2) show $*''$ is associative.

$$\text{Consider } (s_1, t_1) *'' ((s_2, t_2) *'' (s_3, t_3)) = (s_1, t_1) *'' (s_2 *' s_3, t_2 *' t_3)$$

$$\begin{aligned}
&= (s1*(s2*s3), t1*(t2*t3)) \\
&= ((s1*s2)*s3, (t1*t2)*t3) \quad \text{by } (S,*) \text{ and } (T,*) \text{ be associative.} \\
&= (s1*s2, t1*t2)*''(s3, t3) \\
&= ((s1, t1)*''(s2, t2)) *''(s3, t3) \\
&\text{Thus } (S \times T, *'') \text{ is a semigroup.}
\end{aligned}$$

(3) show $(S \times T, *'')$ has a identity (es, et) .

Let es is a identity of $(S, *)$, et is a identity of $(T, *)$.

Let $(s, t) \in S \times T$. then $(s, t)*''(es, et) = (s*es, t*et) = (s, t)$.

$$(es, et)*''(s, t) = (es*s, et*t) = (s, t).$$

Thus $(S \times T, *'')$ is a monoid.

22. Let G be an Abelian group with identity e , and let $H = \{x \mid x^2 = e\}$. Show that H is a subgroup of G .

Proof:

(1) show H is closed.

$$\text{Let } a, b \in H. (a*b)*(a*b) = a*(b*a)*b = a*(a*b)*b = a^2*b^2 = e*e = e.$$

Thus $(a*b) \in H$.

(2) show $e \in H$.

Because $e*e = e$, so $e \in H$.

(3) show if $x \in H$ then $x^{-1} \in H$.

$$\text{Let } x \in H, \text{ then } e = x*x = x*x^{-1}, \text{ so } x^{-1} = x \text{ Thus } x^{-1} \in H.$$

24. Let G be a group and let $a \in G$. Define $H_a = \{x \mid x \in G \text{ and } xa = ax\}$. Prove that H_a is a subgroup of G .

Proof: show $H_a = \{x \mid xa = ax\}$ is a subgroup.

(1) show H_a is closed.

$$\text{Let } x, y \in H_a. (x*y)*a = x*(y*a) = x*(a*y) = (x*a)*y = (a*x)*y = a*(x*y).$$

Thus $x*y \in H_a$.

(2) show $e \in H_a$.

Because $e*a = a = a*e$, so $e \in H_a$.

(3) show if $x \in H_a$ then $x^{-1} \in H_a$.

$$\text{Let } x \in H_a, \text{ then } xa = ax, \text{ so } a = x^{-1}*(xa) = x^{-1}*(a*x) = (x^{-1}*a)*x$$

$$a * x^{-1} = ((x^{-1}*a)*x) * x^{-1} = (x^{-1}*a)*(x*x^{-1}) = x^{-1}*a$$

Thus $x^{-1} \in H_a$.

27. Find all subgroups of the group given in Exercise 17.

27. $\{f_1\}, \{f_1, f_2, f_3, f_4\}, \{f_1, f_3, f_5, f_6\}, \{f_1, f_3, f_7, f_8\},$
 $\{f_1, f_5\}, \{f_1, f_6\}, \{f_1, f_7\}, \{f_1, f_8\}, D_4.$

答:

补充 9.4 同态定理、正规子群和同态核

28. Let $(S_1, *)$, $(S_2, *')$, and $(S_3, *'')$ be semigroups, and let $f: S_1 \rightarrow S_2$ and $g: S_2 \rightarrow S_3$ be isomorphisms. Show that $g \circ f: S_1 \rightarrow S_3$ is an isomorphism.

proof: $(g \circ f)(x * y) = g(f(x * y)) = g(f(x) *' f(y))$
 $= g(f(x)) *'' g(f(y)) = (g \circ f)(x) *'' (g \circ f)(y)$.

one-to-one: suppose $(g \circ f)(a) = (g \circ f)(b)$, $g(f(a)) = g(f(b))$, $f(a) = f(b)$, $a = b$.

onto: $\forall z \in S_3$ 有 $g(y) = z$; $\forall y \in S_2$ 有 $f(x) = y$;

24. Let $A = \{0, 1\}$ and consider the free semigroup A^* generated by A under the operation of catenation. Let N be the semigroup of all nonnegative integers under the operation of ordinary addition.

(a) Verify that the function $f: A^* \rightarrow N$, defined by $f(\alpha) =$ the number of digits in α , is a homomorphism.

(b) Let R be the following relation on A^* : $\alpha R \beta$ if and only if $f(\alpha) = f(\beta)$. Show that R is a congruence relation on A^* .

(c) Show that A^*/R and N are isomorphic.

Proof: Let $A = \{0, 1\}$ and consider (A^*, \cdot) , $(N, +)$.

(1) $f(\alpha) = \text{length}(\alpha)$, show $f: A^* \rightarrow N$ is homomorphism.

$f(\alpha \cdot \beta) = f(\alpha\beta) = \text{length}(\alpha) + \text{length}(\beta) = f(\alpha) + f(\beta)$

(2) R : $f(\alpha) = f(\beta)$, show R is congruence relation.

First show R is equivalence relation.

if $f(\alpha) = f(\beta)$ and $f(\gamma) = f(\delta)$, then $f(\alpha \cdot \gamma) = f(\beta \cdot \delta)$

(3) A^*/R and N is isomorphic.

$(A^*/R, *) : [\alpha] * [\beta] = [\alpha \cdot \beta]$.

Let $g([\alpha]) = \text{length}(\alpha)$, (1) show $g: A^*/R \rightarrow N$ is homomorphism.

$g([\alpha] * [\beta]) = g([\alpha \cdot \beta]) = \text{length}(\alpha) + \text{length}(\beta) = g([\alpha]) + g([\beta])$

(2) onto : $\forall x \in N$, let $\alpha = 00 \cdots 0$ (x factors), $g([\alpha]) = x$.

(3) one-to-one : suppose $g([\alpha]) = g([\beta])$,

$\text{length}(\alpha) = \text{length}(\beta)$, so $f(\alpha) = f(\beta)$, then $\alpha R \beta$, $[\alpha] = [\beta]$.

28. Let G be an Abelian group and n a fixed integer. Prove that the function $f: G \rightarrow G$ defined by $f(a) = a^n$, for $a \in G$, is a homomorphism.

proof: (数学归纳法证)

1. because $ab = ba$, $ab * ab = aabb = a^2b^2$,

2. if $(ab)^n = a^n b^n$, then $ab * (ab)^n = ab * a^n b^n = a a^n b b^n = a^{n+1} b^{n+1}$

Hence, $f(ab) = (ab)^n = a^n b^n = f(a)f(b)$.

30. Let G be a group with identity e . Show that the function $f: G \rightarrow G$ defined by $f(a) = e$ for all $a \in G$ is a homomorphism.

Proof: Let $a, b \in G$.

$$f(a*b) = e = e*e = f(a)*f(b)$$

Thus f is a homomorphism.

32. Let G be a group. Show that the function $f: G \rightarrow G$ defined by $f(a) = a^{-1}$ is an isomorphism if and only if G is Abelian.

Proof: (1) Suppose f is isomorphism,

$$f(xy) = (xy)^{-1} = f(x)f(y) = x^{-1}y^{-1}$$

so $xy = ((xy)^{-1})^{-1} = (x^{-1}y^{-1})^{-1} = yx$. G is Abelian.

(2) Suppose G is Abelian.

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y), \text{ homomorphism.}$$

onto: $\forall x \in G, f(x^{-1}) = (x^{-1})^{-1} = x$.

one-to-one: suppose $f(x) = f(y), x^{-1} = y^{-1}$,

$xx^{-1} = e = yy^{-1}$, right cancellation $x = y$.

34. Let $G = \{e, a, a^2, a^3, a^4, a^5\}$ be a group under the operation of $a^i a^j = a^r$, where $i + j \equiv r \pmod{6}$. Prove that G and Z_6 are isomorphic.

Proof: Let $f: G \rightarrow Z_6$, where $f(a^i) = [i]$. $f(e) = [0]$.

(1) show f is a homomorphism.

$$\text{Let } a^i, a^j \in G, f(a^i a^j) = f(a^r) = [r] = [i] +_6 [j] = f(a^i) +_6 f(a^j)$$

Thus f is a homomorphism.

(2) show f is onto.

$$\text{Let } [x] \in Z_6, \text{ then } f(a^x) = [x].$$

(3) show f is one-to-one.

$$\text{Let } f(a^x) = f(a^y) = [x]. \text{ so } x \equiv y \pmod{6},$$

But $0 \sim 5$ is distinct in $(\text{mod } 6)$, so $x = y, a^x = a^y$

Thus f is one-to-one.

4. Let G_1 and G_2 be groups. Show that the function $f: G_1 \times G_2 \rightarrow G_1$ defined by $f(a, b) = a$, for $a \in G_1$ and $b \in G_2$, is a homomorphism.

Proof: Let (a, b) and $(c, d) \in G_1 \times G_2$.

$$f((a, b) * (c, d)) = f(a * c, b * d) = a * c = f(a, b) * f(c, d)$$

Thus f is homomorphism.

10. Let $G = S_3$. Determine all the left cosets of $H = \{f_1, g_1\}$ in G .

Solution:

If $a \in H$, then $aH = H$. Thus $fH = g_1H = H$.

$$f_2H = \{f_2, g_3\}$$

$$f_3H = \{f_3, g_2\}$$

$$g_2H = \{g_2, f_3\} = f_3H$$

$$g_3H = \{g_3, f_2\} = f_2H$$

The distinct left cosets of H in S_3 are H , f_2H , and f_3H .

18. Let N be a subgroup of a group G , and let $a \in G$. Define

$$a^{-1}Na = \{a^{-1}na \mid n \in N\}.$$

Prove that N is a normal subgroup of G if and only if $a^{-1}Na = N$ for all $a \in G$.

Proof: (1) If N is normal subgroup,

then $\forall a \in G, aN = Na$, and $e \in N$.

so $a^{-1}Na = Na^{-1}a = Ne = N$.

(2) If $a^{-1}Na = N$ for all $a \in G$,

let $n \in N, a^{-1}na = n'$ for some $n' \in N$.

$a \cdot a^{-1}na = a \cdot n', na = an' \in aN$, Then $Na \subseteq aN$.

Similarly, let $n \in N, n = a^{-1}n'a, an = a^{-1}n'a = n'a$, Then $aN \subseteq Na$.

Hence, $aN = Na$, N is normal subgroup.

20. Find all the normal subgroups of S_3 .

Solution: (1) find all subgroups.

$$\{f1\}, \{f1, g1\}, \{f1, g2\}, \{f1, g3\}, \{f1, f2, f3\}, \{f1, f2, f3, g1, g2, g3\}$$

(2) select normal subgroups.

$$\{f1\}, \{f1, f2, f3\}, \{f1, f2, f3, g1, g2, g3\}.$$

28. Let G be an Abelian group and N a subgroup of G . Prove that G/N is an Abelian group.

Proof:

(1) As G be an Abelian group,

then $\forall a \in G, \forall h \in N, ah = ha$; so $aN = Na$,

then N is a normal subgroup.

(2) G/N is $= \{aN \mid a \in G\}, N = eN = [e]$.

$(aN)(bN) = [a]*[b] = abN$, by Theroem 3 corollary 1,

as $ab = ba, abN = baN = [b]*[a] = (bN)(aN)$.

Hence, G/N is an Abelian group.

30. Let H and N be subgroups of the group G . Prove that if N is a normal subgroup of G , then $H \cap N$ is a normal subgroup of H .

Proof: Prove that if N is a normal subgroup of G , then $H \cap N$ is a normal subgroup of H .

(1) show $H \cap N$ is a subset of H ;

$\forall x \in H \cap N, x \in H, H \cap N$ is a subset of H .

(2) show $H \cap N$ is a closure;

$\forall x, y \in H \cap N, x \in H$ and $y \in H, x * y \in H$; $x \in N$ and $y \in N, x * y \in N$; so $x * y \in H \cap N$.

(3) Since H and N are subgroups of $G, e \in N$ and $e \in H$,
so $e \in H \cap N$.

(4) $\forall x \in H \cap N, x \in H, x^{-1} \in H$, and $x \in N, x^{-1} \in N$;
so $x^{-1} \in H \cap N$.

(5) $\forall x \in H, x(H \cap N) = \{xn \mid n \in H \cap N\}$, let any $n_1 \in H \cap N$,
because $aN = Na, x * n_1 = n_2 * x$ for some $n_2 \in N$,
 $n_2 = x * n_1 * x^{-1}$,
since $x^{-1} \in H, n_1 \in H$, then $n_2 \in H$.
 $n_2 \in H \cap N$,

Thus $x(H \cap N) = (H \cap N)x$.

Hence, $H \cap N$ is a normal subgroup of H .

31. Let $f : G \rightarrow G'$ be a group homomorphism. Prove that f is one to one if and only if $\ker(f) = \{e\}$.

Proof: (1) show if $\ker(f) = e$, then f is one to one.

Suppose $\ker(f) = e$. Let $g_1, g_2 \in G$, and $f(g_1) = f(g_2)$.

Then $f(g_1 g_2^{-1}) = f(g_1) f(g_2^{-1}) = f(g_1) (f(g_2)^{-1}) = f(g_1) (f(g_1)^{-1}) = e$.

Hence $g_1 g_2^{-1} \in \ker(f)$, thus $g_1 g_2^{-1} = e$ and $g_1 = g_2$.

So f is one-to-one.

(2) show if f is one to one, then $\ker(f) = e$.

Suppose $f : G \rightarrow G'$ is one-to-one. Let $x \in \ker(f)$.

Then $f(x) = e' = f(e)$. Thus $x = e$ and $\ker(f) = \{e\}$.