1.1 1, 2

1.2 8, 9, 10, 12, 13, 14, 22

1.3 7, 8, 12, 19, 23, 28, 29

1.4 5, 9, 10, 14, 21, 27, 30, 32

1.5 1, 4, 7, 13, 17

1.6 1, 2, 8, 14

1.7 1, 2, 3, 6, 11, 13, 20, 21, 22

1.8

2.1 8, 9, 19, 20, 26, 27, 28

2.2 1, 2, 5

2.2 1, 2, 5

2.3 4, 5, 11, 22, 24, 26, 28, 29

2.4 1, 5, 18, 24, 30, 35, 37, 38, 42, 43

2.5 3, 17, 18, 19, 24, 26, 29, 38, 42

2.6 11, 12, 13, 18

2.7 4, 5, 7

2.8 4, 6, 7, 8, 11, 12

2.9 1, 2, 3

2.10

2.11 3, 4, 11, 14, 18, 19, 25, 26, 28

3.1 1, 2, 3

3.2 3, 9, 12, 21, 23, 24, 25

3.3 1, 3, 5, 6, 8

4.1 9, 11, 13, 16, 23, 36, 37

4.2 2, 3, 7, 9

4.3 3, 4, 17, 20, 24, 27

4.4 1, 9, 10, 11

4.5 2, 3, 10, 11, 12, 13, 19, 26, 28

4.6 3, 4, 7, 11

4.7 3, 4

5.1 3, 8, 9, 10

5.2 2, 3, 6, 10, 11, 14, 17

5.3 1, 4, 6, 10, 13, 14

5.4 1, 3, 5, 6

~~5.5 2, 3, 4~~

~~5.6 3, 4, 7, 8, 11, 14, 15~~

Chapter 1 / Set theory

Section 1.1

① If $a \cdot b = a$ and $a \cdot b = b \cdot a$, then $a = b \cdot a$ and $ab = ba$

$\therefore a = a$ $\quad\therefore$ S has one element

② a) $a \cdot b \neq b \cdot a$ unless $a = b$ $\quad [a \cdot b = a - b$

$a - b = b \cdot a$ with $a = b$

and $a \cdot b = b \cdot a$

$a - b = a - b$ and $a - a = b - b$

b) $(a-b) \circ c \neq a \circ (b \circ c)$ $\quad \boxed{a \cdot b = a - b}$

$a - b - c \neq a - (b - c)$

$a - b - c \neq a - b + c$ with $c = 0$, equality holds

c) $\boxed{a \cdot b = a - b}$

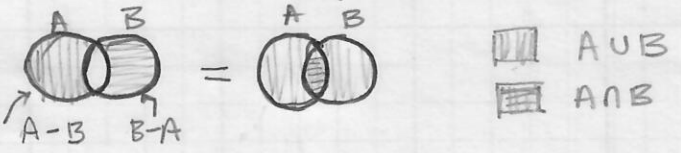
$a \cdot 0 = a \not\Rightarrow a - 0 = a$

d) $\boxed{a \cdot b = a - b}$

$a \cdot a = 0 \not\Rightarrow a - a = 0$

Section 1.2

⑧ $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$



let $x \in A$ and $x \notin B$ then $x \in (A - B)$

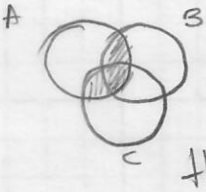
and $x \notin A \cap B$

$\therefore x \in (A - B) \cup (B - A)$ and $x \in (A \cup B) - (A \cap B)$

$(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$

Section 1.1

(9) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$



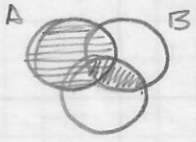
$(A \cap B) \subset (B \cup C)$ and

$(A \cap C) \subset (B \cup C)$

then from the diagram $(A \cap B) \subset B$ and $(A \cap C) \subset C$

$\therefore A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(10) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$



$(B \cap C) \subset (A \cup B)$ and

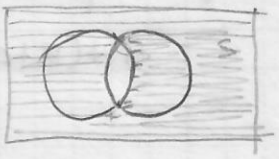
$(B \cap C) \subset (A \cup C)$

and from the diagram

$\therefore A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

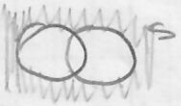
(12) (a) $(A \cap B)' = A' \cup B'$

$A \neq B \subset S$ $\quad A' = S - A$ $\quad B' = S - B$



then $(A \cap B) \subset A$ similarly $(A \cap B) \subset B$

so $(A \cap B)' \subset A' \cup B' \Rightarrow (A \cap B)' = A' \cup B'$



(b) $(A \cup B)' = A' \cap B'$

Using results from (a) and $(C')' = C$

$(A' \cup B')' = ((A \cap B)')' = A \cap B$

$(A \cup B)' = (A')' \cap (B')' = A' \cap B'$

$\Rightarrow (A \cup B)' = A' \cap B'$

(13) $A + B = (A - B) \cup (B - A)$ and $A \cdot B = B \cap A$

(a) $A + B = B + A = (A - B) \cup (B - A)$

$= (B - A) \cup (A - B) = B + A$

(b) $A + \emptyset = A = (A - \emptyset) \cup (\emptyset - A)$

$= A \cup \emptyset = A$

(c) $A \cdot A = A$

$= A \cap A = A$

(d) $A + A = \emptyset$

$= (A - A) \cup (A - A) = \emptyset \cup \emptyset$

$= \emptyset$

(e) $A + (B + C) = (A + B) + C$

$= (A - (B + C)) \cup ((B + C) - A)$

$= C + (A + B)$ FROM (a)

$= C - (A + B) \cup ((A + B) - C)$

using the proof for the theorem

$A + (B + C) = (A \cup B \cup C) - \{[(A \cap B) \cup (A \cap C) \cup (B \cap C)] - (A \cap B \cap C)\}$

then $C + (A + B) = C \cup A \cup B - \{[(C \cap A) \cup (C \cap B) \cup (A \cap B)] - (A \cap B \cap C)\} = A + (B + C)$

(f) if $A + B = A + C$, then $B = C$

using (e) $(A + A) + B = (A + A) + C$

using (d) $\emptyset + B = \emptyset + C$

using (b) $B = C$

(g) $A \cdot (B + C) = A \cdot B + A \cdot C$ using (g)

$= A \cap (B - C) \cup (C - B) = (A \cap (B - C)) \cup (A \cap (C - B))$

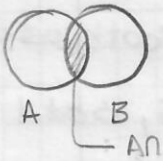
and $A \cap (B - C) = (A \cap B) - (A \cap C)$ it follows

$A \cdot (B + C) = [(A \cap B) - (A \cap C)] \cup [(A \cap C) - (A \cap B)] =$

$= A \cap B + A \cap C = A \cdot B + A \cdot C$ ☺

(14) C is finite ; A & B finite ; $m(C) = [C]$

$m(A \cup B) = m(A) + m(B) - m(A \cap B)$



$m(A)$ = elements of A not in B
$m(B)$ = elements of B not in A
$m(A \cap B)$ are elements that are in both A & B

∴ the number of element in the intersection must be subtracted to get an accurate count

$m(A \cup B) = m(A) + m(B) - m(A \cap B)$

(22) A set with n elements has 2^n subsets

By assigning an n-binary number to each subset (combination) we find that a set with n elements would have 2^n subsets

(b) choose m, the number of combinations

$C(n, m) = n! / (m!(n-m)!)$

Section 1.3

(7) $g = S \to T$; $h = S \to T$; $f : T \to U$ is 1-1

$f \circ g = f \circ h$ then $g = h$

$f(g(s)) = f(h(s))$ if $f(s_1) = f(s_2)$ implies $s_1 = s_2$

f is one to one ; by definition then

$g = h$

(8) $f : S \to T$ is defined by $f(s) = 1$ if s is even
$f(s) = -1$ if s is odd

(a) $f : S \to T$ is a function from S to T as defined

$f(s) = 1$ & $f(s) = -1$ for even and odd on T
no integer is both odd and even

(b) $f(s_1 + s_2) = f(s_1) f(s_2)$ from even $= 2n$; odd $= 2n+1$

$2n + 2n_1 = 2(2n)$	even	$(2n)(2n) = 2(2n)$	even
$2n + (2n+1) = 2(2n) + 1$	odd	$(2n)(2n+1) = 2(2n+n)$	even
$(2n+1)(2n+1) = 2(2n+1)$	even	$(2n+1)(2n+1) = 2(2n^2 + 2n + 1)$	odd

does not work

however if $f(s) = (-1)^s$

then $f(s_1+s_2) = (-1)^{s_1+s_2} = (-1)^{s_1}(-1)^{s_2} = f(s_1)(f(s_2))$

so s_1+s_2 is even if $s_1 \neq s_2$ are both even or both odd

s_1+s_2 is odd if s_1 is even and s_2 is odd or s_1 is odd and s_2 is even.

(c) Use $s_1 = s_2 = 1$.

Then $s_1 s_2 = 1$. We get $f(s_1 s_2) = f(1) = -1$,

but $f(s_1)f(s_2) = f(1)f(1) = (-1)(-1) = 1$ FALSE

(12) (a) The function f is not well defined. Let $s = 1/2$, which is an $\in S$. Note $s = 2/4$. But $2^1 2^3 \neq 2^2 3^4$.

Then, there is not a unique element $f(s)$ in T

(b) if $s \in S$ then $s = u/v$ where $v \in \mathbb{Z} \geq 0$ and $a \in \mathbb{Z}$

for a fixed s, using $\{ v \in \mathbb{N} \mid vs \in \mathbb{Z} \}$

This is a nonempty subset of the natural numbers $\mathbb{N}$ it has an infimum n, then $ns = m$ is in $\mathbb{Z}$. Thus $s = m/n$

Define $f(s) = 2^m 3^n$. This defines a function $f: S \to T$!

(19) $f(s) = s^2 + as + b$ with $a \neq 0$ $f(a) = f(-2a) = 2a^2 + b$

$f(a) = a^2 + a \cdot a + b = 2a^2 + b$

$f(-2a) = 4a^2 - 2a \cdot a^2 + b = 2a^2 + b$

with $a = 0$ $f(1) = f(-1) = 1 + b$ not $1 - b = -1$

$f(s) = b - 1 - \frac{a^2}{4}$; $s^2 + as + b = b - 1 - \frac{a^2}{4}$ so $\left(s + \frac{s}{2}\right)^2 = -1$

then f is not onto

(20) PROVE $|z+w|^2+(z-w)^2 = 2(|z|^2+|w|^2)$

$|z+w|^2+|z-w|^2 = (z+w)(\overline{z+w}) + (z-w)(\overline{z-w}) = z\bar{z} + w\bar{w} +$

$+ zw + wz + z\bar{z} + w\bar{w} - zw - wz = z(z\bar{z} + w\bar{w}) = 2(|z|^2+|w|^2)$ ☺

(21) Consider the set $A = \{a+bi \mid a,b \in \mathbb{Z}\}$ Prove that there is a 1-1 correspondence of A onto $\mathbb{N}$. (A is called the set of Gaussian...

interpreting solution notes

defining a mapping from A to $\mathbb{N}$: if $a+bi$ is in A then

if $a \geq 0$ and $b \geq 0 \Rightarrow f(a+bi) = 2^a 3^b$

$a \geq 0$ and $b < 0 \rightarrow f(a+bi) = 5^a 7^{-b}$

$a < 0$ and $b \geq 0 \Rightarrow f(a+bi) = 11^{-a} 13^b$

$a < 0$ and $b < 0 \Rightarrow f(a+bi) = 17^{-a} 19^{-b}$

By the unique factorization of positive integers into products of powers of prime numbers $\rightarrow$ f is a well defined function from A to N.

(22) $x^n + \alpha_1 x^{n-1} + \cdots + a_{n-1}x + \alpha_n \ldots$ $\bar{a}$ must also be a root.

Suppose a is a root then $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$

then $\overline{(a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n)} = 0 \Rightarrow \bar{a}^n + \bar{\alpha}_1 \bar{a}^{n-1} + \cdots + \bar{\alpha}_n = 0$

for $\alpha_i \in \mathbb{R}$ then $\bar{\alpha}_i = \alpha_i$ and

$\bar{a}^n + \alpha_1 \bar{a}^{n-1} + \cdots + \alpha_n = 0 \Rightarrow p(\bar{a}) = 0$ and $\bar{a}$ is a root of $p(x)$

Chapter 2 / Groups

Section 1.1

(8) $(a*b)^n = a^n \cdot b^n \ \forall \ n$

by induction

$(a \cdot b)^1 = a^1 \cdot b^1$ we wish to prove that $(a \cdot b)^k = a^k \cdot b^k \ \forall n$

then $(a \cdot b)^{k+1} = a^{k+1} \cdot b^{k+1}$

$(a^k \cdot b^k)(a \cdot b) = a^{k+1} \cdot b^{k+1}$ then by MI

$(a \cdot b)^n = a^n \cdot b^n \ \forall n$ ∎

(9) $a^2 = e \ \forall \ a \in G \Rightarrow G$ is abelian

$a, b \in G$ $a^2 = e$ for all a in G. Then $b^2 = e$ and $(ab)^2 = e$. Then $(ab)^2 = e = a^2 b^2$ and from (8) G is abelian

(19) In S_3 --- $x^2 = e$

The four elements satisfying x^2 are e, (12), (13), (23), and three elements satisfying $y^3 = e$; e, (123), (132)

(20) Using (19) then for S_4 which satisfy $x^4 = e$

We have e, f, f^2, f^3 with respective groups of 2, 3

f sends $x_1 \to x_2$, $x_2 \to x_3$, $x_3 \to x_4$, $x_4 \to x_1$

g send s $x_1 \to x_3$, $x_3 \to x_2$, $x_2 \to x_4$, $x_4 \to x_1$

g^2, g^3 h which sends $x_1 \to x_2$, $x_2 \to x_4$, $x_4 \to x_3$, $x_3 \to x_1$, h, h^2, h^3 and

6 interchanges of 2

Section 2.1

(26) G is a finite group $\Rightarrow a^n = e$

Let $a \in G$, with G of order k; then $a, a^2, a^3, \ldots a^{k+1}$ are $k+1$ elements in G which only has k elements.

Thus 2 of $a, a^2, \ldots a^{k+1}$ are equal;

that is $a^i = a^j$ for some $1 \le i < j \le k+1$ and so

$a^{j-1} = e$ where

$0 < j - i \le k$. Let $n = j - i$

(27) $m > 0 \Rightarrow a^m = e \; \forall \; a \in G$

If t is the product of all n's for all the a's in G then

$a^t = e$ for all a in G.

(28) Let G be a set...

Let $a \in G$. Then $aG = \{a \cdot a_1, a \cdot a_2, \ldots a \cdot a_n\} \subseteq G$

given that G is closed under $\cdot$. Also $a \cdot a_1, a \cdot a_2 \ldots a \cdot a_n$ are all distinct. For, if $a \cdot a_i = a \cdot a_j$ for some $i \neq j$

$\Rightarrow a_i = a_j$ by (3). Since $a \in G$, $\exists i$ such that $a = a \cdot a_i$ for some $1 \le i \le n$. This is $a_i \Rightarrow \Leftarrow$

So G satisfies identity law.

Now $e \in G = \{a \cdot a_1, a \cdot a_2 \ldots a \cdot a_n\}$ implies $\exists j$ such that

$e = a \cdot a_j = a_j \cdot a$ So, a_j is inverse of a in G

Hence, G satisfies inverse law.

Therefore, G is a group

Section 2.3

① Suppose that G...

There is a unique solution for $ax = y$ for $a, b \in G$

if $a \in G$ then taking $a = b$ $\exists$ an element $e \in G \ni$

$e \cdot a = a$

let $b \in G$, now $ax=b \Rightarrow e(ax) = eb$

also $e(ax) = (ea)x = ax = b$

$\therefore eb = b$ for all b in G

$\therefore$ e is the identity element in G

now $a \in G$; since $e \in G$ $\exists$ a unique solution in $G \Rightarrow c$

$\therefore ca = e \Rightarrow$ the left inverse of a is c

then the left inverse exists for every element in G

$\therefore$ similarly we can prove that right inverse exists for every element in $G \Rightarrow G$ is a group!

(2) If G is a finite set... $x=b$, $y=c$

Closure and associativity are given, to prove identity

Consider the set $\{a, a^2, \ldots a^n\} \subseteq G$ since G is finite $a^n = a^m$ for some $m > n \geq 1$.

Set $e = a^{m-n}$, we need to prove that e is an identity

let $x \in G$ and write $ex = y \in G$ to prove $x=y$. Multiplying by a^n

$$a^n y = a^n ex = a^n a^m x = a^m x = a^n x$$

using cancelation implies $y=x$ as desired; now

Let $a \in G$ and choose $m-n > 1$ such that $m > n$ and $a^n = a^m$. then $a^1 = a^{m-n+1}$ so $ea = a^{m-n+1}$

$\Rightarrow e = a \cdot a^{m-n-1} = a^{m-n-n} a$ and so since $m-n-1 > 0$, we see that a^{m-n-1} makes sense is an inverse to a

the inverse exists $\Rightarrow G$ is a group

(3) Let G be a group...

let $a, b \in G$ then $(ab)(ab)(ab)(ab)(ab) = (ab)^5 = a^5 b^5$ and cancelation or multiplication by inverses implies that $(ba)^4 = b(ab)(ab)(ab)a = a^4 b^4$. Likewise $(ab)(ab)(ab) = (ab)^3 = a^3 b^3$ which implies $(ba)^2 = a^2 b^2$

again by cancelation. But $(ba)^4 = (ba)^2(ba)^2 = a^2b^2a^2b^2$ so that $a^4b^4 = a^2b^2a^2b^2$. Cancelation again implies $a^2b^2 = b^2a^2$. Now using $(ba)^2 = a^2b^2$ switching a and b, we have $(ab)^2 = b^2a^2$ so that $a^2b^2 = b^2a^2 = (ab)^2 = (ab)(ab)$. cancelation of the end-terms one last time leads to $ab = ba \Rightarrow G$ is abelian ☺

Section 3

(4) Verify that $Z(G)$

By definition $Z(G) = \{g \in G : gx = xg \ \forall \ x \in G\}$

since $ex = xe \ \forall \ x \in G$, we have $e \in Z(G)$

Suppose $g, h, \in Z(G)$ so that $gx = xg$ and $hx = xh \ \forall \ x = in G$

then $(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh) \Rightarrow gh \in Z(G)$

now $g \in Z(G)$, then $gx = xg$ for every $x \in G$.

Multiplying left & right by $g^{-1} \Rightarrow xg^{-1} = g^{-1}x$ for every $x \in G$

This shows that $x^{-1} \in Z(G)$ $\therefore$ the inverse of every element in $Z(G)$ is also in $Z(G)$

$\therefore$ $Z(G)$ is a subgroup.

(5) If $C(a)$ is the centralizer of a in G ...

Suppose $x \in Z(G)$ then $xa = ax$ for each $a \in G$ and so $x \in C(a)$ for each $a \in G$. Then $x \in \bigcap_{a \in G}$ so that $Z(G) \subseteq \bigcap_{a \in G} C(a)$. Conversely, let $x \in \bigcap_{a \in G} C(a)$ Let $a \in G$, then since $x \in C(a)$, $xa = ax$ but this holds for all a $\therefore$ $x \in Z(G) \Rightarrow \bigcap_{a \in G} C(a) \subseteq Z(G)$

Thus these two imply that $\bigcap_{a \in} C(a) = Z(G)$

(11) If G is an abelian group. . .

Let H be a subset of G such that $H = \{a \in G \mid a^2 = e\}$

$a^2 = e$, using the subgroup test

let x and $y \in H$ then $x^2 = y^2 = e$ and

$(xy)^2 = xy \cdot xy$ (since G is abelian) $\Rightarrow e \cdot e = e$

$\therefore xy \in H$ so H is a subgroup of G

(22) If A and B are finite subgroups

from solution to (19)

Suppose that $x = a_1 b_1$ and $y = a_2 b_2$ are in AB where a_1, a_2 are in A ($\in A$) and $b_1, b_2 \in B$. Since G is abelian then $xy = a_1 b_1 a_2 b_2 = a_1 a_2 b_1 b_2 \in AB$ and $x^{-1} = (a_1 b_1)^{-1} = b_1^{-1} a_1^{-1} = a_1^{-1} b^{-1} \in AB$

$\Rightarrow AB$ is a subgroup of G

now if for some distinct pairs $(a_1 b_1), (a_2 b_2)$ we have $a_1 b_1 = a_2 b_2$. But this implies that $a_2^{-1} a_1 = b_2 b_1^{-1}$ and since the left side is in A and the right side is in B, the elements on both sides are in $A \cap B$. Then $a_1 = a_2 c$ and $b_1 = c^{-1} b_2$ where $c \in A \cap B$. But if $c \in A \cap B$ and if $a \in A$, $b \in B$ then $a_1 = ac \in A$ and $b_1 = c^{-1} b \in B$ and $a_1 b_1 = (ac)(c^{-1} b) = ab$. Then there are exactly $|A \cap B|$ pairs giving rise to the same ab. Thus $|AB| = mn / |A \cap B| = |A||B| / |A \cap B|$. If $|A|$ and $|B|$ are relatively prime then $A \cap B = \{e\}$ so that $|A \cap B| = 1$

Section 2.3

(24) If H is a subgroup of G, let $N = \bigcap_{x \in G} x^{-1}Hx$ ---

interpreted from solution manual

N is a subgroup because the intersection of any number of subgroups of G is a subgroup of G.

If $x, y \in G$ then $y^{-1}(x^{-1}Hx)y = (xy)^{-1}H(xy)$ and as x runs over G with fixed y then xy runs over all the elements of G. Thus $y^{-1}(n(x^{-1}Hx))y = n(xy)^{-1}H(xy)$ as x runs over G, $= nx^{-1}Hx$, as x runs over G by above $\neq y^{-1}Ny = N$

(26) Let G be a group, H a subgroup of G.

The relation $a \sim b$ is an equivalence relation if $ab^{-1} \in H$ and

$$[a] = Ha = \{ha \mid h \in H\}$$

let k be the number of distinct classes $Ha_1, \dots Ha_k$,

$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$ and we know that $Ha_j \cap Ha_i = \emptyset$ if $i \neq j$

Any Ha_i has $|H|$ = order of H number of elements. Map $H \to Ha_i$ by sending $h \to ha_i$. We claim that this map is 1-1 for if $ha_i = h'a_i$ then by cancellation in G we could have $h = h'$; thus the map is 1-1. It is definitely onto by the definition of Ha_i. So H and Ha_i have the same number $|H|$ of elements since $G = Ha_1 \cup \dots \cup Ha_k$ and Ha_i are disjoint and each Ha_i has $|H|$ elements we have that $|G| = k|H|$. Thus $|H|$ divides $|G|$

(27) If H is a finite subgroup of G ...

To prove that Ha and Hb have the same number of elements define $f: Ha \to Hb$ by $f(ha) = hb$ for all $ha \in Ha$

Let $x, y \in Ha$ then $x = h_1a$ $y = h_2a$ for some $h_1, h_2 \in H$

let $f(x)=f(y)$ or $f(h_1a)=f(h_2a)$ or $h_1b=h_2b$

$\therefore h_1=h_2$. Then $h_1a=h_2a$ or $x=y$

$\Rightarrow f$ is a one to one mapping

With $x\in H_b$ and $x=h_1b$ for $h_1\in H$ also

for $h_1\in H$ $\exists\, h_1a\in Ha$ such that $f(h_1a)=h_1b$

Thus $\forall x_1\in H_b$ $\exists\, h_1a=y\in Ha$ such that $f(y)=x$

Therefore, $Ha\to H_b$ is both 1-1 and onto, so

Ha and H_b have the same number of elements

(28) Let M, N be subgroups of G such that $x^{-1}Mx\subset M$ and ...

interpretation from solution set

If mn, m_1n_1 are in MN where m, n_1 are in M and n, n_1 are in N then $(mn)(m_1n_1)=(mnm_1mn^{-1})nn_1$ and by the hypothesis on M, nmn^{-1} is in M thus $mnmn^{-1}$ is in M, and nn_1 is in N. Therefore $(mn)(m_1n_1)$ is in MN hence MN is closed under the product in G.

Also $(mn)^{-1}=n^{-1}m^{-1}=(n^{-1}m^{-1}n)n^{-1}$ so is in MN since $n^{-1}m^{-1}n$ is in M and n^{-1} is in N. Thus MN is a subgroup of G. If $x\in G$ then $x^{-1}(MN)x=(x^{-1}Mx)(x^{-1}Nx)\subset MN$ by the hypothesis on M and N

(29) If M is a subgroup of G such that $x^{-1}Mx\subset M$ $\forall x\in G$,

interpretation from solution set

Since $x^{-1}Mx\subset M$ $\forall x$ in G, $xMx^{-1}=(x^{-1})^{-1}M(x^{-1})\subset M$

thus $M=x^{-1}(xMx^{-1})x\in x^{-1}Mx\subset M$.

This forces $M=x^{-1}Mx$

Section 2.4

① Verify that the relation $\sim$ is an equivalence relation.

a) $S = \mathbb{R}$, $a \sim b$ if $a - b$ is rational

$a - a = 0$ is rational if $a - b$ is rational then $b - a = -(a-b)$ is rational and if $a - b$ and $b - c$ are rational then $a - c = (a-b) + (b-c)$ is rational.

Thus $a \sim a$, if $a \sim b$ then $b \sim a$, and if $a \sim b$, $b \sim c$ then $a \sim c$. Then $\sim$ is an equivalence relation on S ☺

(b) $a \sim b$ if $|a| = |b|$. Then $z = a + bi \Rightarrow |z| = \sqrt{a^2 + b^2}$

the equality establishes an equivalence relation

(c) $a \sim b$ if a, b are parallel

The relation is symmetric but fails to be reflexive (or transitive) if a line is not parallel to itself then $\sim$ is not reflexive, however if a line is parallel to itself $\sim$ is an equivalence relation

④ Having the same color eyes is an equivalence relation in the set of all people

⑤ Let G be a group and H a subgroup of G.

Because $a^{-1}a \in H$, we know that $a \sim a$ (reflexivity)

Given $a \sim b$ we need to verify that $b \sim a$ (symmetry)

We are given $a^{-1}b \in H$. Because H is a subgroup, it contains the inverse of each of its elements, and so $(a^{-1}b)^{-1} \in H$

But $(a^{-1})b^{-1} = b^{-1}a$, and if $b^{-1}a \in H$, then $b \sim a$

Given $a \sim b$ and $b \sim c$, we need to see that $a \sim c$ (TRANSITIVITY)

We are given $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$, which shows $a \sim c$

Now, if $a \sim b$, then $a^{-1}b = h$ for some $h \in H$, and then $b = ah$

On the other hand, if $b = ah$, then $a^{-1}b \in H$. This shows that $[a] = aH$

(18) Using the results of problem 15 and 16, prove that if p is...

Let $p=7$. We have $(7-1)! = 6! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6$. Rearranging grouping together pairs of inverses modulo 7 note $2\cdot 4 \equiv (1 \bmod 7)$ and $3\cdot 5 \equiv 1 \pmod{(7)}$

Hence $6! \equiv 1\cdot(2\cdot 4)\cdot(3\cdot 5)\cdot 6 = 1\cdot 6 = -1 \pmod 7$

so $(p-1)! = 1\cdot 2\cdot 3\cdots(p-3)(p-2)(p-1) \equiv 1\cdot(p-1) \equiv -1 \pmod p$

(24) If p is a prime number of the form $4n+3$ show that...

If p is a prime of the form $4n+3$ then U_p is a group of order $p-1 = 4n+2$ so its order is not divisible by 4. However, if $a^2 \equiv -1 \bmod p$ then $[a]$ has order 4 in U_p which would force 4 to divide $|U_p|$, a contradiction. So there is no such a.

(30) If in G $a^5 = e$ and $aba^{-1} = b^2$, find $o(b)$ if $b \neq e$

from solution set

Since $aba^{-1} = b^2$, by $a^r b a^{-r} = b^k$ where $k = i^r$

$a^5 b a^{-5} = b^{32}$ since $a^5 = e$ we end up with $b^{32} = b$ and so $b^{31} = e$. Because 31 is a prime and $b \neq e$ we know that $o(b) = 31$

(35) If $f \in A(S)$ has order p, p a prime, and S is a finite

from solution set

The orbits of the elements of S under f are the equivalence classes of an equivalence relation so are equal or disjoint. If f has order p and $f(s) \neq s$ for every s in S then each such orbit has p elements by $f^i(s) = s$ only if $i = p$. But then $n = kp$ where k is the number of distinct orbits under f this says that $p|n$, contrary to $(n,p) = 1$

Section 2.4

(37) In a cyclic group of order n,

Let $G = \langle x \rangle$ be a cyclic group which order is n.

Then, $n = |G| = \sum_{1 \le m \le n} |\text{elements of order } m|$

$= \sum_{m|n} |\text{elements of order } m|$

G has a unique cyclic subgroup of order m for each $m|n$, $\langle x^{n/m} \rangle$ so if each subgroup has a total of $\phi(m)$ generators then $n = \sum_{m|n} \phi(m)$ ... I get lost...

If G is cyclic of order n and a a generator G then $b = a^{n/m}$ has order m as do all the elements $a^{kn/m}$ where $(k,m) = 1$

If $(a^i)^m = e$ then $n|im$, hence $i = mj/n$. Thus the only elements of order m are the elements $b^{kn/m}$ where k is relatively prime to m, and there are $\phi(m)$ such.

(38) Show that $n = \sum_{m|n} \phi(m)$

G is a cyclic group so $n = |G|$ for any $m|G$, $\exists\, x \in G = O(x) = m$. Thus suppose that if Z_m it the of all elements of cyclic group G with order m: $Z_m \neq \emptyset \Leftrightarrow p|n$

so $|G| = n = \sum_{m|n} |Z_m| = \sum_{m|n} \phi(m)$

(42) Using Wilson's theorem

from solution set

$(p-1)! \equiv -1 \pmod p$ thus $1 \cdot 2 \cdots (p-1)/2 \cdots -(p-1) = p-1 =$

$= (p-1) \equiv -1 \pmod p$.

If $y = 1 \cdot 2 \cdots (p-1)/2$ then, since $p-1 \equiv -1 \pmod p$

$p-2 \equiv -2 \pmod p, \ldots, (p+1)/2 \equiv (p-1)/2 \pmod p$ we

get $z = (p+1)/2 \cdots (p-1) \equiv (-1)^{(p-1)/2} 1 \cdot 2 \cdots (p-1)/2 \equiv (-1)^{(p-1)/2} y \pmod p$

thus $-1 \equiv (p-1) \equiv yz(-1)^{(p-1)/2} y^2 \pmod p$

If $p = 4n+1$ then $(p-1)/2 = 2n$ is even, hence

$(-1)^{(p-1)/2} = 1 \Rightarrow y^2 \equiv -1 \pmod p$

(43) Let G be an abelian group of order n, $a_1, \ldots, a_n$ from the solution set

(a) $a_1 a_2 \cdots a_n$ is the product of those elements of G which are their own inverses. Since e and b are the only elements of G with this property, we have that $a_1 a_2 \cdots a_n = eb = b$

(b) let $b \neq e$ and $c \neq e$, $b \neq c$, such that $b^2 = c^2 = e$; then $(bc)^2 = b^2c^2 = e$. Thus any such pair b, c gives rise to the triple b, c, bc of elements which are their own inverses

Moreover, $bc(bc) = b^2c^2 = e$. In the product $a_1 a_2 \cdots a_n$, which reduces to the product of the elements of G which are their own inverses, every pair b, c with $b^2 = c^2$ gives rise to the triple a, b, bc such that $bc(bc) = e$

Thus $a_1 a_2 \cdots a_n = e$

(c) if $n = |G|$ is odd, by (a), we have $x = e$ since $x^2 = e$

Section 2.5

(1) Determine in each of the parts if the given mapping is a

(a) $G = \mathbb{Z}$ under $+$, $G' = \mathbb{Z}_n$, $\phi(a) = [a]$ for $a \in \mathbb{Z}$

This is a homomorphism since $\phi(a+b) = [a+b] = [a] + [b]$
$= \phi(a) + \phi(b)$. The kernel is $n\mathbb{Z}$. It is onto but not 1-1

(b) Not a homomorphism since $\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} =$
$= \phi(b)\phi(a)$ which need not equal $\phi(a)\phi(b)$ in general.

(c) If G is abelian it is a homomorphism then the map from (b) is a homomorphism and it is both injective and surjective

(d) This is a homomophism. We have $\phi(r) = r/|r|$. Then $\phi(rs) =$
$= (rs)/|rs| = (r/|r|)(s/|s|) = \phi(r)\phi(s)$. Not injective
$\phi(1) = \phi(2)$. Not surjective since nothing goes to $1/2$

(e) Homomorphism. $\phi(ab) = (ab)^n = a^n b^n = \phi(a)\phi(b)$ using the fact that G is abelian, However if $G = \{e, a\}$ is a cyclic group of order 2 and if $n = 2$, then the ϕ map is neither injective or surjective. It might be sometimes though (if $n = 3 \ldots$)

(3) Given G be any group and $A(G)$ the set. --

(a) Well, since x in G then

$x = (xa)a^{-1} \Rightarrow x = L_a(xa) \Rightarrow L_a$ is onto

with $L_a(x) = L_a(y) \Rightarrow xa^{-1} = ya^{-1}$

$\therefore x = y \Rightarrow L_a$ is 1-1 and $L_a \in A(G)$

(b) $(L_a L_b)(x) = L_a(L_b(x)) = L_a(xb^{-1}) = (xb^{-1})(a^{-1}) =$

$x(b^{-1}a^{-1}) = x(ab)^{-1} = L_{ab}(x) \Rightarrow L_{ab} = L_a L_b$

(17) If $M \trianglelefteq G$, $N \trianglelefteq G$, prove that $M \cap N \trianglelefteq G$

For a subgroup N in G we have

$$N \trianglelefteq G \Leftrightarrow gNg^{-1} \subset N \text{ for all } g \in G$$

So let $g \in G$ and $x \in M \cap N$. then $x \in M$ and $x \in N$ so

$$gxg^{-1} \in gMg^{-1} \subset M \text{ and } gxg^{-1} \in gNg^{-1} \subset N$$

because M & N are normal in G then

$gxg^{-1} \in M \cap N$, and so

$g(M \cap N)g^{-1} \subset M \cap N, \Rightarrow M \cap N \trianglelefteq G$

(18) If H is any subgroup of G, ...

$N \cap H$ is a subgroup of G. since $N \cap H \subset H$, it is a subgroup of H also. let $h \in H$ and $x \in N \cap H$ then $x \in N$ and $x \subset H$ then $hxh^{-1} \in hNh^{-1} \subset N$ assuming $N \trianglelefteq G$ and $h \in G$

$h \in h^{-} \in H$, since $h, x \in H$ and $H \leq G$

$\therefore hxh^{-1} \in N \cap H$ and $h(N \cap H)h^{-1} \subset N \cap H$ so $N \cap H$ is normal in H

(19) If H is a subgroup of G,

(a) If a, b are in $N(H)$ then

$a^{-1}Ha = H$ and $b^{-1}Hb = H$ so

$(ab)^{-1}H(ab) = b^{-1}(a^{-1}Ha)b = b^{-1}Hb = H$ so

$ab \in H$.

Also $a^{-1}Ha = H$ implies that $aHa^{-1} = H$ so that

$(a^{-1})^{-1}Ha^{-1} = H \Rightarrow a^{-1}$ is in $N(H)$

$\therefore N(H)$ is a subgroup of G since $h^{-1}Hh = H$ for h in H, $H \subset N(H)$.

(24) If G_1, G_2 are two groups, let $G = G_1 \times G_2$, the cartesian product of G_1, G_2 [i.e., G is the ordered set of all ordered pairs (a,b) where $a \in G_1$, $b \in G_2$]. Define a product in G by $(a_1,b_1)(a_2,b_2) = (a_1 a_2, b_1 b_2)$

(a) Prove that G is a group

For all $(a_1,b_1)(a_2,b_2) \in G_1 \times G_2$, we have $(a_1,b_1)(a_2,b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$ and $(a_1,a_2) \in G_1$; $(b_1,b_2) \in G_2$. So $(a_1,b_1)(a_2,b_2) \in G_1 \times G_2$

$G_1 \times G_2$ is closed under the group operation

let's have $(a_1,b_1), (a_2,b_2), (a_3,b_3) \in G \times H$ we get

$$[(a_1,b_1)(a_2,b_2)(a_3,b_3) = (a_1 \cdot a_2; b_1 \cdot b_2)(a_3,b_3) = ((a_1 \cdot a_2) \cdot a_3 (b_1 \cdot b_2) b_3)$$

$$((a_1 \cdot a_2) \cdot a_3, (b_1 \cdot b_2) b_3 = (a_1 (a_2 \cdot a_3), b_1 (b_2 \cdot b_3)))$$

$$= (a_1,b_1)(a_2 \cdot a_3, b_2 \cdot b_3)$$

$$= (a_1,b_1)(a_2,b_2)(a_3,b_3)$$

$\therefore$ associative

e_a, e_b is the identity element in G_1 and e_b in G_2

The inverse of of $(a,b) \in G \times H$ is $(a^{-1}, b^{-1}) \in G \times H$

Hence $G \times H$ is a group.

(b) $\phi_1(a_1) = (a_1, e_2) \neq \phi_1(a_1 a_2) = (a_1 a_2, e_2) = (a_1, e_2)(a_2, e_2)$

$= \phi_1(a_1)(\phi_1)(a_2) \Rightarrow \phi_1$ is a mononorphism

Similarly for G_2

(d) follows from interpretation of solution manual

Given (a_1, a_2) in G then $(a_1, a_2) = (a_1, e_2)(e_1, a_2)$

and (a_1, e_2) is in ϕG_1 and (e_1, a_2) is in $\phi_2(G_2)$

With (a_1, a_2) in $\phi_1(G_1) \cap \phi_2(G_2)$ then $a_1 = \phi_1$ and

$a_2 = e_2$, $\Rightarrow$ the intersection is the identity element of G...

(26) If G is a group and $a \in G$, define $\sigma_a : G \to G$ by $\sigma_a(x) = axa^{-1}$
I got discouraged with problems 26, 29, 38. & 42 studied solution.

(a) If a, b are in G then for all g in G

$(\sigma_a \sigma_b)(g) = \sigma_a(bgb^{-1}) = a(bgb^{-1})a^{-1} = (ab)g(ab)^{-1} =$
$= \sigma_{ab}(g)$

Therefore $\sigma_{ab} = \sigma_a \sigma_b$

$\psi(ab) = \sigma_{ab} = \sigma_a \sigma_b = \psi(a)\psi(b)$, so ψ is a homomorphism of G into $A(G)$

(b) If $z \in Z(G)$ then $\sigma_z(g) = zgz^{-1} = g$ for all g in G;
σ_z is the identity mapping on G, hence z is in $\ker \psi$
$\therefore Z(G) \subset \ker \psi$

(29) A subgroup T of a group W is called characteristic ...

(a) The conjugation by any elements is an automorphism of G
$\sigma_a(x) = a^{-1}xa$ is an automorphism of G
If M is characteristic, $gMg^{-1} = M$ for all $g \in G$
Then M is normal in G.

(b) M and N are normal in $G \Rightarrow MN$ is a normal subgroup of G.
Let ϕ be an automorphism of G then since $\phi(M) = M$, $\phi|_M$ as an automorphism of M therefore since $\phi|_M(N) = N$, we have $\phi(N) = N$ as well.

(c) from the solution set
Let G be the group of order 4 having the elements e, a, b, ab where $a^2 = b^2 = e$ and
$ab = ba$

(29) ...
Since the group G is abelian, every subgroup of G is normal in G.
Thus $A = \{e, a\}$ is a normal subgroup of G.
The mapping ϕ defined on G by $\phi(e) = e$, $\phi(a) = b$, $\phi(b) = a$ and $\phi(ab) = ab$ can be seen to be an automorphism of G.
But $\phi(A) = \{e, b\}$ is not contained in A.
Thus A is not a characteristic subgroup of G.

(38) Let G be a group and H a subgroup of G. Let S...

(a) $(T_b T_c) H_a = T_b (T_c (Ha)) = T_b (Hac^{-1}) = Hac^{-1}b^{-1} =$
$= Ha(bc)^{-1} = T_{bc}(Ha)$
for every a in G. $\therefore T_{bc} = T_b T_c$

(b) Suppose u is in $K(\psi)$; thus $Tu = \psi(u) = i_s$
For every a in G, $Hau = Tu(Ha) = Ha$
and so $Hau = Ha$, $\therefore Haua^{-1} = H$
Therefore aua^{-1} is in H for every a in G.
Conversely, if aua^{-1} is in H for every a in G the argument reverses to show
$$Tu = \psi(u) = i_s \Rightarrow K(\psi) = \{u \in G \mid aua^{-1} \in H \ \forall a \text{ in } G\}$$
so if a is in $K(\psi)$ then u is in every $a^{-1}Ha$, from this $K(\psi)$ is the intersection of all $a^{-1}Ha$ as a runs over G.

(c) $K(\psi)$ is a normal subgroup of G, since its the kernel of a homomorphism of G, and lies in H since aua^{-1} is in H for every a in G, so $K(\psi) < H$; $N < H$ then
$aNa^{-1} < N < H \Rightarrow N < K(\psi)$ ... Ha!

(42) Suppose that you know that a group G of order 36 has a subgroup --
If $|G| = 36$ and H is a subgroup of order 9 then
$i_G(H) = 4$ and 9 does not divide $4! = 24$
Thus there is a normal subgroup N of G, $N \neq (e)$,
and $N \subset H$.
Since every subgroup of H different from (e) is
of order 3 or 9, G has a normal subgroup of order
3 or 9 which is contained in H ∴

milk
Eggs
3 oranges
pick up Teddy

Chapter 2 - Section 2.6

(11) If G is a group and $Z(G)$ ---

Z is a normal subgroup; Let $G/Z = (aZ)$ since G/Z is cyclic. Now choose $b, c \in G$. We need to show that $bc = cb$. Because the cosets of Z partition G, the cosets are of the form $a^i Z$ for some $i \in \mathbb{Z}$ we know that $b \in a^i Z$ and $c \in a^j Z$ for some $i, j \in \mathbb{Z}$. Write $b = a^i z_1$ and $c = a^j z_2$ for some $z_1, z_2 \in Z$. then

$bc = (a^i z_1)(a^j z_2) = (a^i a^j)(z_1 z_2) = (a^{i+j})(z_1 z_2) = a^j a^i z_2 z_1 =$

$= a^j z_2 a^i z_1 = cb.$ $\nRightarrow$ the elements of $Z = Z(G)$ commute with everything $\Rightarrow$ being cyclic implies G is abelian.

(13) If G is a group and $N \triangleleft G$ is such that ---

If $aba^{-1}b^{-1}$ is in N for all a, b in G then

$Naba^{-1}b^{-1} = N \rightarrow Nab = Nba$

but $NaNb = Nab = NbNa$; $\nRightarrow$ G/N is abelian,

(18) Let G be an abelian group (possibly infinite) and let the set ---

(a) H is a subgroup of G.

(b) from the solution set

for some $n > 1$ Tx in G/T satisfies $(Tx)^n = Tx^n = T$ the identity element of G/T then a^n is in T

so by definition $(a^n)^s = \emptyset$ for some $s > 0$.

Then $a^{ns} = \emptyset$ this puts a in T; then $Ta = T$,

The identity element of G/T ...

Section 2.7

(4) If G_1, G_2 are two groups and $G = G_1 \times G_2 = \ldots$

(a) $(g,h)^{-1}(a,e_2)(g,h) = (g^{-1},h^{-1})(a,e_2)(g,h) =$

$= (g^{-1}ag, h^{-1}e_2h) = (g^{-1}ag, e_2)$ so is in N

$\therefore$ N is normal in G.

(b) The mapping $t: G_1 \to N = (a,e_2)$ is an isomorphism of G_1 onto N

(c) $G_2 \simeq G_1/\ker\phi = G_1/N$

then $(G_1 \times G_2)/N \simeq G_2$

(7) If ϕ is a homomorphism of G onto G'...

$\phi(N)$ is a subgroup, prove that is normal.

Choose $y = \phi(x) \in \phi(N)$ (so $x \in N$) and $g' \in G'$. Then $\exists\ g \in G \ni \phi(g) = g'$ and $gxg^{-1} \in N$ since N is normal. Then

$$g'yg'^{-1} = \phi(g)(\phi)x\,\phi(g)^{-1} = \phi(gxg^{-1}) \in \phi(N)$$

Section 2.8

(4) Construct a nonabelian group of order 21

Using $a^3 = e$, $b^7 = e$ $\nRightarrow a^{-1}ba = a^i \neq a$

$a^3 = b^7 = e$

There are 21 distinct elements b^ia^j; where $0 \le j < 3$, $0 \le i < 7$

then $(b^ja^m)(b^ja^n) = b^ra^s$ where

$r = i + 2^mj$ and $s = m+n$

⑥ Let G be a finite group and suppose A, B subgroups of G such that $|A| > \sqrt{|G|}$ ---

interpretation from solution notes

$|AB| = |A||B|/|A \cap B| \leq |G|$,

$|A \cap B| \geq |A||B|/|G| > \sqrt{|G|}\sqrt{|G|}/|G| = 1$

$\therefore A \cap B \neq \emptyset$

⑦ Let G a group and A, B, subgroups. - - -

Since AB has $|A||B|/|A \cap B|$ distinct elements and since $A \cap B$ is $\subset$ of A and B $|A \cap B|$ must divide both $m = |A|$ and $n = |B|$.

Since m and n are relatively prime we get that $|A \cap B| = 1 \Rightarrow AB$ has $|A||B| = mn$ distinct elements

⑧ Prove that a group of order 99 has. --

then by the Cauchy's theorem, if a prime p divides the order of a finite abelian group G, then G contains an element of order p $\Rightarrow$ true even if group is not abelian

G has an element a of order 11.

for the subgroup $A = (a)$ of order 11

$i_G(a) = 9$ does not divide $9 \Rightarrow A$ is a normal subgroup of G

⑪ If G is a group and A, B finite subgroups of G, prove. --

Since $|AB| = (|A||B|)/(|A \cap B|)$

AB has $|A||B|$ elements with $ab = a'b'$ and $a \neq a'$ and $b \neq b'$

then $\forall\ t \in A \cap B$, $ab = (at)(t^{-1}b)$ so each group has at least $|A \cap B|$ products in AB.

Let $ab = a'b' \rightarrow t = a^{-1}a' = b(b^{-1}) \in A \cap B$ so that $a' = at$ and $b' = t^{-1}b$ $\therefore$ each element in AB has exactly $|A \cap B|$ products then

$$|AB| = (|A||B|)/(|A \cap B|)$$

(12) Prove that any two non abelian groups of order 21 are isomorphic.

A group of order 21 has a normal subgroup of order 7 let this be generalized by a and let b be an element of order 3 following development on solution guide

The subgroup $A = (a)$ of order 7 is normal in G since 7 does not divide $i_G(A)! = 3! = 6$

Then $bab^{-1} = a^i$,

Since G is nonabelian $i \neq 1$ however $b^3 = e$

thus we get $a = a^k$ where $k = i^3$ and $i^3 - 1$ is divisible by 7

We get $i = 2$ or 4.

If $i = 2$ then $b^2ab^{-2} = a^4$ so G has an element c such that $cac^{-1} = a^4$

If G_1 is another nonabelian group of order 21 the same procedure follows to show that $u \& v \in G_1$, and $u^4 = v^3 = e$ and $vuv^{-1} = u^4$ Define $f: G \rightarrow G_1$ by $f(a) = u$ & $f(c) = v$ and $f(a^i c^j) = u^i v^j$.

Thus this is an isomorphism of G onto G_1.

Section 2.9

① If G_1 & G_2 are groups, prove that $G_1 \times G_2 \simeq G_2 \times G_1$

$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$

$(g_2, g_1) \cdot (h_2, h_1) = g_2 \cdot h_2, g_1 h_1)$

$G_2 \times G_1 = \{(g_2, g_1) \mid g_1 \in G_1, g_2 \in G_2\}$

Let $\phi : G_1 \times G_2 \to G_2 \times G_1$ such that $\phi(g_1, g_2) = (g_2, g_1)$

$\phi[(g_1, g_2) \cdot (h_1, h_2)] = \phi(g_1 \cdot h_1, g_2 \cdot h_2) = (g_2 \cdot h_2, g_1 h_1) =$

$= (g_2, g_1) \cdot (h_2, h_1) = \phi(g_1, g_2) \cdot \phi(h_1, h_2)$

$\therefore \phi$ is a homomorphism

now for every $(g_2, g_1) \in G_2 \; \exists \; (g_1, g_2) \in G_1 \ni$

$\phi(g_1, g_2) = (g_2, g_1)$ since ϕ is onto then

ϕ is an isomorphism

assume $\phi(g_1, g_2) = \phi(h_1, h_2)$, prove $(g_1, g_2) = (h_1, h_2)$

$\phi(g_1, g_2) = \phi(h_1, h_2) \Rightarrow (g_2, g_1) = (h_2, h_1) \Rightarrow g_2 = h_2$ and

$g_1 = h_1 \Rightarrow (g_1, g_2) = (h_1, h_2) \Rightarrow \phi$ is 1-1

$G_1 \times G_2$ is an isomorphism of $G_1 \times G_2$ onto $G_2 \times G_1$

(2) If G_1 and G_2 are cyclic groups of orders m and n ...
$G_1 \times G_2$ is cyclic if it's an element of order m and n
If we have $\gcd(m,n)=1 \Rightarrow G_1^n$ has order m and
G_2^m has order $n \Rightarrow G_1 \times G_2$ has order $n \cdot m$ and
therefore $G_1 \times G_2$ is cyclic
Now if $\gcd(m,n)>1$ then let $G_1^k \in G_1$ and
$G_2^j \in G_2$. Since the lcm of $mn < mn$ that is
$\text{lcm}(m,n) < (m \cdot n)$ and since
$(G_1^k)^{\text{lcm}(m,n)} = e_{G_1}$ and $(G_2^j)^{\text{lcm}(m,n)} = e_{G_2}$
we get $(G_1^k \times G_2^j)^{\text{lcm}(m,n)} = e_{G_1 \times G_2}$

$\Rightarrow$ every element of $G_1 \times G_2$ has order lower than $m \cdot n$
and therefore $G_1 \times G_2$ cannot be cyclic

(3) Let G be a group, $A = G \times G$. In A let $T = \{(g,g) \mid g \in G\}$
from the solution to 25 and $(a,a) \to (g,g) \mid g \in G$
$\phi(a) = (a,a)$ and $\phi(b) = (b,b)$ for $a \neq b$ in G
$\phi(ab) = (ab, ab) = (a,a)(b,b) = \phi(a)\,\phi(b)$
then ϕ is a homomorphism of G into $G \times G$
If $\phi(G)$ is normal in $G \times G$ then $(g,e)^{-1}(a,a)(g,e)$
$= (g^{-1}ag, a)$ is in $\phi(G)$ for all g in G

Section 2.11

(3) If $a \in G$, show that $C(x^{-1}ax) = x^{-1}C(a)x$

Using the solution from 4

$\phi(a) = x^{-1}ax$ $\forall$ G is an automorphism on G

If $ax = xa$ then $\phi(a)\phi(x) = \phi(ax) = \phi(xa) =$

$= \phi(x)\phi(a)$, then $\phi(x) \in C(\phi(a))$; so

$\phi(C(a)) \subset C(\phi(a))$

Conversely if y is in $C(\phi(a))$ then $y\phi(a) = \phi(a)y$

with $\phi^{-1}(y)a = a\phi^{-1}y$ so that $\phi^{-1}(g) \in C(a)$

$\Rightarrow y \in \phi(C(a))$.

so $C(\phi(a)) \subset \phi(C(a)) \Rightarrow C(\phi(a)) = \phi(C(a))$

(4) If ϕ is an automorphism of G, show that

$C(\phi(a)) = \phi(C(a))$ for $a \in G$.

Define $ax = xa \Rightarrow \phi(ax)\phi(xa) = (ax)(xa)$

$= \phi((ax)(xa))$

let $\phi(x) \in C(\phi(a)) \Rightarrow \phi(C(a)) \subset C(\phi(a))$

and $C(\phi(a)) = \phi(C(a))$

(11) If p is a p-Sylow group...

from the solution set

Given that p is a p-Sylow subgroup of G

$P \subset N(P) \Rightarrow P$ is also a p-Sylow subgroup of $N(P)$

P is normal in $N(P)$, $\forall \neq P$ is a p-Sylow subgroup

of G of order p^n then $PQ = QP$ so

PQ is a subgroup of G and

$$|PQ| = |P||Q|/(|P\cap Q|) = p^{2n}/(|P\cap Q|) \geq p^{n+1}$$

must divide G since $|G| = p^n m$ but $(m,p) = 1$

$\therefore$ $P = Q$ and P is the only p-Sylow subgroup of $N(P)$

(14) If P is a p-Sylow subgroup of G, show that the number of distinct $x^{-1}Px$ cannot be a multiple of p

For a p-Sylow subgroup $P \subset N(P)$

and $p^n = |P|$ must divide $|N(P)|$

$\Rightarrow |N(P)| = p^n k$ and $i_G(N(P)) = |G|/(|N(P)|)$

$= p^n m/p^n k = m/k \in \mathbb{Z}$

since p does not divide m

$\Rightarrow$ p does not divide $i_G(N(P))$ since the number of distinct $x^{-1}Hx$ equals $i_G(N(P))$ it cannot be a multiple of p

(18) Show that $N(N(P)) = N(P)$

$a \in N(N(P)) \Rightarrow a^{-1}(N(P))a \subset N(P)$ also $P \subset N(P)$

so $a^{-1}Pa \supset N(P)$ then $a^{-1}Pa$ is a p-Sylow subgroup of $N(P)$

since we know that P is the only p-Sylow subgroup in $N(P)$ $\Rightarrow a^{-1}Pa = P$ and $a \in N(P)$

$\therefore N(N(P)) \subset N(P) \Rightarrow N(N(P)) = P$

Section 11, chapter 2

#19 If $|G| = p^n$, show that G...

By induction $n=1 \Rightarrow$ a group of order p has an element of order p

asume $|G| = p^k$ is true

We wish to prove that $|G| = p^{k+1}$ is true

Suppose that any group G of order p^n has a subgroup of order p^m for $0 \leq m \leq n$

Let G be a group of order p^{n+1}

Since $|G| = p^{n+1}$ then $\exists$ an element a of order p in $Z(G)$.

If $A = (Z)$ then A is a normal subgroup of G and $G_1 = G/A$ is a group of order p^k

$\Rightarrow G_1$ has a subgroup T_1 of order p^r for all $r \leq k$

If as stated $T = \{ g \in G \mid Ag \in T, \}$ then T is a subgroup of G and

$T/A = T_1 \Rightarrow |T| = |T_1||A| = p^r p = p^{r+1}$ then for every $r+1 < k+1$ G has a group of order $k+1$

∎

Chapter 3/1

① Find the products

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

② Find σ^k for all k

(a) $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$; $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$

$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}$; $\sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

$\sigma^6 = I$

(b) $\sigma^2 = \sigma^4 = \sigma^6 = I$

$\sigma^3 = \sigma^5 = \sigma^7 = \sigma$

(c) $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 6 & 5 \end{pmatrix}$; $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 2 & 3 & 5 \end{pmatrix}$

$\sigma^4 = I$

③ Prove

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} = I$$

Section 3.2

(3) Express as the product ...

(a) Order 2

$(1\ 6)(2\ 5)(3\ 7)(4)$

(b) Order 4

$(1\ 4\ 3\ 2)$

(c) Order 7

$(1\ 4\ 7\ 3\ 6\ 2\ 5)$

(d) Order 1

$(1)(2)(3) = I$

(e) Order 4

$(1\ 5\ 7\ 8)$

(f) Order 5

$(1\ 4\ 2\ 5\ 3)$

(9) Given $(1\ 2)$ and $(1\ 3)$ as transpositions ...

$\sigma = (2\ 3)$

then $(2\ 3)(1\ 2)(2\ 3)^{-1} = (1\ 3)$

(12) Prove that there is no permutation σ ...

$(1\ 2)^3 = I$

$(1\ 2)^2 = I \not\Rightarrow (1\ 2) \neq I$

∎

Section 3.2

(21) If σ and τ are two permutations having no letter in common and $\sigma\tau = \epsilon \Rightarrow \sigma = \tau = \epsilon$

Choose a letter not in common k

Then $\left.\begin{matrix}\sigma(k) = k \\ \tau(k) = k\end{matrix}\right\} (\sigma\tau) = k$ and $(\tau\sigma) = k$

Being disjoint permutations if k is in σ then it is not in τ

$\therefore\ k = \tau(\sigma(k)) = \sigma(k) = \sigma\tau(k)$

Conversely if k is in τ it is not in σ

then $\sigma\tau = \tau\sigma$

Section 3.3

(1) Find the parity

(a) even ; (b) even ; (c) even ; (d) odd

(3) Prove that σ and $\tau^{-1}\sigma\tau$ --- are of the same parity

τ & τ^{-1} have the same parity

$\therefore$ parity of $\tau^{-1}\sigma\tau = \sigma$ parity

and $\sigma, \tau \in S_n$

(5) In the permutation, what must be the images of 5 & 4

Since it's an even permutation there is an even number of 2 element transpositions

∞ 1 2 3 4 5 6 7 8 9 → 3 1 2 * * 7 8 9 6

then ① 1 & 3 ; ② 2 & 1 ③ 6 & 9 ④ 9 & 7 ⑤ 9 & 8

for an even number there is one more switch

then initially 4 5 ≠ 5 4

image of 4 = 5

image of 5 = 4

(6) If $n \geq 3$, show that every element in An ...

An even number of permutations is the product of an even number of transpositions.

We have to show that every element of An is the product of 3-cycles

Suppose γ_1 & γ_2 move a common number a and we have the product

Then $\gamma_1 = (a\ b)$, $\gamma_2 = (a\ c)$

with $\gamma_1 \gamma_2 = (ab)(ac) = (acb)$

now for γ_1 & γ_2 with different numbers

$\gamma_1 = (a\ b)$; $\gamma_2 = (c\ d)$

and $\gamma_1 \gamma_2 = (dac)(abd)$

∴ the product of transpositions is a product of 3-cycles

Chapter 4 - Section 1

(9) Find all 2x2 matrices

Commute $a \cdot b = 0$ either $a=0$ or $b=0$

If $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ commutes with all matrices it commutes with

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and with $I \Rightarrow a=d$

(11) Let $F = \mathbb{C} \to \mathbb{C}$ be defined by $f(a+bi) = a-bi$

(a) $f(xy) = F(x)F(y)$ for $x, y \in \mathbb{C}$

$= a^2 + 2iab - b^2$

(b) $F(x\bar{x}) = a^2 - b^2$

(c) $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$

for $(a+bi)(a-bi)$

(13) Find the following products

$i^2 = j^2 = k^2 = -1$

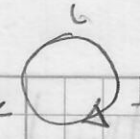
$ij = k$, $jk = i$

$ki = -j$ & $ji = -k$

(a) $(i+j)(i-j) =$

$i^2 - ik - kj - j^2 = -2k$

(b)
$$\begin{array}{r} 1 - i + 2j - 2k \\ 1 + 2i - 4j + 6k \\ \hline 1 - i + 2j - 2k \\ +2i - 2i^2 + 4k - 4j \\ +8i \qquad +4k - 4j - 8j^2 \\ -12i \qquad +6k - 6j \qquad -12k^2 \end{array} = 5i + 4k + 23$$



(c) $2i - 3j + 4k$
$2i - 3j + 4k$

$4i^2 - 6ij + 8ik$
$+9j^2 - 12jk - 6ji + 8ki - 12kj + 16k^2$
$-4 - 6k - 8j - 9 - 12i + 6k - 8j + 12i - 16$
-29

(d) $i\alpha_0 - \alpha_1 - \alpha_2 ij + \alpha_3 ki - i\alpha_0 + \alpha_1 - \alpha_2 ji - \alpha_3 ki$
$= -2\alpha_3 j + 2\alpha_2$

(16) Verify that
$\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$
$\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$

$\alpha_0^2 + \alpha_1\alpha_0 i + \alpha_0\alpha_2 j + \alpha_0\alpha_3 k - \alpha_0\alpha_1 i + \alpha_1^2 - \alpha_1\alpha_2 ij - \alpha_1\alpha_3 ik$
$- \alpha_0\alpha_2 j - \alpha_1\alpha_2 ji + \alpha_2^2 - \alpha_2\alpha_3 jk - \alpha_0\alpha_3 k -$
$- \alpha_1\alpha_3 ki - \alpha_2\alpha_3 kj + \alpha_3^2$
$= \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$

(23) Define the map * in the quaternions by...

(a) If $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$
then $x^* = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$
$\Rightarrow x^{**} = \alpha_0 - (-\alpha_1) i - (-\alpha_2) j - (-\alpha_3) k =$
$= \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k = x$

(b) $(x+y)^* = x^* + y^*$

with $y = b_0 + b_1 i + b_2 j + b_3 j$

$x + y = (a_0+b_0) + (a_1+b_1)i + (a_2+b_2)j + (a_3+b_3)k$

$(x+y)^* = (a_0+b_0) - (a_1+b_1)i - (a_2+b_2)j - (a_3+b_3)k$

$= (a_0 - a_1 i - a_2 j - a_3 k) + (b_0 - b_1 i - b_2 j - b_3 k)$

$= x^* + y^*$

(c) $(xy)^* = y^* x^* \Rightarrow a_0^2 + a_1^2 + a_2^2 + a_3^2$

(36) If $F = \mathbb{C}$, show that ---

Let $a^2 = -i$ then $1 + aj \neq$ is in $H(F)$

and $(1+aj)(1-aj) = 1 - a^2 j^2 = 1 - (-1)(-1) = 0$

$\therefore$ $H(F)$ has zero divisors so cannot be a division ring

Section 4.2

(2) If R is an integral domain and $ab = ac$

Assume R is an integral domain

If $ab = ac \Rightarrow a(b-c) = ab - ac = 0_R$

either $a = 0$ or $b - c = 0$ since $a \neq 0$

then $b - c = 0 \Rightarrow b = c$

③ If R is a finite integral domain, show that R is a field.

Let R be a finite integral domain $\Rightarrow$ elements are not distinct

For R to be a field, every nonzero element of R is a unit.

Let $r \in R$ be nonzero; for an infinite sequence of ring elements $r^1, r^2 \ldots$ there exist positive integers $n > m$ with $r^n = r^m$. By the axioms we have

$$0 = r^n - r^m = r^k r^m - r^m = (r^k - 1) r^m$$

with $k = n - m$ then because R is an integral domain either $r^k - 1 = 0$ or $r^m = 0$

if $r^m = 0 \Rightarrow r = 0$ but we defined $r \neq 0$ then it follows that $r^k - 1 = 0 \Rightarrow r^k = 1$ and $r \cdot r^{k-1} = 1$. This shows that r is a unit R, since r^{k-1} is the multiplicative inverse of r, and R is a field

④ Let R be a ring in which $x^4 = x$ for every $x \in R$.

We have $x = x^4 = (-x)^4 = -x \Rightarrow 2x = 0$

then $(x^2 + x^2) = x^2 + x$

this implies that $y(x^2 + x) = (x^2 + x)y$;

then $(x+y)^2 + x + y + x^2 + x + y^2 + y = xy + yx$

this shows that $xy + yx$ commutes with every element in R.

Hence, $x(xy + yx) = (xy + yx)x$, and this shows that $xy = yx$

$=$

(4) Let p be an odd prime

interpreting from the solution

The elements $[1]^{-1} = [1], [2]^{-1} = [2]^{-1}, \ldots, [i]^{-1} =$

$= [i^{-1}], \ldots, [p-1]^{-1} = [(p-1)^{-1}]$ give us all the

nonzero elements of Z_p

$\Rightarrow [1] + [2^{-1}] + \ldots + [(p-1)^{-1}] = [1] + [2] + \ldots + [p-1]$

Using congruences we have

$1 + 1/2 + 1/3 + \ldots + 1/(p-1)] \equiv 1 + 2 + \ldots + (p-1) \bmod p$

However $1+2+\ldots+(p-1) \equiv p(p-1)/2 \equiv 0 \bmod p$

since p is an odd prime.

Thus, $1 + 1/2 + \ldots + 1/(p-1) \equiv 0 \bmod p$

If $1 + 1/2 + \ldots + 1/(p-1) = a/b$ where $a \notin b \in \mathbb{Z}$

$\Rightarrow p \mid a$

Section 4.3

(3) If $\phi: R \to R'$ is a homomorphism of R onto R'

since ϕ is a homomorphism

of R onto R', given x in R', $x = \phi(a)$

for some a in R

$\therefore x = \phi(a \cdot 1) = \phi(a)\phi(1) = x\phi(1)$

Similarly $x = \phi(1)x \Rightarrow \phi(1)$ is the unit element of R'

(4) If I, J are ideals of R define $I+J$ by $I+J = \ldots$

Given $I+J = \{i+j \mid i \in I, j \in J\}$

Since $0 \in I \cap J$ we have $I = I+0 \subseteq I+J$ and $J = J+0 \subseteq I+J$, so $I+J$ does contain both I and J

$\therefore$ $I+J$ is an ideal of R

(17) If A is a subring of R...

Let $a+i_1$ and a_2+i_2 where $a_1, a_2 \in A$ and $i_1, i_2 \in I$ then

$(a_1+i_1)+(a_2+i_2) = (a_1+a_2)+(i_1+i_2)$ is in $A+I$ since A & I are additive groups of R.

Also $(a_1+i_1)(a_2+i_2) = a_1a_2 + a_1i_2 + i_1a_2 + i_1i_2$ is in $A+I$ since A is a subring and I an ideal of R

(20) If I, J are ideals of R, let $R_1 = R/I$ ...

To show it is a homomorphism

$\phi(rr') = ((rr')+I, (rr')+J) = (r+I, r+J)(r'+I, r'+J) =$

$= \phi(r)\phi(r')$

$\phi(r+r') = ((r+r')+I, (r+r')+J) = (r+I, r+J)+(r'+I, r'+J) =$

$= \phi(r) + \phi(r')$

$\ker\phi = \{r \in R \mid (r+I, r+J) = (0+I, 0+J)\}$

$= \{r \in R \mid r \in I, r \in J\} = I \cap J$ ▨

(22) Let $\mathbb{Z}$ be the ring ...

$I_m \cap I_n$ is the set of all numbers that are multiples of m & n. Given that m & n are relatively prime, this is the same as the integers that are multiples of mn.

(27) If $p_1, p_2 \ldots p_n$ are distinct primes

Studying solution on proof by induction.

given that $\mathbb{Z}/(p_1 p_2 \ldots p_n) \cong \mathbb{Z}(p_1) \oplus \mathbb{Z}(p_2) \oplus \ldots$

$\ldots \oplus \mathbb{Z}/(p_n)$

$x = (a_1, a_2, \ldots, a_n)$ where each a_i is in $\mathbb{Z}/(p_i)$

satisfy $x^2 = x$ iff each $a_i^2 = a_i$

That is, if $a_i = 0$ or 1 in $\mathbb{Z}/(p_i)$

Then there are 2^n possible choices for the a_i

and 2^n elements x in $\mathbb{Z}/(p_1) \oplus \mathbb{Z}/(p_2) \oplus \ldots \oplus \mathbb{Z}/(p_n)$

satisfying $x^2 = x$

hence there are 2^n elements in $\mathbb{Z}/(p_1 p_2 \ldots p_n)$

such that $x^2 = x$.

In terms of congruence modulo $(p_1 p_2 \ldots p_n) \Rightarrow$

$\Rightarrow$ There are 2^n solutions of $x^2 \equiv x \bmod (p_1 p_2 \ldots p_n)$

with $0 \leq x \leq p_1 p_2 \ldots p_n$

Section 4.4

① If a, b are integers and ...

$a \equiv 1$ or $2 \bmod 3$

$b \equiv 1$ or $2 \bmod 3$

$a^2 \equiv 1^2$ or $2^2 \equiv 1$ or $1 \bmod 3$

$\Rightarrow a^2 \equiv 1 \bmod 3$; $b^2 \equiv 1 \bmod 3$

and $a^2 + b^2 \equiv 2 \bmod 3$

so $3 \nmid a^2 + b^2$

④ Show that $(p-1)/2$ of the numbers ...

A nonzero number that is congruent to a square modulo p is called a quadratic residue modulo p

Then these would be the numbers $1^2, 2^2, \ldots, (p-1)^2 \pmod p$

since there are $(p-1)/2$ quadratic residues modulo p and $(p-1)/2$ nonresidues modulo p we just need to go halfway then $1^2, 2^2, \ldots, ((p-1)/2)^2 \pmod p$

because the same numbers are repeated in reverse order

check that $1^2, 2^2, \ldots, ((p-1)/2)^2$ are all different modulo p

Suppose that b_1 and b_2 are between 1 and $(p-1)/2$ and $b_1^2 \equiv b_2^2$. To show that $p \mid b_1^2 - b_2^2 = (b_1 - b_2)(b_1 + b_2)$

but $b_1 + b_2$ is between 2 and $p-1 \Rightarrow$ not divisible by $p \Rightarrow p$ must divide $b_1 - b_2$. But $|b_1 - b_2| < (p-1)/2$ so $b_1 = b_2$ is the only way for $b_1 - b_2$ to be divisible by p

then $1^2, 2^2, \ldots, ((p-1)/2)^2$ are all different modulo p, so there are exactly $(p-1)/2$ quadratic residues modulo p. Also, there are p-1 numbers between 1 and p-1, so if half of them are quadratic residues the other half must be nonresidues. ∎

(10) Let $m>0$ be in $\mathbb{Z}$...

$R = \{a + \sqrt{m}b \mid a,b \in \mathbb{Z}\}$

$(a + b\sqrt{m}) + (c + d\sqrt{m}) = (a+c) + (b+d)\sqrt{m}$

and

$(a+b\sqrt{m})(c+d\sqrt{m}) = (ac + bdm) + (ad+bc)\sqrt{m}$

R is closed under addition and product. Given that this is a subset of $\mathbb{R}$ all ring axioms apply $\Rightarrow$ R is a ring.

Section 4.5

(2) If R is a ring ---

For x; $f(x)g(x)$ where x^{m+n} is the highest power of x; similarly $f(x) \to x^m$, $g(x) \to x^n$

The coefficient of x^{m+n} is ab for $f(x)g(x)$

If $ab = 0$ then $\deg f(x)g(x) < \deg f(x) + \deg g(x)$

(b) For $f(x) = 2x+1$ and $g(x) = 3x$ and $R = \mathbb{Z}_6$

then $\deg f(x)$ is 1

$\deg g(x)$ is 1

and $f(x)g(x) = 6x^2 + 3x = 3x$ since $6 = 0$ in $\mathbb{Z}_6$

$\therefore \deg(f(x)g(x)) = 1 < \deg f(x) + \deg g(x) = 2$

(3) Find gcd of the ...

(a) $x^3 - 6x + 7$ and $x + 4 \Rightarrow$ no common divisor or 1

(b) $x^2 - 1$ and $2x^7 - 4x^5 + 2$

$(x+1)(x-1)$ $(x-1)(---)$

$\Rightarrow (x-1)$

(c) $3x^2 + 1$ and $x^6 + x^4 + x + 1$

no common factor or $\underline{1}$

(d) $x^3 - 1$ and $x^7 - x^4 + x^3 - 1$

$(x-1)(x^2+x+1)$ $(x-1)(---)$

$\Rightarrow (x-1)$

(6) Show that the following ...

(a) $x^2 + 1$ over $F = \mathbb{R}$. It is degree 2 and has no roots

(b) $x^3 - 3x + 3$ over $F = \mathbb{Q}$. $\Rightarrow 3$

(c) $x^2 + x + 1$ over $F = \mathbb{Z}_2$. It is degree 2.

has no roots

(d) x^2+1 over $F = \mathbb{Z}_{\text{Mod } 19}$ one can check all potential roots and see that there are none or when -1 has a square root.

(e) x^3-9 over $F = \mathbb{Z}_{13}$ Yikes!

(f) x^4+2x^2+2 over $F = \mathbb{Q} \Rightarrow \mathbb{Z}$

(11) If $p(x) \in F[x]$

If a polynomial $f(x)$ of degree 3 or less over a field F is not irreducible it has a factor of degree one, hence there is an element a in F such that $f(a)=0$

$P(x) = (ax+b)(cx^2+dx+e)$ if $x_i = -b/a$

then x_i is in F and $p(x_i)=0$

(12) If $F \subset K$ ...

$\exists\ s,t \in F[x] \subseteq K[x] \ni sf+tg=1$

since f, g are relatively prime in F.

But s,t also have coeficients in K, so $f \& g$ are relatively prime in $K[x]$ as well.

(13) Show that $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$

$\phi : \mathbb{R}[x] \to \mathbb{C}$ where x goes to i

and $f(x)$ to $f(i)$

x^2+1 is in the kernel $K = \langle d \rangle$ which is principal

since $\mathbb{R}[x]$ is a principal ideal domain

then d divides x^2+1 so it is either equal to it or

equal to 1; $d=1$ implies ϕ as the zero map, then

$d = x^2+1$ ▨

(19) Construct a field...

The polynomial $x^2 - [a]$ is irreducible in $\mathbb{Z}_p[x]$

if a is a non quadratic residue modulo p

so $\mathbb{Z}_p[x]/(x^2-[a])$ is a field and has p^2 elements

(26) & (28) Let R be a commutative ring in which $a^2 = 0$

from the text

If $t^r = 0$ in R then $(t^{r-1})^2 = 0$ so, by hypothesis, $t^{r-1} = 0$

following on this path we get $t = 0$

Suppose $a_0x^n + a_1x^{n-1} + \dots + a_n \neq 0$ is a zero divisor in R

then $(a_0x^n + \dots + a_n)(b_0x^m + b_1x^{m-1} + \dots + b_m) = 0$ with $b_0 \neq 0$

$\Rightarrow a_0b_0 = 0$; $a_0b_1 + a_1b_0 = 0$; $a_0b_2 + a_1b_1 + a_2b_0 = 0$

Then $a_0b_1b_0 + a_1b_0^2 = 0 \Rightarrow a_1b_0^2 = 0$

and so $(a_1b_0)^2 = 0$ giving us $a_1b_0 = 0$

Also $a_0b_2b_0^2 + a_1b_1b_0^2 + a_2b_0^3 = 0$

$\Rightarrow a_2 b_0^3 = 0$ so that $(a_2 b_0)^3 = 0$ and so $a_2 b_0 = 0$

Similarly with the other coefficients

$a_i b_0^i = 0 \Rightarrow (a_i b_0)^i = 0$ and so $a_i b_0 = 0$

for each $i = 0, 1, \ldots, n$. $\Rightarrow b_0 \neq 0$ ▨

(2e) $a^2 = 0$ iff $a = 0$ $\Rightarrow$ By contradiction

Suppose $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$

$g(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m$

are such that $f(x)g(x) = 0$ and $g(x)$ is the polynomial of lowest degree with this property

Then $b_m \neq 0$

Assume that $f(x) b_m = 0 \Rightarrow a_n b_m = 0$

If $a_i b_m = 0$ for all i then $f(x) b_m = 0$ ✓✓✓

Suppose then that $a_{n-i} b_m = 0$ for $i < t$ and $a_{n-t} b_m \neq 0$

Thus for $i \leq t$, $g(x) a_{n-i} = a_{n-i} b_0 x^n + \ldots + a_{n-i} b_{m-1} x =$

$= (a_{n-i} b_0 x^{n-1} + \ldots + a_{n-i}) x$ and

$f(x)(g(x) a_{n-i}) = 0 \Rightarrow f(x)(a_{n-i} b_0 x^{n-1} + \ldots +$

$+ a_{n-i} b_m) = 0$

contradicting that $g(x)$ is the polynomial of lowest degree with this property

$\neq g(x) a_{n-i} = 0$ for all $i < t$

Thus $0 = f(x)\,g(x) = (a_0 x^n + \dots + a_{n-t} t^{x^t} + \dots + a_n)\,g(x) =$

$= (a_0 x^n + \dots + a_{n-t} x^t)(b x^m + \dots + b_m)$;

but this contradits $a_{n-t} b_m \neq 0$

because $a_{n-t} b_m = 0$

$\blacksquare$

Section 4.6

(3) Show that there is an infinite...

Set $a = 5p$ where p is any prime $\neq 5$.

There are infinitely many such a, and the polynomial is irreducible for all such a by Eisenstein's criterions.

(11) Let ϕ be an automorphism...

Let $g(x) = \phi(x) \Rightarrow \phi(f(x)) = f(g(x))$ for all $f(x) \in F[x]$

Suppose now that $\deg g(x) \geq 2$ then

$$\deg \phi(f(x)) = \deg(f(g(x))) = (\deg f)(\deg g)$$

Thus $\deg(f(g(x))) \neq 1$ no matter what f is

It follows that ϕ is not surjective because there is no $f(x)$ such that $\phi(f(x)) = x$, since the latter side has degree 1... but then ϕ is not an isomorphism either

Suppose that $\deg g(x) = 0 \Rightarrow \deg \phi(f(x)) = \deg(f(g(x))) = 0$ for all $f(x) \in F[x]$

again this implies that ϕ is not onto and not an automorphism

$\therefore \deg g(x) = 1$ and $g(x) = bx + c$ where $b \neq 0$ and $b, c \in F$

$\therefore \phi(f(x)) = f(bx + c)$ ☺

(7) Let F be a field.

$\phi(a) = a$ for every a in F,

and $\phi(f(x)+g(x)) = f(x+1)+g(x+1) = \phi(f(x)) + \phi(g(x))$

similarly $\phi(f(x)\,g(x)) = \phi(f(x))\,\phi(g(x))$

ϕ is surjective since $f(x) = \phi(f(x-1))$

$\Rightarrow$ ϕ is a homomorphism of $F[x]$ onto itself

Also if $f(x)$ is in $\ker \phi$ then $f(x+1) = 0$

which implies that $f(x) = 0$

$\Rightarrow$ ϕ is an automorphism of $F[x]$

(6) If V...

a) Prove $\dim_F(W) \leq \dim_F(V)$ ... by contradiction

Suppose not, then there exists a linearly independent set $w_1, \ldots, w_k$ in W with $k > \dim_F(V)$

But $w_i \in W \leq V$, and so the w_i are in V as well where they are also linearly independent... what!? $\Rightarrow$ contradiction to theorem 5.2.6

(b) if $\dim_F(W) = \dim_F(V)$ ...

Suppose that $\dim_F(W) = \dim_F(V) = n$

Then any basis of W over F has n linearly independent elements.

But by theorem 5.2.7, these elements form a basis of V over F. Thus $W = V$

(10) If $\phi: V \to V'$ is a homomorphism

A homomorphism ψ of V into W, where V and W are vector spaces over F is a mapping $\psi: V \to W$ such that $\psi(v_1 + v_2) = \psi(v_1) + \psi(v_2)$ and $\psi(\alpha v) = \alpha \psi(v)$ for all v, v_1, v_2 and all α in F.

Define $\psi = G/K \to G'$ by $\psi(Ka) = \phi(a)$ for $a \in G$

If $Ka = Kb$, then $\psi(Ka) = \psi(Kb)$

$\Rightarrow$ if $Ka = Kb$, then $\phi(a) = \phi(b)$. But if $Ka = Kb$ then $a = kb$ for some $k \in K$

hence $\phi(a) = \phi(kb) = \phi(k)\phi(b)$?

since $k \in K$, the kernel of ϕ

then $\phi(k) = e'$, the identity element of G' so we get $\phi(a) = \phi(b)$. $\Rightarrow$ ψ is well defined

Chapter 5. Section 1

(9) Let F be a field. ---

Let $R = \mathbb{Z} \bmod p [x]$ and suppose that F is the field of fractions of R as in 4.7.1

$\Rightarrow F = \{f/g \mid f, g \in R, g \neq 0\}$

then $\phi(\lambda) = \lambda$ for every $\lambda \in \mathbb{Z} \bmod p$

by Fermat's. $\Rightarrow \phi(f(x)/g(x)) = f(x^p)/g(x^p)$

since ϕ is a ring homomorphism.

(10) If F is a finite field of characteristic p. ---

$\phi = F \to F$ is a one to one map between two sets of the same size $\Rightarrow \phi$ is bijective and onto as well.

Section 2

(2)
$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 \\ 3 & 4 & 2 & 0 \end{bmatrix} \sim \begin{matrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 1 & -1 & 0 \end{matrix} \quad \begin{matrix} \\ \\ \\ \end{matrix} \quad \begin{matrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & -3 & 0 \end{matrix}$$

(-3, -1)

The system has no non-trivial solution

(3) If V is a vector

With a basis $v_1 \dots v_n$ for V over $\mathbb{Z} \bmod p$ every element in V can be written as a linear combination $y = a_1 v_1 + \dots + a_n v_n$ for some $a_i \in V$

There are p choices for a_1, p choices for a_2, etc.

So, there are p^n choices in all. ∎

Because ϕ is onto G', given $x \in G'$, then $x = \phi(a)$ for some $a \in G$, thus $x = \phi(a) = \psi(Ka)$

This shows that ψ map G/K onto G'

Suppose that $\psi(Ka) = \psi(Kb)$; then $\phi(a) = \psi(Ka) =$

$= \psi(Kb) = \phi(b)$;

therefore $e' = \phi(a)\,\phi(b)^{-1} = \phi(a)\,\phi(b^{-1}) = \phi(ab^{-1})$

Because ab^{-1} is thus in the kernel of ψ – which is K – we have that $ab^{-1} \in K$. This implies that $Ka = Kb$

ψ is injective.

If $\psi((Ka)(Kb)) = \psi(Kab) = \phi(ab) = \phi(a)\,\phi(b) =$

$\psi(Ka)(Kb)$, using that ϕ is a homomorphism and that $(Ka)(Kb) = Kab$

$\therefore$ ψ is a homomorphism of G/K onto G'.

Section 3

① Show...

(a) $\sqrt{2} + \sqrt{3}$

$\alpha \in \mathbb{C}$ is an algebraic number if it is a root of a polynomial with integer coefficients

If $a = \sqrt{2} + \sqrt{3}$

$a^2 = 2 + 3 + 2\sqrt{6}$

so that $(a^2 - 5)^2 = 2 \Rightarrow a^4 - 10a^2 + 1 = 0$ so $\sqrt{2} + \sqrt{3}$ is an algebraic number

(b) $\sqrt{7} + \sqrt[3]{12} \rightarrow a = \sqrt{7} + \sqrt[3]{12} \Rightarrow (a - \sqrt{7})^3 = 12$

or $a^3 - 3\sqrt{7}a^2 + 37a - 7\sqrt{7} = 12$

$(a^3 + 21a - 12)^2 = 7(3a^2 + 7)^2 = 0$

$\sqrt{7} + \sqrt[3]{12}$ is an algebraic number

(c) $2+i\sqrt{3}$

$a = 2+i\sqrt{3}$

$a-2 = i\sqrt{3}$

$(x-2)^2 = (i\sqrt{3})^2$

$x^2-4x+4 = -3$

$x^2-4x+7 = 0 \Rightarrow 2+i\sqrt{3}$ is an algebraic number

(4) $a = \cos(2\pi/k) + i\sin(2\pi/k), \quad k>0$

$a = e^{i2\pi/k}$

$a^k = e^{i2\pi} = 1 \Rightarrow x^k - 1 = 0$

a is an algebraic number

(6) Show that

$e = 1 + \frac{1}{1!} + \cdots$ is irrational --- By contradiction

Suppose that e is a rational number. Then there exist positive integers a and b such that $e = a/b$

Define the number $x = b!\left(e - \sum_{n=0}^{b} \frac{1}{n!}\right)$

to see that x is an integer, substitute $e = a/b$ to get

$$x = b!\left(\frac{a}{b} - \sum_{n=0}^{b} \frac{1}{n!}\right) = a(b-1)! - \sum_{n=0}^{b} \frac{b!}{n!}$$

the first term is an integer and every fraction in the sum is an integer since $n \le b$ for each term. $\therefore x$ is an integer

We now prove that $0 < x < 1$. First insert the above series representation of e into the definition of x to obtain

$$x = \sum_{n=b+1}^{\infty} (b!)/(n!) > 0$$

For all items with $n \geq b+1$ we have the upper estimate

$$b!/n! = \frac{1}{(b+1)(b+2)(b+3)+\cdots+(b+(n-b))} \leq \frac{1}{(b+1)^{n-b}}$$

which is even for every $n \geq b+2$

Changing the index of summation to $k = n-b$ and using the formula for the infinite geometric series, we get

$$x = \sum_{n=b+1}^{\infty} \frac{b!}{n!} < \sum_{k=1}^{\infty} \frac{1}{(b+1)^k} = \frac{1}{b+1}\left(\frac{1}{1-\frac{1}{b+1}}\right) = \frac{1}{b} \leq 1$$

since there is no integer between 0 and 1 we have a contradiction and α must be IRRATIONAL.

(10) Is $\cos(1^\circ)$ algebraic over $\mathbb{Q}$ Note that

$\alpha^{2\pi i/360} = \alpha^{\pi i/180}$ is algebraic over $\mathbb{Q}$ because it is a root of the polynomial $x^{360} - 1 \in \mathbb{Q}[x]$

$\therefore \mathbb{Q}(\alpha^{i\pi/180})$ is an algebraic extension of $\mathbb{Q}$ and therefore any element of $\mathbb{Q}(\alpha^{i\pi/180})$ is algebraic over $\mathbb{Q}$.

$$\frac{\alpha^{i\pi/180} + \alpha^{-\pi i/180}}{2} = \frac{\cos\left(\frac{\pi}{180}\right) + i\sin\left(\frac{\pi}{180}\right) + \cos\left(\frac{\pi}{180}\right) - i\sin\left(\frac{\pi}{180}\right)}{2}$$

$$= \cos\left(\frac{\pi}{180}\right) = \cos(1^\circ) \Rightarrow \alpha^{-\pi i/180} = 1/\alpha^{\pi i/180}$$

implies $\cos(1^\circ) \in \mathbb{Q}(\alpha^{\pi i/180})$

(13) Let K be a finite field

Given that K and F are finite-dimensional as a vector space over F. With a basis $v_1 \dots v_n$ for V over $\mathbb{Z} \bmod p$ every element in V can be written as a linear combination $y = a_1 v_1 \dots a_n v_n$ for some $a_i \in V$. There are p choices for a_1, p choices for a_2, etc. So, there are p^n choices in all.

(14) Using (13)

Using K, a finite field, then K is of characteristic $p \neq 0$ where p is a prime number, and K contains the field F consisting of $0, 1, 2 \dots, p-1$ which has p elements and using result from (13) K has p^n elements

Section 5.4

① Show that

$a^2 = (\sqrt{2} - \sqrt{3})^2 = 5 - 2\sqrt{6}$

$(a^2 - 5)^2 = 24 \Rightarrow a^4 - 10a^2 + 1 = 0$

$\therefore f(x) = x^4 - 10x^2 + 1$ is a polynomial of degree 4 over $\mathbb{Q}$ such that $f(a) = 0$

③ $p(x) = x^5 + \sqrt{2}\,x^3 + \sqrt{5}\,x^2 + \sqrt{7}\,x + \sqrt{11}$

This is a polynomial over the field $\mathbb{Q}(\sqrt{2}\ \sqrt{5}\ \sqrt{7}\ \sqrt{11})$

If we were to adjoin a to this field the extension would be at most degree 5, since a's minimal polynomial must divide $p(x)$. So extending the square roots would be a maximum of 2 degrees at a time so 2 for each of the roots accounts for at most 16 degrees with the 5 it would be at most 80 degrees to the top.

⑤ If $[K:F] = 2^n$

Since $[T=F][K=F] = 2^n$

$[T=F]$ must be 2^m for some $m \leq n$

Section 5.5

(2)