EXERCISES AND SOLUTIONS IN GROUPS RINGS AND FIELDS

Mahmut Kuzucuoğlu
Middle East Technical University
matmah@metu.edu.tr
Ankara, TURKEY
April 18, 2012

TABLE OF CONTENTS

Preface

These notes are prepared in 1991 when we gave the abstract algebra course. Our intention was to help the students by giving them some exercises and get them familiar with some solutions. Some of the solutions here are very short and in the form of a hint. I would like to thank Bülent Büyükbozkırlı for his help during the preparation of these notes. I would like to thank also Prof. İsmail Ş. Güloğlu for checking some of the solutions. Of course the remaining errors belongs to me. If you find any errors, I should be grateful to hear from you. Finally I would like to thank Aynur Bora and Güldane Gümüş for their typing the manuscript in LATEX.

Mahmut Kuzucuoğlu

I would like to thank our graduate students Tuğba Aslan, Büşra Çınar, Fuat Erdem and İrfan Kadıköylü for reading the old version and pointing out some misprints. With their encouragement I have made the changes in the shape, namely I put the answers right after the questions.

20, December 2011

M. Kuzucuoğlu

1. SETS, INTEGERS, FUNCTIONS

1.1. *If A is a finite set having n elements, prove that A has exactly 2^n distinct subsets.*

Solution: Apply Induction on n.

If $|A| = 1$, then A has exactly two subsets namely ϕ and A. So the claim is true for $n = 1$.

Induction hypothesis: For any set having exactly $n-1$ elements, the number of subsets is 2^{n-1}. Let now $A = \{a_1, a_2, \cdots, a_n\}$ be a set with $|A| = n$. Any subset X of A is either contained in $B = \{a_1, \cdots, a_{n-1}\}$ or $a_n \in X$. By induction hypothesis, there are exactly 2^{n-1} subsets of A contained in B. Any other subset X of A which is not contained in B is of the form. $X = \{a_n\} \cup Y$ where Y is a subset of B. Their number is therefore equal to the number of subsets of B, i.e. 2^{n-1}. Then the number of all subsets of A is $2^{n-1} + 2^{n-1} = 2^n$.

1.2. *For the given set and relations below, determine which define equivalence relations.*

(a) S is the set of all people in the world today, $a \sim b$ if a and b have an ancestor in common.

(b) S is the set of all people in the world today, $a \sim b$ if a and b have the same father.

(c) S is the set of real numbers $a \sim b$ if $a = \pm b$.

(d) S is the set of all straight lines in the plane, $a \sim b$ if a is parallel to b.

Solution: $''$ b, c and d $''$ are equivalence relations, but $''$ a $''$ is not.

1.3. *Let a and b be two integers. If $a|b$ and $b|a$, then show that $a = \pm b$.*

Solution: If $a|b$, then $b = ka$ for some integer k. If $b|a$, then $a = \ell b$ for some integer l. Hence $b = ka = k\ell b$, then we obtain $b - k\ell b = 0$. This implies $b(1 - k\ell) = 0$ so either $b = 0$ or $k\ell = 1$. If $b = 0$, then $a = 0$ and hence $a = \pm b$ and we are done.

If $k\ell = 1$, then either $k = -1$ and $\ell = -1$ or $k = 1$ and $\ell = 1$. In the first case $b = -a$, in the second case $b = a$.
Hence $b = \pm a$.

1.4. *Let $p_1, p_2, \cdots, p_n$ be distinct positive primes. Show that $(p_1 p_2 \cdots p_n) + 1$ is divisible by none of these primes.*

Solution: Assume that there exists a prime say p_i where $i \leq n$ such that p_i divides $p_1 p_2 \cdots p_n + 1$. Then clearly $p_i | p_1 p_2 \cdots p_n$ and $p_i | p_1 p_2, \cdots p_n + 1$ implies that $p_i | 1 = (p_1 \cdots p_n + 1) - (p_1 \cdots p_n)$.

Which is impossible as $p_i \geq 2$. Hence none of the p_i's divides $p_1 \cdots p_n + 1$.

1.5. *Prove that there are infinitely many primes.*
(Hint: Use the previous exercise.)

Solution: Assume that there exists only finitely many primes say the list of all primes $\{p_1, p_2, \ldots p_n\}$. Then consider the integer $p_1 p_2 \cdots p_n + 1$.

Then by previous Question 1.4 none of the primes p_i $i = 1, \ldots, n$ divides $p_1 p_2 \cdots p_n + 1$. Hence either $p_1 p_2 \cdots p_n + 1$ is a prime which is not in our list or when we write $p_1 p_2 \cdots p_n + 1$ as a product of primes we get a new prime q which does not appear in $\{p_1, p_2, \cdots p_n\}$. Hence in both ways we obtain a new prime which is not in our list. Hence we obtain a contradiction with the assumption that the number of primes is n. This implies that the number of primes is infinite.

1.6. *If there are integers a, b, s, and t such that, the sum $at+bs = 1$, show that* $\gcd(a, b) = 1$.

Solution: We have

$$at + bs = 1$$

Assume that $\gcd(a, b) = n$. Then by definition $n|a$ and $n|b$ and if there exists $m|a$ and $m|b$, then $m|n$.

Since $n|a$ we have $n|at$ and $n|bs$. Hence $n|at + bs$. This implies $n|1$. i.e. $n = 1$

1.7. *Show that if a and b are positive integers, then*

$$ab = lcm(a, b) \cdot \gcd(a, b).$$

Solution: Let $\gcd(a, b) = k$ and $lcm(a, b) = l$. Then

$a = ka_1$ and $b = kb_1$ where $\gcd(a_1, b_1) = 1$ and $ab = k^2a_1b_1$.

By definition $a|l$ and $b|l$, moreover if there exists an integer s such that $a|s$ and $b|s$, then $l|s$.

Claim. $l = ka_1b_1 = ab_1 = a_1b$. Indeed we have $a|ka_1b_1$ and $b|ka_1b_1$. Assume that there exists an integer t such that $a|t$ and $b|t$. Then $t = ak_1$ and $t = bk_2$. We have $t = ak_1 = bk_2 = ka_1k_1 = kb_1k_2$. It follows that $a_1k_1 = b_1k_2$. Since a_1 and b_1 are relatively prime we have $a_1|k_2$ and $b_1|k_1$. Then $k_2 = a_1.c$ and $k_1 = b_1.u$. Then we have $a_1k_1 = a_1b_1u = b_1a_1c$ it follows that $u = c$ and $t = ak_1 = ka_1b_1c$ hence $l = ka_1b_1|t$.

2. GROUPS

2.1. *Let* S *be any set. Prove that the law of multiplication defined by* ab = a *is associative.*

Solution: Let $x, y, z \in S$. We want to show that $x(yz) = (xy)z$. Indeed

$x(yz) = xy = x$ by the law of multiplication in S. And $(xy)z = xz = x$, by the same law so $x(yz) = x = (xy)z$.

2.2. *Assume that the equation $xyz = 1$ holds in a group G. Does it follow that $yzx = 1$? That $yxz = 1$? Justify your answer.*

Solution: $xyz = 1$ implies that $x(yz) = 1$. Let $yz = a$. Then we have $xa = 1$ and so $ax = 1$ since a is invertible and $a^{-1} = x$. (See solution 6) It follows that $(yz)x = 1$. Hence $yzx = 1$.

On the other hand, if $xyz = 1$, it is not always true that $yxz = 1$. To see this, let G be the group of 2×2 real matrices and let $x = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$ $y = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$ and $z = \begin{pmatrix} -1/2 & 3/4 \\ 1 & -1 \end{pmatrix}$. Then $xyz = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$ in G. But $yxz = \begin{pmatrix} 2 & -2 \\ 5 & -9/2 \end{pmatrix} \neq 1$.

2.3. *Let G be a nonempty set closed under an associative product, which in addition satisfies:*

(a) There exists an $e \in G$ such that $ae = a$ for all $a \in G$.

(b) Given $a \in G$, there exists an element $y(a) \in G$ such that $ay(a) = e$.

Prove that G must be a group under this product.

Solution: Given $a \in G$. Since right inverse exists, there exists $y(a) \in G$ such that $ay(a) = e$. Then, $y(a) = y(a)e = y(a)(ay(a)) = (y(a)a)y(a)$. Also, there exists $t \in G$ such that $y(a)t = e$. This implies

that $(y(a)a)y(a)t = e$ then $(y(a)a)e = e$ Hence $y(a)a = e$. So every right inverse is also a left inverse.

Now for any $a \in G$ we have $ea = (ay(a))a = a(y(a)a) = ae = a$ as e is a right identity. Hence e is a left identity.

2.4. *If G is a group of even order, prove that it has an element $a \neq e$ satisfying $a^2 = e$.*

Solution: Define a relation on G by $g \sim h$ if and only if $g = h$ or $g = h^{-1}$ for all $g, h \in G$.

It is easy to see that this is an equivalence relation. The equivalence class containing g is $\{g, g^{-1}\}$ and contains exactly 2 elements if and only if $g^2 \neq e$. Let $C_1, C_2, \cdots, C_k$ be the equivalence classes of G with respect to $\sim$. Then

$$|G| = |C_1| + |C_2| + \cdots + |C_k|$$

Since each $|C_i| \in \{1, 2\}$ and $|G|$ is even the number of equivalence classes C_i, with $|C_i| = 1$ is even. Since the equivalence class containing $\{e\}$ has just one element, there must exist another equivalence class with exactly one element say $\{a\}$. Then $e \neq a$ and $a^{-1} = a$. i.e. $a^2 = e$.

2.5. *If G is a finite group, show that there exists a positive integer m such that $a^m = e$ for all $a \in G$.*

Solution: Let G be finite group and $1 \neq a \in G$.

Consider the set

$$a, a^2, a^3, \cdots, a^k \cdots$$

It is clear that $a^i \neq a^{i+1}$ for some integers from the beginning . Since G is a finite group there exists i and j such that $a^i = a^j$ implies $a^{i-j} = 1$.Therefore every element has finite order . That is the smallest positive integer k satisfying $a^k = 1$ (One may assume without loss of generality that $i > j$). One can do this for each $a \in G$. The least common multiple m of the order of all elements of G satisfies $a^m = 1$ for all $a \in G$.

2.6. *If G is a group in which $(ab)^i = a^i b^i$ for three consecutive integers i for all $a, b \in G$, show that G is abelian.*

Solution: Observe that if there exist two consecutive integers $n, n+1$ such that

$(ab)^n = a^n b^n$ and $(ab)^{n+1} = a^{n+1}b^{n+1}$ for all $a, b \in G$, then $a^{n+1}b^{n+1} = (ab)^{n+1} = (ab)^n ab = a^n b^n ab$. Then we obtain $a^{n+1}b^{n+1} = a^n b^n ab$.Now by multiplying this equation from left by a^n and from right by b^{-1} we obtain $ab^n = b^n a$.

In our case taking $n = i$ and $n = i + 1$, we have $ab^i = b^i a$ and by taking $n = i + 1$ and $i + 2$ we have $ab^{i+1} = b^{i+1}a$.

This shows that $ab^{i+1} = b^{i+1}a = bb^i a = bab^i$ and now multiplying from right by b^i we obtain $ab = ba$. Hence G is abelian.

2.7. *If G is a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$, then show that G must be abelian.*

Solution: $abab = a^2b^2$ apply a^{-1} from left and b^{-1} from right. We obtain $ba = ab$ for all $a, b \in G$.
Hence G is abelian.

2.8. *Let a, b be elements of a group G. Assume that a has order 5 and $a^3b = ba^3$. Prove that $ab = ba$.*

Solution: We have $a^5 = e$ and $a^3b = ba^3$. Applying a^3 to the second equation we obtain $a^3(a^3b) = a^3(ba^3) = (a^3b)a^3 = (ba^3)a^3$ and hence $a^6b = ba^6$

As $a^6 = a^5 \cdot a = ea = a$ we obtain $ab = ba$.

2.9. *Let a and b be integers.*

(a) Prove that the subset $a\mathbf{Z} + b\mathbf{Z} = \{ak + bl \mid l, k \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$.

(b) Prove that a and $b + 7a$ generate the subgroup $a\mathbf{Z} + b\mathbf{Z}$.

Solution: a) Clearly $a\mathbf{Z} + b\mathbf{Z} \neq \phi$. Let $ak_1 + b\ell_1, ak_2 + b\ell_2$ be two elements in $a\mathbf{Z} + b\mathbf{Z}$ where $k_1, k_2, \ell_1, \ell_2 \in \mathbf{Z}$.We have $(ak_1 + b\ell_1) - (ak_2 + b\ell_2) = a(k_1 - k_2) + b(\ell_1 - \ell_2) \in a\mathbf{Z} + b\mathbf{Z}$ as $k_1 - k_2, \ell_1 - \ell_2 \in \mathbf{Z}$ This implies $a\mathbf{Z} + b\mathbf{Z}$ is a subgroup of $\mathbf{Z}$.

b) Firstly $a, b+7a \in a\mathbf{Z}+b\mathbf{Z}$. Secondly, given any $ak+b\ell \in a\mathbf{Z}+b\mathbf{Z}$ we can write $ak + b\ell = a(k - 7\ell) + (b + 7a)\ell$ this implies a and $b + 7a$ generate $a\mathbf{Z} + b\mathbf{Z}$.

2.10. *Let H be the subgroup generated by two elements a, b of a group G. Prove that if $ab = ba$, then H is an abelian group.*

Solution: The elements of H are of the form: $a^{i_1}b^{i_2}a^{i_3}\cdots a^{i_{k-1}}b^{i_k}$ where $i_1, \cdots i_k \in \mathbf{Z}$, for some k.

So let $x, y \in H$ Then we can write $x = a^{i_1}b^{i_2}\cdots a^{i_{k-1}}b^{i_k}$ and $y = a^{j_1}b^{j_2}\cdots a^{j_{\ell-1}}b^{j_\ell}$.

Then $xy = (a^{i_1}\cdots b^{i_k})(a^{j_i}\cdots b^{j_\ell})$ since $ab = ba$ we can interchange each term in this multiplication, and obtain: $xy = (a^{j_1}\cdots b^{j_\ell})(a^{i_1}\cdots b^{i_k}) = yx$.

This implies H is abelian.

2.11. *(a) Assume that an element x of a group has order rs. Find the order of x^r.*

(b) Assuming that x has arbitrary order n, what is the order of x^r?

Solution: (a) Since $x^{rs} = 1$, we have $(x^r)^s = 1$. This implies that the order of $x^r \leq s$. Let us assume that order of x^r is k.

Since $(x^r)^k = 1, x^{rk} = 1 = x^{rs}$ This implies that $x^{rs-rk} = 1$ It follows that $rs - rk = 0$ since rs is the order of x and $rs - rk < rs$.This implies $s = k$.that is to say the order of x^r is s.

(b) Let k be the order of x^r. Then $(x^{rk}) = 1 \Rightarrow x^{rk} = 1$. We also have $x^n = 1$ which implies rk is a multiple of n. Since it should be the smallest such number and it also is a multiple of r, we conclude that rk is the least common multiple of r and n.Then $k = \frac{\ell cm(r,n)}{r}$.

2.12. *Prove that in any group the orders of ab and of ba are equal.*

Solution: Let $(ab)^k = 1$. Then

$$abab\cdots ab = 1 \text{ This implies } a(ba)(ba)\cdots(ba)b = 1$$

$$\text{We have } a(ba)^{k-1}b = 1 \Rightarrow (ba)^{k-1} = a^{-1}b^{-1} = (ba)^{-1}$$

$$\text{We obtain } (ba)^{k-1}(ba) = 1 \text{which implies } (ba)^k = 1.$$

Similarly if $(ba)^\ell = 1$, then $(ab)^\ell = 1$.
Hence orders of ab and ba are the same.

2.13. *Let G be a group such that the intersection of all its subgroups which are different from $\{e\}$ is a subgroup different from identity. Prove that every element in G has finite order.*

Solution: Let $\cap_{\{e\}\neq H\leq G} H = K \neq \{e\}$. Let $e \neq a \in G$.

Then consider the subgroups $H_i = \langle a^i \rangle$ for $i = 1, 2, 3 \cdots$ are subgroups of G. For each $i \in \mathbf{N}$ such that $H_i \neq \{e\}$ we have $K \leq H_i$. Hence K is cyclic as every subgroup of a cyclic group is cyclic. Hence $K = \langle a^n \rangle$ for some fixed positive integer n. Since $\langle a^n \rangle \leq \langle a^i \rangle$ if and only if $a^n = a^{ik}$ if and only if $n = ik$ if and only if $i|n$, we obtain $i|n$ for each $i = 1, 2, 3, \ldots$ with $H_i \neq \{e\}$. As n is a fixed given positive integer it has only finitely many divisors. Since $K \neq e$ we have only finitely many $H_i \neq e$ i.e. So there exists j, such that $H_j = \langle a^j \rangle = e$ i.e. $a^j = e$.

2.14. *Show that if every element of the group G is its own inverse, then G is abelian.*

Solution: For all $x, y \in G$ we have

$(xy)^{-1} = xy$ and $x^{-1} = x$ and $y^{-1} = y$. Then $(xy)^{-1} = xy$. This implies $y^{-1}x^{-1} = xy$. Hence $yx = xy$

.

2.15. *Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo 2, such that $ad - bc \neq 0$. Using matrix multiplications as the operation in G prove that G is a group of order 6.*

Solution: In the first row of any matrix belonging to G, each entry could be 0 or 1 in $\mathbf{Z}_2$, but $(0, 0)$ should be extracted since $ad - bc \neq 0$. Hence we have $2^2 - 1$ different choices for the first row. The second row is not a multiple of the first row. Hence G has $(2^2 - 1)2$ elements, namely 6. It can be checked that this set is closed under multiplication, and also obviously each element has its inverse in this set. Since matrix multiplication is associative, G is a group with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

2.16. *Let G be the group of all non-zero complex numbers $a+bi$ (a, b real, but not both zero) under multiplication, and let*

$$H = \{\ a+bi \in G \mid a^2+b^2 = 1\ \}$$

Verify that H is a subgroup of G.

Solution: If $a=1,\ b=0$, then $a+bi \in H$ so H is non-empty. Let $a+bi, c+di \in H$. Then

$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i$$

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

$$= a^2(c^2+d^2)+b^2(c^2+d^2) = (a^2+b^2)(c^2+d^2) = 1.$$

Hence H is closed with respect to multiplication. Now for the inverse

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = a-bi \ \text{ as } \ a^2+b^2 = 1$$

Hence $\frac{1}{a+bi} = (a+bi)^{-1} \in H$ and H is a subgroup of G.

2.17. *Let G be a finite group whose order is not divisible by 3. Suppose that $(ab)^3 = a^3b^3$ for all $a, b \in G$. Prove that G must be abelian.*

Solution: Let $|G| = n$. Since $(3, n) = 1$ there exist $x, y \in Z$ such that $3x+ny = 1$. Here x can be taken positive.

Now consider

$ab = (ab)^{3x+ny} = (ab)^{3x}(ab)^{ny}$. Since $|G| = n$ and $ab \in G$, we have $(ab)^n = e$. Hence

$$ab = (ab)^{3x} = (a^3b^3)^x = \underbrace{a^3b^3a^3b^3\cdots a^3b^3}_{x-\text{times}}$$

$$= a^3\underbrace{(b^3a^3)(b^3a^3)\cdots(b^3a^3)}_{(x-1)\ \text{times}}b^3$$

$$\begin{aligned} = a^3(b^3a^3)^{x-1}b^3 &= a^3(ba)^{3x-3}b^3 \\ &= a^3(ba)^{3x}(ba)^{-3}b^3 \\ &= a^3(ba)^{3x}(ba)^{ny}(ba)^{-3}b^3 \\ &= a^3(ba)^{3x+ny}(ba)^{-3}b^3 \\ &= a^3(ba)(ba)^{-3}b^3 = a^3(ba)^{-3}(ba)b^3 \\ = a^3a^{-3}b^{-3}(ba)b^3 &= b^{-2}ab^3 = b^{-2}a^{-2}a^3b^3 = (b^{-2}a^{-2})(ab)^3 \end{aligned}$$

Hence we get $ab = b^{-2}a^{-2}(ab)^3$.

Now multiplying from right by $(ab)^{-1}$ and from left by b^2 and a^2 we obtain

$$(ab)^2 = a^2b^2 \ \ i.e. \ \ abab = a^2b^2$$

Multiply from left by a^{-1} and from right by b^{-1} we obtain $ba = ab$ for all $a, b \in G$.

2.18. *Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $ad - bc \neq 0$ and a, b, c, d are integers module 3 relative to matrix multiplication. Show that $|G| = 48$.*

b) If we modify the example of G in part (a) by insisting that $ad - bc = 1$, then what is $|G|$?

Solution: For the first row (a, b) of a matrix in G a and b could be anything in Z_3, but we must exclude the case $a = 0$ and $b = 0$. Hence $(3 \times 3) - 1$ possibilities for the first row. The second row should be <u>not</u> a multiple of the first row. Hence for the second row $(3 \times 3) - 3$ possibilities. Hence the number of elements in G is $8 \times 6 = 48$.

(b) The set of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $ad - bc = 1$ forms a subgroup H of G. Moreover for any $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ either $ad - bc =$ $\det(g) = 1$ or $\det(g) = -1 (\equiv 2 (mod\ 3))$. On the other hand for any $Hg_1, Hg_2 \in G$, $Hg_1 = Hg_2$ if and only if $\det(g_1) = \det(g_2)$. (Why?)

Hence the above subgroup has index 2 in G, i.e. H has order 24.

(By using determinant homomorphism; this can be seen more easily.)

2.19. *(a) If H is a subgroup of G, and $a \in G$ let $aHa^{-1} = \{\ aha^{-1} \mid h \in H\ \}$*

Show that aHa^{-1} is a subgroup of G.

(b) If H is finite, what is the order $o(aHa^{-1})$.

Solution: (a) Since H is a subgroup clearly aHa^{-1} is non-empty. Let ah_1a^{-1} and $ah_2a^{-1} \in aHa^{-1}$. Then

$$\begin{aligned}(ah_1a^{-1})(ah_2a^{-1})^{-1} &= (ah_1a^{-1})(ah_2^{-1}a^{-1}) \\ &= ah_1h_2^{-1}a^{-1} \in aHa^{-1}\end{aligned}$$

as $h_1h_2^{-1} \in H$.

(b) Define a map $\alpha : H \to aHa^{-1}$ by $\alpha(h) = aha^{-1}$ for all $h \in H$. The map

α is $1-1$ and onto. Hence if H is a finite group then $o(H) = o(aHa^{-1})$.

2.20. *The center Z of a group G is defined by $Z = \{\ z \in G \mid zx = xz$ for all $x \in G\ \}$.*

Prove that Z is a subgroup of G.

Solution: Let $z, w \in Z$. Hence $xw = wx$ for all $x \in G$. Then we have $w^{-1}x = xw^{-1}$ for all $x \in G$, i.e. $w^{-1} \in Z$. Moreover $(zw)x = z(wx) = z(xw) = (zx)w = x(zw)$

Hence $zw \in Z$ and Z is a subgroup of G.

2.21. *If H is a subgroup of G, then by the centralizer $C_G(H)$ of H we mean the set $\{\ x \in G \mid xh = hx$ for all $x \in H\ \}$. Prove that $C_G(H)$ is a subgroup of G.*

Solution: Clearly $1 \in C_G(H)$, so $C_G(H) \neq \emptyset$. Let $x, y \in C_G(H)$. By assumption $xh = hx$ and $yh = hy$ for all $h \in H$. Hence $hy^{-1} = y^{-1}h$ for all $h \in H$. Hence $y^{-1} \in C_G(H)$. Now consider

$$\begin{aligned}(xy)(h) = x(yh) &= x(hy) \text{ as } y \in C_G(H)\\ &= (xh)y\\ &= h(xy). \text{ Hence } xy \in C_G(H)\end{aligned}$$

2.22. *If $a \in G$ define $C_G(a) = \{\ x \in G \mid xa = ax\ \}$. Show that $C_G(a)$ is a subgroup of G. The group $C_G(a)$ is called the centralizer of a in G.*

Solution: Let $x, y \in C_G(a)$. If $ya = ay$, then $ay^{-1} = y^{-1}a$ hence $y^{-1} \in C_G(a)$ and moreover $(xy)a = x(ya) = x(ay) = a(xy)$. Hence $xy \in C_G(a)$. (Observe that $C_G(a) = C_G(\langle a \rangle)$.)

2.23. *If N is a normal subgroup of G and H is any subgroup of G prove that NH is a subgroup of G.*

Solution: Let n_1h_1 and n_2h_2 be two elements in NH, where $n_i \in N$,and $h_i \in H, i = 1, 2$. Then

$$\begin{aligned}n_1h_1(n_2h_2)^{-1} &= n_1h_1h_2^{-1}n_2^{-1}\\ &= n_1h_1h_2^{-1}n_2^{-1}(h_2h_1^{-1})(h_1h_2^{-1})\\ &= n_1h_1h_2^{-1}n_2^{-1}(h_1h_2^{-1})^{-1}(h_1h_2^{-1})\\ &= n_1n_3h_1h_2^{-1} \in NH \text{ as } n_1n_3 \in N\\ \text{where } n_3 &= (h_1h_2^{-1})n_2^{-1}(h_1h_2^{-1})^{-1} \in N\end{aligned}$$

and $h_1h_2^{-1} \in H$.

2.24. *Suppose that H is a subgroup of G such that whenever $Ha \neq Hb$, then $aH \neq bH$. Prove that $gHg^{-1} \subseteq H$.*

Solution: Assume (if possible) that $gHg^{-1} \not\subseteq H$ for some g in G. Then there exists $1 \neq h \in H$ such that $ghg^{-1} \notin H$. Hence $ghg^{-1}H \neq H$. This implies $hg^{-1}H \neq g^{-1}H$ (otherwise $ghg^{-1}H = H$). Then by assumption and by the above observation we have, $Hhg^{-1} = Hg^{-1} \neq Hg^{-1}$. This is a contradiction. Hence gHg^{-1} must lie in H for any

$g \in G$.

2.25. *Suppose that N and M are two normal subgroups of G and that $N \cap M = \{e\}$. Show that for any $n \in N, m \in M$, $nm = mn$.*

Solution: Consider $nmn^{-1}m^{-1}$ in two ways. Firstly $(nmn^{-1})m^{-1} \in M$ as $nmn^{-1} \in M$ and $m^{-1} \in M$, secondly $n(mn^{-1}m^{-1}) \in N$ as $n \in N$ and $mn^{-1}m^{-1} \in N$. Hence

$nmn^{-1}m^{-1} \in N \cap M = \{e\}$. We obtain $nmn^{-1}m^{-1} = e$ i.e. $nm = mn$ for all $n \in N$ and $m \in M$.

2.26. *If G is a group and H is a subgroup of index 2 in G, then prove that H is a normal subgroup of G.*

Solution: Let H and aH be the left cosets of H in G and H and Hb be right cosets of H in G.

Since there are only two cosets $aH = G \setminus H$ and $Hb = G \setminus H$, then we have $aH = Hb$. In order to show that H is normal in G, we want to see that $xH = Hx$ for any $x \in G$. Let $x \in G$. If $x \in H$, then certainly $xH = H = Hx$ i.e. $xH = Hx$. If $x \in G \setminus H = aH = Hb$, then there exist $h_1, h_2 \in H$ such that $x = ah_1 = h_2b$. Then $xH = (ah_1)H = aH = Hb = H(h_2b) = Hx$, i.e. $xH = Hx$ for any $x \in G$.

2.27. *Show that the intersection of two normal subgroups of G is a normal subgroup of G.*

Solution: It is clear that the intersection of two subgroups of G is a subgroup of G.

Let N and M be normal subgroups of G.

Then for any $g \in G$ and any $n \in N$ and any $m \in M$ we have $gng^{-1} \in N$ and $gmg^{-1} \in M$.

Let $w \in N \cap M$. Since $w \in N$ we have $gwg^{-1} \in N$ and since $w \in M$ we have $gwg^{-1} \in M$. Hence $gwg^{-1} \in N \cap M$ for any $g \in G$ i.e. $N \cap M$ is a normal subgroup of G.

2.28. *If N and M are normal subgroups of G, prove that NM is also a normal subgroup of G.*

Solution: By Question 2.23 NM is a subgroup of G. We need to show that for any $g \in G$ any $nm \in NM$ where $n \in N, m \in M$, we have $gnmg^{-1} \in NM$.

But $gnmg^{-1} = gng^{-1}gmg^{-1} \in NM$ since $gmg^{-1} \in M$ and $gng^{-1} \in N$.

2.29. *If a cyclic group T of G is normal in G, then show that every subgroup of T is a normal subgroup in G.*

Solution: Let $T = \langle t \rangle$ be a cyclic group. Then for any $g \in G$ we have $gtg^{-1} = t^i$ for some $i \in Z$. Let H be a subgroup of T. Hence H is cyclic and generated by t^n for some n. Now consider

$gt^ng^{-1} = (gtg^{-1})^n = t^{in} = (t^n)^i \in H$. Hence H is a normal subgroup of G.

2.30. *If N is a normal subgroup in the finite group such that $(|G : N|, |N|) = 1$. Show that any element $x \in G$ satisfying $x^{|N|} = e$ must be in N.*

Solution: Let x be an element in G such that $x^{|N|} = e$. Since $(|G : N|, |N|) = 1$ there exist $m, n \in \mathbf{Z}$ such that

$$m|G : N| + n|N| = 1.$$

Then $x = x^{m|G:N|+n|N|} = x^{m|G:N|}x^{n|N|}$. Since $x^{|N|} = e$ we have

$x = x^{m|G:N|}$. Consider the element xN of G/N. Since $(xN)^{|G/N|} = (x^{|G/N|}\ N)$ we have $(xN)^{|G/N|} = N$ the identity element of G/N that means $x^{|G/N|} \in N$ and so $x = (x^{|G:N|})^m \in N$.

2.31. *Let G be a group in which for some integer $n > 1, (ab)^n = a^nb^n$ for all $a, b \in G$. Show that*

a) $G^n = \{\ x^n \mid x \in G\ \}$ is a normal subgroup of G.

b) $G^{n-1} = \{\ x^{n-1} \mid x \in G\ \}$ is a normal subgroup of G.

Solution: (a) First we show that G^n is a subgroup of G. Let $x^n, y^n \in G^n$. Then $x^ny^n = (xy)^n \in G^n$ and $(x^{-1})^n = (x^n)^{-1} \in G^n$. Hence G^n is a subgroup of G.

Let $g \in G$. Then $gx^ng^{-1} = (gxg^{-1})^n \in G^n$ hence G^n is a normal subgroup of G.

(b) Let x^{n-1} and y^{n-1} be two elements in G^{n-1}. Then first observe that for any $x, y \in G$ we have $(xy)^n = x(yx)^{n-1}y = x^n y^n$ and by making the cancellations we get $(yx)^{n-1} = x^{n-1}y^{n-1}$. So for $x^{n-1}, y^{n-1} \in G^{n-1}$, their product $(yx)^{n-1}$ is also in G^{n-1}. Clearly $(x^{n-1})^{-1} = (x^{-1})^{n-1} \in G^{n-1}$.

Let $g \in G$ and $x^{n-1} \in G^{n-1}$. Then $gx^{n-1}g^{-1} = (gxg^{-1})^{n-1} \in G^{n-1}$. Hence G^{n-1} is normal in G.

2.32. *Let P and Q be two normal p-subgroups of a finite group G. Show that PQ is a normal p-subgroup of G.*

Solution: We already know that PQ is a normal subgroup of G by exercise 2.28

As $|PQ| = \frac{|P||Q|}{|P \cap Q|}$ and $|P|$ and $|Q|$ are powers of $p, |P \cap Q|$ is also a power of p. And so PQ is a p-group.

2.33. *If H is a subgroup of G such that the product of any two right cosets of H in G is again a right coset of H in G, prove that H is normal in G.*

Solution: Let Ha and Hb be two right cosets of H in G. By assumption $HaHb$ is a right coset of H in G. The set $Ha\,Hb$ contains the element ab. So the right coset should contain ab. Since there is only one right coset of H in G containing ab, which is Hab, we have $HaHb = Hab$ for all $a, b \in G$. Hence $HaH = Ha$ for all $a \in G$. i.e. h_1ah_2 is equal to h_3a for some $h_3 \in H$. But $h_1ah_2 = h_3a$ implies $ah_2a^{-1} = h_1^{-1}h_3$.

So for any $h_2 \in H$ and any $a \in G$

$ah_2a^{-1} = h_1^{-1}h_3 \in H$ i.e. H is normal in G.

2.34. *If $\varphi : G \to H$ is a homomorphism and G is abelian, then $Im\varphi = \{\ \varphi(g) \mid g \in G\ \}$ is abelian.*

Solution: Let $\varphi(g_1), \varphi(g_2) \in Im\varphi$. Then $\varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1g_2^{-1}) \in Im\varphi$. Hence $Im\varphi$ is a subgroup of H.

$\varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \varphi(g_2g_1)$ as G is abelian. Now φ is a homomorphism implies

$\varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \varphi(g_2g_1) = \varphi(g_2)\varphi(g_1)$. Hence $Im\varphi$ is abelian.

2.35. *If N, M are normal subgroups of G prove that $NM/M \cong N/N \cap M$.*

Solution: Define a map $\psi : N \longrightarrow NM/M$ as $\psi(x) = xM$ for $x \in N$.

ψ is clearly well defined and a homomorphism since $\psi(xy) = (xyM) = (xM)(yM) = \psi(x)\psi(y)$ for any $x, y \in N$

$$\begin{aligned} K_\psi &= \{\ x \in N \mid xM = M\ \} \\ &= \{\ x \in N \mid x \in M\ \} = N \cap M. \end{aligned}$$

Obviously ψ is onto. Hence by isomorphism theorem:

$$N/K_\psi = N/N \cap M \cong NM/M.$$

2.36. *Let V be the set of real numbers, and for $a, b \in$ real numbers, $a \neq 0$, let $\tau_{a,b} : V \to V$ defined by $\tau_{a,b}(x) = ax + b$. Let $G = \{\ \tau_{a,b} \mid a, b$ real $a \neq 0\ \}$ and*

$N = \{\ \tau_{1b} \in G\ \}$

a) Prove that G is a group with respect to composition of maps.

b) Prove that N is a normal subgroup of G and that G/N is isomorphic to a group of non-zero real numbers under multiplication.

Solution: (a) G is closed with respect to composition of maps. Indeed

let $g, h \in G$. Then there exist $a, b, c, d \in \mathbf{R}$, $a \neq 0 \neq c$ such that $g = \tau_{a,b}$, $h = \tau_{c,d}$.Then for any $x \in \mathbf{R}$, we have

$(\tau_{a,b} \circ \tau_{c,d})(x) = \tau_{a,b}(cx + d) = a(cx + d) + b$

$= acx + (ad + b)$

Since with $a \neq 0 \neq c$ we have $ac \neq 0, ac \in \mathbf{R}$, $ad + b \in \mathbf{R}$, we see that

$$(\tau_{a,b} \circ \tau_{c,d})(x) = \tau_{ac,ad+b}(x)$$

for any $x \in \mathbf{R}$. i.e. $\tau_{a,b} \circ \tau_{c,d} = \tau_{ac,ad+b} \in G$. This means that $g.h \in G$ for any $g, h \in G$. This binary operation on G is associative, since composition of maps is associative. $\tau_{1,0}$ is the identity function on $\mathbf{R}$ and hence is the identity element of G. For any $0 \neq a \in \mathbf{R}, b \in \mathbf{R}$

$\tau_{a,b} \circ \tau_{a^{-1},-a^{-1}b} = \tau_{aa^{-1},a(-a^{-1}b)+b} = \tau_{1,0}$

$\tau_{a^{-1},-a^{-1}b} \circ \tau_{a,b} = \tau_{a^{-1}a,a^{-1}(b)-a^{-1}b} = \tau_{1,0}$ thus $\tau_{a^{-1}b} = (\tau_{a,b})^{-1}$. i.e. every element of G has an inverse in G. Hence G is a group with respect to this operation.

(b) Observe that the map $\psi : G \to \mathbf{R} - \{0\}$ defined by $\psi(\tau_{a,b}) = a$ is a homomorphism from the group G onto the multiplicative group of real numbers:

$$\begin{aligned} \psi(\tau_{a,b} \circ \tau_{c,d}) &= \psi(\tau_{ac,ad+b}) = ac \\ &= \psi(\tau_{a,b})\psi(\tau_c, d) \end{aligned}$$

for any $\tau_{a,b}, \tau_{c,d} \in G$.

$$K_\psi = \{\ \tau_{a,b} \mid \psi(\tau_{a,b}) = 1\ \} = \{\ \tau_{1,b} \mid b \in \mathbf{R}\ \} = N$$

Hence N is a normal subgroup of G. Therefore by isomorphism theorem G/N is isomorphic to the multiplicative group of real numbers.

2.37. *Let G be a finite group and α be an automorphism of G satisfying $\alpha(x) = x$ implies that $x = e$ and $\alpha^2(x) = x$ for all $x \in G$. Then show that G is an abelian group.*

Remark. Such an automorphism of G is called a **fixed point free automorphism** of G of order 2 or fixed point free involutory automorphism of G.

Solution: First consider the following map $f : G \to G$, $f(y) = y^{-1}\alpha(y)$. The map f is a one to one map. Indeed if

$y^{-1}\alpha(y) = t^{-1}\alpha(t)$, then multiplying from left by t and from right by $\alpha(y)^{-1}$ we obtain

$ty^{-1} = \alpha(ty^{-1})$. Since α does not fix any element except identity we have

$ty^{-1} = e$. Hence $t = y$ and f is one to one.

Since G is a finite group a one to one map from G to G is onto. So for every element g in G there exists $x \in G$ such that $g = x^{-1}\alpha(x)$. Now

$\alpha(g) = \alpha(x^{-1}\alpha(x)) = \alpha(x^{-1})x = \alpha(x)^{-1}x = g^{-1}$. This means α inverts every element of G. But then $\alpha(gh) = \alpha(g)\alpha(h)$ implies

$(gh)^{-1} = g^{-1}h^{-1}$

$h^{-1}g^{-1} = g^{-1}h^{-1}$. Hence $gh = hg$ for all $h, g \in G$. i.e. G is abelian.

2.38. *In the following, verify if the mappings defined from G to $\overline{G}$ are homomorphisms, and in those cases in which they are homomorphisms, determine the kernel.*

(a) $G = \overline{G}$ is the group of non-zero real numbers under multiplication, $\psi(x) = x^2$ for all $x \in G$.

(b) $G, \overline{G}$ as in (a) and $\psi(x) = 2^x$.

(c) G is the group of real numbers under addition, $\overline{G} = G,\ \psi(x) = x + 1$ all $x \in G$.

(d) $G, \overline{G}$ as in (c), $\psi(x) = 13x$ for all $x \in G$.

(e) G is any abelian group $\overline{G} = G,\ \psi(x) = x^5$ all $x \in G$.

Solution: a) ϕ is a homomorphism as $\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y)$ since real numbers are commutative group with respect to multiplication.

$$K_\phi = \{x \in \mathbf{R} \mid x^2 = 1\} = \{\pm 1\}$$

(b) $\phi(xy) = 2^{xy}$

$\phi(x) = 2^x$ and $\phi(y) = 2^y$ but $\phi(x)\phi(y) = 2^{x+y} \neq 2^{xy}$. Hence ϕ is**not** a homomorphism.

(c) $\phi(x + y) = x + y + 1$ but $\phi(x) + \phi(y) = x + y + 2$. Hence ϕ is not a homomorphism.

(d) $\phi(x + y) = 13(x + y) = 13x + 13y = \phi(x) + \phi(y)$. Hence ϕ is a homomorphism.

$K_\phi = \{x \in G \mid \phi(x) = 0\} = \{x \in G \mid 13x = 0\} = \{0\}$

(e) $\phi(xy) = x^5y^5 = \phi(x)\phi(y)$. Hence ψ is a homomorphism $K_\phi = \{x \in G \mid x^5 = e\}$.

2.39. *Let G be the group of non-zero complex numbers under multiplication and let N be the set of complex numbers of absolute value 1 (that is $a + bi \in N$ if $a^2 + b^2 = 1$).*

Show that G/N is isomorphic to the group of all positive real numbers under multiplication.

Solution: First we show that the set of complex numbers of absolute value 1 is a normal subgroup of the set of complex numbers.

Indeed if $z_1, z_2 \in N$, then $|z_1| = 1, |z_2| = 1$. Then $|z_1z_2| = |z_1||z_2| = 1$ and $|\frac{1}{z_1}| = \frac{1}{|z_1|} = 1$. Hence N is a subgroup of $\mathbf{C}$; moreover since $\mathbf{C}$ is abelian, every subgroup is normal. Hence N is normal in $\mathbf{C}$.

Define a map $\psi : C \longrightarrow \mathbf{R}$

$$x + iy \longrightarrow x^2 + y^2$$

ψ is a homomorphism as

$$\psi((x + iy)(t + iv)) = \psi(x + iy)\psi(t + iv).$$

Image of ψ is the set of all positive real numbers. Indeed, if a is a positive real number there exists $w \in \mathbf{R}$ such that $w^2 = a$. $w + 0i \in \mathbf{C}$ such that $\psi(w + 0i) = a$. Hence ψ is onto. By isomorphism theorem $\mathbf{C}/N$ is isomorphic to the multiplicative group of positive real numbers.

2.40. *Let $x, y \in G$ and let $xy = z \in Z(G)$, show that x and y commute.*

Solution: Now $zx = xz$. Namely $xyx = xxy$. Now multiplying from left by x^{-1} we obtain $yx = xy$.

2.41. *If $G/Z(G)$ is cyclic, show that G is abelian.*

Solution: Let $G/Z(G) = \langle xZ(G)\rangle$

Let $a, b \in G$. Then there exist an integer such that $aZ(G) = x^iZ(G)$ as $G/Z(G)$ is cyclic. This implies $a = x^iz$ for some $z \in Z(G)$. Similarly there exists an integer j such that $b = x^jw$ for some $w \in Z(G)$.

Now consider $ab = x^izx^jw = x^ix^jzw$ as $z \in Z(G)$, then $ab = x^ix^jzw = x^{i+j}zw = x^jx^izw = x^jwx^iz$ as $\omega \in Z(G)$, which is ba.

Hence for all $a, b \in G$ $ab = ba$ i.e. G is abelian.

2.42. *Compute* $a^{-1}ba$ *where*
$a = (1,3,5)(1,2)$ *and* $b = (1,5,7,9)$

Solution: $a^{-1} = (1,2)(5,3,1)$
$a^{-1}ba$
$= (1,2)(5,3,1)(1,5,7,9)(1,3,5)(1,2) = (3,7,9,5)$

2.43. *Find the cycle structure of all the powers of* $(1,2,\cdots,8)$

Solution:

$$\begin{aligned}
g^2 &= (1,2,3,4,5,6,7,8)(1,2,3,4,5,6,7,8) = (1,3,5,7)(2,4,6,8)\\
g^3 &= (1,2,3,4,5,6,7,8)(1,3,5,7)(2,4,6,8) = (1,4,7,2,5,8,3,6)\\
g^4 &= (1,2,3,4,5,6,7,8)(1,4,7,2,5,8,3,6) = (1,5)(2,6)(3,7)(4,8)\\
g^5 &= (1,2,3,4,5,6,7,8)(1,5)(2,6)(3,7)(4,8) = (1,6,3,8,5,2,7,4)\\
g^6 &= (1,2,3,4,5,6,7,8)(1,6,3,8,5,2,7,4) = (1,7,5,3)(2,8,6,4)\\
g^7 &= (1,2,3,4,5,6,7,8)(1,7,5,3)(2,8,6,4) = (1,8,7,6,5,4,3,2)\\
g^8 &= (1)
\end{aligned}$$

2.44. *Prove that* $(1,2,\cdots,n)^{-1} = (n,n-1,n-2,\cdots,2,1)$.

Solution: To show that it is the inverse we look at $gg^{-1} = g^{-1}g = e$.

$(1,2,3,4,\cdots,n)(n,n-1,\cdots,2,1) = (1)$

$(n,n-1,\cdots,2,1)(1,2,3,\cdots n) = (1)$

2.45. *Express as the product of disjoint cycles:*
a) $(1,2,3)(4,5)(1,6,7,8,9)(1,5)$.
b) $(1,2)(1,2,3)(1,2)$.

Solution: Express as the product of disjoint cycles:
a) (1,2,3)(4,5) (1,6,7,8,9) (1,5) = (1,2,3,6,7,8,9,5,4)
b) (1,2)(1,2,3)(1,2)= (1,3,2)

2.46. *Find all normal subgroups in S_4.*

Solution: $\{(1)\}$, S_4,
$V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$
$A_4 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3),$
$(1,2,3), (1,3,4), (2,3,4), (1,2,4), (2,4,3), (1,4,3), (1,3,2), (1,4,2)\ \}$
So S_4 has four normal subgroups.

2.47. *Give an example of a group G, subgroup H and an element $a \in G$ such that $aHa^{-1} \subset H$ but $aHa^{-1} \neq H$*

Solution: $G = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \ \ a, b, c, d \in \mathbf{R}\}$

Let $H = \{\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \mid x \in Z\}$, obviously $H \leq G$ and let

$$g = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix},$$

Then $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2x & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2x & 1 \end{pmatrix}$
$gHg^{-1} = \{\begin{pmatrix} 1 & 0 \\ 2x & 1 \end{pmatrix} \mid x \in Z\}$ so

$gHg^{-1} \leq H$ but $gHg^{-1} \neq H$ as $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \notin gHg^{-1}$ but $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in H$.

2.48. *Prove that any group of order 15 is cyclic.*

Solution: Let G be a group of order 15. By Cauchy's theorem there exists a subgroup M of order 5 and a subgroup N of order 3. $[G : M] = \frac{|G|}{|M|} = 3$. Hence there exists a homomorphism from G into the symmetric group on the cosets of M in G. Since $15 \not| \ 3!$ we have a

kernel and since M is cyclic group of order 5, kernel must be M. Hence M is normal in G.

Let g be an element of N of order 3.

$\alpha_g : M \to M$

$$x \longmapsto \alpha_g(x) = g^{-1}xg$$

is an automorphism of M and order of this automorphism divides 3. But M is a cyclic group of order 5, hence the automorphism of M has order $\varphi(5) = 4$ where φ Euler's φ function. So the order of α_g has to divide also 4. Hence α_g has order 1 and becomes the identity automorphism. This implies $g^{-1}xg = x$ for all $x \in M$. i.e. the elements of M and N commute. Since M and N are itself abelian we obtain G is abelian. Now if x is a generator of M and g is a generator of N, then $o(xg) \neq 5, 3$ as

$$\begin{aligned} (xg)^5 &= x^5g^5 = eg^2 = g^2 \neq e. \\ (xg)^3 &= x^3g^3 = x^3 \neq e. \end{aligned}$$

Hence $\langle xg \rangle = G$.

2.49. *Prove that if a group G of order 28 has a normal subgroup of order 4, then G is abelian.*

Solution: Let G be a group of order 28. By Cauchy's Theorem G has a subgroup H of order 7. Let N the given normal subgroup of order 4. Since $\frac{|G|}{|H|} = 4$ We have a homomorphism from a group G into symmetric group on the cosets of H in G. So by isomorphism theorem G/K_ψ is isomorphic to a subgroup of S_4.

If $|K_\psi| = 1$, then by Lagrange theorem $|G| \mid |S_4|$ which is impossible, since $|G| = 28$ and $|S_4| = 24$. Hence $K_\psi \neq \{e\}$ But $K_\psi = \cap_{g \in G} gHg^{-1} \leq H$. The group H is a cyclic group of prime order 7 and $K_\psi \neq \{e\}$ implies $K_\psi = H$. But kernel of a homomorphism is always a normal subgroup. Hence H is normal in G. Now consider $H \cap N$ since this is a subgroup of H and N, so $|H \cap N|$ divides 7 and 4. Hence $H \cap N = \{e\}$. Now for any $h \in H$, $n \in N$, $h^{-1}n^{-1}hn \in H \cap N = \{e\}$. Hence $hn = nh$. Now for any $g \in G$, there exist $h \in H$ and $n \in N$ such

that $g = hn$. let $g_1, g_2 \in G$, so there exists $h_1, h_2 \in H, n_1, n_2 \in N$, $g_1g_2 = (h_1n_1)(h_2n_2) = h_1(n_1h_2)n_2 = h_1(h_2n_1)n_2 = (h_2h_1)(n_2n_1)$ as H is abelian and N is abelian (we use the fact that every group of order 4 is abelian).

so $g_1g_2 = (h_2h_1)(n_2n_1) = h_2(h_1n_2)n_1 = h_2(n_2h_1)n_1 \quad = (h_2n_2)h_1n_1 \quad = g_2g_1$

Hence G is abelian.

2.50. *If $o(G) = p^n$, p a prime number, and $N \neq \{e\}$ is a normal subgroup of G, prove that $N \cap Z(G) \neq 1$ where $Z(G)$ is the center of G.*

Solution: Let G be a group of order p^n. Since every finite $p-$group has a non-trivial center we have $Z(G) \neq \{e\}$.

Now $G/Z(G)$ is again a $p-$group, hence if $G/Z(G)$ is not $\{e\}$, then $G/Z(G)$ has a non-trivial center, say $Z(G/Z(G)) = Z_2(G)/Z(G)$, and continuing like this we have a series of G :

$$G \trianglerighteq Z_k(G) \trianglerighteq Z_{k-1}(G) \cdots \trianglerighteq Z_1(G) = \{e\}$$

here we have

$$[Z_i(G), G] \leq Z_{i-1}(G).$$

Now

$N = N \cap G \trianglerighteq Z_k(G) \cap N \trianglerighteq Z_{k-1}(G) \cap N \triangleright \cdots \trianglerighteq Z_1(G) \cap N = \{e\}$.
There exists i such that $Z_i(G) \cap N = \{e\}$ but $Z_{i+1}(G) \cap N \neq \{e\}$

Now $[G, Z_{i+1}(G) \cap N] \leq Z_i(G) \cap N = \{e\}$. Hence $Z_{i+1}(G) \cap N \leq Z(G)$. So

$$Z_{i+1}(G) \cap N \cap Z(G) \neq \{e\}$$

but $Z(G) \subseteq Z_{i+1}(G)$. This gives $Z_{i+1}(G) \cap N \cap Z(G) = N \cap Z(G) \neq \{e\}$

2.51. *Suppose that $K \lhd G$ with $|G/K| = n < \infty$.*

(i) Show that $g^n \in K$ for every $g \in G$.

(ii) If $g \in G$ and $g^m \in K$ for some integer m such that $(m, n) = 1$, then $g \in K$.

Solution: (i) The group G/K is a finite group of order n. By Lagrange Theorem for any $g \in G$ the order of the subgroup $\langle gK \rangle$ divides the order of the group G/K. i.e $(gK)^n = K$ implies $g^n \in K$.

(ii)Since $(m, n) = 1$, there exist a and b in $\mathbb{Z}$ such that $am+bn = 1$. Then $g = g^{am+bn} = g^{am}g^{bn}$. Then $g^m \in K$ implies $g^{ma} \in K$ and by (i) $g^n \in K$ implies g^{nb} is in K . Hence we get $g = g^{am+bn} \in K$.

2.52. *Let G be a group and Z the center of G. If T is any automorphism of G, prove that $T(Z) \subseteq Z$.*

Solution: Let $w \in Z$ and $g \in G$. There exists $x \in G$ such that $Tx = g$ as T is an automorphism. So

$gT(w) = T(x)T(w) = T(xw) = T(wx) = T(w)T(x) = T(w).g.$

Hence $T(w)$ is in the center of G.

2.53. *If in a finite group G, an element a has exactly two conjugates, prove that G has a normal subgroup $N \neq \{e\}$ and $N \neq G$.*

Solution: For a finite group G and an element $x \in G$ we know that the number of conjugates of x in G is equal to the number of cosets of $C_G(x)$ in G. Since we have only two conjugates $C_G(x)$ has index 2 in G. But any subgroup of index 2 in G is normal (see exercise 2.26. Hence $C_G(x)$ is normal in G. Since $|G : C_G(x)| = 2$ we have $G \neq C_G(x)$. On the other hand $C_G(x) \neq \{e\}$ as $x \neq e$ (otherwise $C_G(x) = G$) and $x \in C_G(x)$.

2.54. *Describe all finite abelian groups of order 2^6.*

Solution: (a) By the structure theorem of finite abelian groups the following list of abelian groups is a complete list of abelian groups of order 2^6. ie. any abelian group of order 2^6 is isomorphic to exactly one group of the following list.

$\mathbf{Z}_{2^6}$

$\mathbf{Z}_{2^5} \times \mathbf{Z}_2$

$\mathbf{Z}_{2^4} \times \mathbf{Z}_{2^2}$

$\mathbf{Z}_{2^4} \times \mathbf{Z}_2 \times \mathbf{Z}_2$
$\mathbf{Z}_{2^3} \times \mathbf{Z}_{2^3}$
$\mathbf{Z}_{2^3} \times \mathbf{Z}_{2^2} \times \mathbf{Z}_2$
$\mathbf{Z}_{2^3} \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$
$\mathbf{Z}_{2^2} \times \mathbf{Z}_{2^2} \times \mathbf{Z}_{2^2}$
$\mathbf{Z}_{2^2} \times \mathbf{Z}_{2^2} \times \mathbf{Z}_2 \times \mathbf{Z}_2$
$\mathbf{Z}_{2^2} \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$
$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$

2.55. *Let G be a group, $K_1, K_2, \cdots, K_n$ normal subgroups of G. Suppose that $K_1 \cap K_2 \cap \cdots \cap K_n = \{e\}$. Let $V_i = G/K_i$. Prove that there is a monomorphism of G into $V_1 \times \cdots \times V_n$.*

Solution: Define a map $\psi : G \to V_1 \times V_2 \times \cdots \times V_n, \quad g \to (gK_1, gK_2, \cdots, gK_n)$, clearly ψ is a homomorphism.

Kernel of ψ is $K_\psi = \{\ g \in G \mid gK_i = K_i \text{ for all } i\ \} = \{g \in G \mid g \in K_i \text{ for all } i\} = \cap_{i=1}^n K_i = \{e\}$

Hence ψ is one to one.

2.56. *Show how to get all abelian groups of order $2^3 3^2 5$.*

Solution:
$\mathbf{Z}_{2^3} \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5$
$\mathbf{Z}_{2^2} \times \mathbf{Z}_2 \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5$
$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5$
$\mathbf{Z}_{2^3} \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$
$\mathbf{Z}_{2^2} \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$
$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_5$

2.57. *List all the conjugate classes in S_3 and verify the class equation.*

Solution: Conjugacy class of (1) is $[1] = \{(1)\}$
Conjugacy class of (1,2) is $[(1,2)] = \{(1,2), (1,3), (2,3)\}$

Conjugacy class of $(1,2,3)$ is $[(1,2,3)] = \{(1,2,3), (1,3,2)\}$. Class equation:

$|G| = \sum_{x\in A} |G : C_G(x)| = \sum_{x\in A} |[x]|$ where A is a complete set of representatives of all conjugacy classes of G.

$6 = 1 + 3 + 2$

2.58. *Let G be a finite abelian group. Prove that G is isomorphic to the direct product of its Sylow subgroups.*

Solution: Let G be a finite abelian group of order m. Let $m = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ be the prime factorization of m.

By Sylow's Theorem we know that G has subgroups S_i of order $p_i^{n_i}, i = 1, 2, \ldots, k$.

Since G is abelian, every subgroup is normal, in particular every Sylow subgroup is normal. So $S_1 \cdots S_{i-1} S_{i+1} \cdots S_k$ is a subgroup of G and

$$S_i \cap S_1 \cdots S_{i-1} S_{i+1} \cdots S_k = \{e\}$$

Since every element in $S_1 \cdots S_{i-1} S_{i+1} \cdots S_k$ is of order a power of the primes $p_1, \cdots, p_{i-1}, p_{i+1} \cdots, p_k$ and every element of S_i is of order a power of the prime p_i. Hence

$$|S_1 S_2 \cdots S_k| = p_1^{n_1} \cdots p_k^{n_k} = |G|.$$

and hence $G = S_1 \cdots S_k$. The property $S_i \cap S_1 \cdots S_{i-1} S_{i+1} \cdots S_k = \{e\}$ implies that G is a direct product of its Sylow subgroups.

2.59. *Let G be a group and let $T = G \times G$*
a) Show that $D = \{(g, g) \in G \times G \mid g \in G\}$ is isomorphic to G.
b) Prove that D is normal in T if and only if G is abelian.

Solution: Define a map $\psi : G \to D$, by $g \to (g, g)$.
Clearly ψ is well defined.

$$\begin{aligned} \psi(xy) = (xy, xy) &= (x, x)(y, y) \\ &= \psi(x)\psi(y) \end{aligned}$$

$K_\psi = \{g \in G \mid (g, g) = (e, e)\} = \{e\}$. So ψ is a monomorphism. Moreover for any $(g, g) \in D$ there exists $g \in G$ such that $\psi(g) = (g, g)$.

Hence ψ is an isomorphism between G and D.

(b) Assume that D is normal in T. Then for any $(x, y) \in T$ and any $(g, g) \in D$,

$(x^{-1}gx, y^{-1}gy) = (u, u)$ i.e. $\left\{ \begin{array}{ll} x^{-1}gx & = u \\ y^{-1}gy & = u \end{array} \right\}$. This implies $x^{-1}gx = y^{-1}gy$ then $yx^{-1}g = gyx^{-1}$ for all $y \in G$ i.e. $yx^{-1} \in Z(G)$.

This is true for all $(x, y) \in T$. Choose $x = e$, hence $y \in Z(G)$ for all $g \in G$. This implies G is abelian. Converse is clear.

2.60. *Give an example of a finite non-abelian group G which contains a subgroup $H_0 \neq \{e\}$ such that $H_0 \subseteq H$ for all subgroups $H \neq \{e\}$ of G.*

Solution: Let $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ with multiplication $i^2 = j^2 = k^2 = ijk = -1$ $\begin{array}{lll} \text{ij} = \text{k}, & \text{ik} = \text{-ki} = \text{-j} \\ \text{ji} = \text{-k}, & \text{jk} = \text{i}, & \text{kj} = \text{-i} \end{array}$

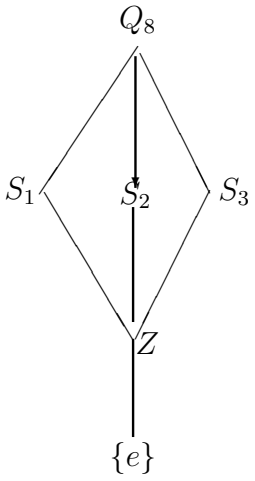
$Z = \{1, -1\} = H_0$ is a subgroup of Q_8 and Z is contained in every subgroup $H_0 \neq \{e\}$ of Q_8.

Indeed if $\{e\} \neq H$ is any subgroup of Q_8, then H contains at least one of the elements $\{-1, \pm i, \pm j, \pm k\}$ if it contains -1 then certainly it contains Z. If it contains one of $\pm i, \pm j, \pm k$, then $i^2 = j^2 = k^2 = -1 \in H$. Hence $H \supseteq Z$.

Subgroups of Q_8 are

$$\begin{array}{rcl} Q_8 & & \\ S_1 & = & \{1, -1, i, -i\} \\ S_2 & = & \{1, -1, j, -j\} \\ S_3 & = & \{1, -1, k, -k\} \\ Z & = & \{1, -1\} \\ \{1\} & & \end{array}$$

Hence the Hasse diagram is



Observe that if H_0 contains two of the elements of $\{i, j, k\}$ then it generates Q_8.

2.61. *Show that every group of order p^2 where p a prime is either cyclic or is isomorphic to the direct product of two cyclic groups each of order p.*

Solution: Let G be a group of order p^2 ($p-$prime). We already know that $Z(G) \neq \{e\}$. If there exists an element $e \neq g \in Z(G)$ such that $o(g) = p^2$, then G is a cyclic group and isomorphic to $\mathbf{Z}_{p^2}$.

So assume that every element in $Z(G)$ is of order p. Then $Z(G) \cong \mathbf{Z}_p$ or $Z(G) \cong \mathbf{Z}_p \times \mathbf{Z}_p$.In the first case, $|Z(G)| = p$, and $|G/Z(G)| = p$ and so $G/Z(G)$ is a cyclic group. This implies G is an abelian group by 2.41. i.e. $Z(G) = G$, which contradicts with $|Z(G)| = p$. In the second case $G = Z(G)$ and G is abelian and $G \cong Z_p \times \mathbf{Z}_p$.

2.62. *Let p, q be primes, $p > q$ and G a group of order $p.q$. Prove:*
a) G has a subgroup of order p and a subgroup of order q.
b) If q does not divide $p - 1$, then G is cyclic.
c) If $q|p - 1$, there exists a non-abelian group of order pq.

Solution: a) By Cauchy's theorem every finite group G has an element of order p for every prime divisor of $|G|$. Let x and y be elements of G of orders p and q respectively. Then $\langle x \rangle$ and $\langle y \rangle$ are subgroups we are looking for.

b) Since $p > q$, the subgroup $P = \langle x \rangle$ has q cosets in G. There exists a homomorphism $\psi : G \to S_q$, from G into the symmetric group on the set of right cosets of P in G with kernel $K_\psi = \cap_{x \in G} xPx^{-1}$. By isomorphism theorem G/K_ψ is isomorphic to a subgroup of S_q. But $|S_q| = q!$. Hence K_ψ can not be identity (otherwise $pq|q!$ and $q < p$). Hence $K_\psi = P$ i.e. P is a normal subgroup of G.

Let Q be the subgroup of G of order q and generated by $\langle y \rangle$. Define a map α_y from P to P such that $\alpha_y : P \to P, \qquad x \to y^{-1}xy$. This homomorphism is one to one and onto, hence an automorphism of P.

Since P is a group of prime order p where $|Aut(P)| = p - 1$ and α_y is an automorphism either of order 1 or of order q as $|\langle y \rangle| = q$. But then $q|p - 1$, which is impossible. Hence α_y is the identity automorphism. This implies $xy = yx$. (see exercise 2.10) Hence $\langle x, y \rangle$ is abelian. But both $p = |x|$ and $q = |y|$ divide $|\langle x, y \rangle|$ and therefore $|\langle x, y \rangle| = |G| = pq$, ie. $\langle x, y \rangle = G$.

(c) $\mathbf{Z}_p^\star$ is a group of order $p - 1$. Since q is a prime dividing $|\mathbf{Z}_p^\star|$, by Cauchy's theorem $\mathbf{Z}_p^\star$ contains a subgroup X of order q.

Let $G = \left\{ \begin{bmatrix} x & 0 \\ z & 1 \end{bmatrix} \mid x \in X, \ z \in \mathbf{Z}_p \right\}$ is a subset of the group of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc \neq 0$ over $\mathbf{Z}_p$. The set G contains exactly $|X| \cdot |\mathbf{Z}_p| = pq$ elements. On the other hand

$$\begin{bmatrix} x_1 & 0 \\ z_1 & 1 \end{bmatrix} \begin{bmatrix} x_2 & 0 \\ z_2 & 1 \end{bmatrix} = \begin{bmatrix} x_1x_2 & 0 \\ z_1x_2 + z_2 & 1 \end{bmatrix}$$

i.e. G is closed with respect to multiplication of matrices since X is a subgroup of $\mathbf{Z}_p^\star$ with respect to multiplication.

Clearly G is a *non-abelian* group of order pq.

2.63. *(a) If G is a finite abelian group with elements $a_1, a_2, \cdots, a_n$ prove that $a_1a_2 \cdots a_n$ is an element whose square is the identity.*

(b) If the G in part (a) has no element of order 2 or more than one element of order 2, prove that $a_1a_2 \cdots a_n = e$.

(c) If G has one element, y, of order 2, prove that $a_1a_2 \cdots a_n = y$.

(d) (Wilson's theorem) If p is a prime number show that $(p-1)! \equiv -1 \pmod{p}$.

Solution: (a) Let G be an abelian group with elements $a_1, a_2, \cdots, a_n$. For every a_i of order greater than 2, $a_i \neq a_i^{-1}$ and so a_i^{-1} appears in the product, therefore only the elements of order 2 remains in the product $a_1 \cdots a_n$. But their square is identity since G is abelian and square of every element of order 2 is identity.

(b) By (a) if G has no element of order 2, then inverse of every element appears in the product, hence the product of the elements in G is identity.

Assume that G has more than one element of order 2. Since the elements of order different from 2 cancels we may assume that G is a 2-group say $x_1, x_2, \cdots, x_{2^m}$ are elements of order 2 where $m \geq 2$.

We prove this by induction on m.

If $m = 2$, then $1, x_1, x_2 \ x_1x_2$ are the elements of the group $\langle x_1, x_2 \rangle$. Hence $x_1x_2 \cdot x_1x_2 = 1$.

Assume that the statement is true for $m-1$ and let $G = \{x_1, \cdots, x_{2^m}\}$ The group G is abelian and every element is of order 2.

Let $H = \{x_1, x_2, \cdots, x_{2^{m-1}}\}$. Let $\{x_1, \ldots, x_m\}$ be the generators of $G = \langle x_1, \cdots, x_m \rangle$

If $x_1x_2x_3 \cdots x_i$ in H, then the new elements are $x_1x_2 \cdots x_ix_m$. Hence in the product of elements of G we have

$\prod_{g \in G} g = 1 \cdot 1(x_m)^{2^{m-1}} = 1.$

We have the product of the elements in H and the product of the elements in H times x_m. Since G is abelian x_m appears 2^{m-1} times. Hence we have the result.

c) If G has one element y of order 2, then by the above explanations $a_1 \cdots a_n = y$

d) $\mathbf{Z}_p$ with multiplication forms a cyclic group of order $p-1$. Hence $\mathbf{Z}_p$ is abelian and the product of the elements is $1.2 \cdots (p-1) = (p-1)!$

Since $\mathbf{Z}_p$ is a cyclic group, it has only one element of order 2, hence the product of the elements is the only element of order 2. But the element of order 2 is -1 (mod p). Hence

$(p-1)! \equiv -1 \ (\mod p)$

2.64. *If p is an odd prime and if*

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}=\frac{a}{b},$$

where a and b are integers, prove that $p|a$. If $p>3$, prove that $p^2|a$.

Solution: Let p be an odd prime.

$$1+\frac{1}{2}+\cdots+\frac{1}{p-1}=\frac{a}{b}$$

For $p=3$, $1+\frac{1}{2}=\frac{a}{b}$. Then $\frac{3}{2}=\frac{a}{b}\quad 2a=3b$. Hence $3\,|a$. Now assume that $p>3$, then write the equation in the form

$$(1+\frac{1}{p-1})+(\frac{1}{2}+\frac{1}{p-2})+\cdots+(\frac{1}{(\frac{p-1}{2})}+\frac{1}{(\frac{p+1}{2})})$$
$$=\frac{p}{1(p-1)}+\frac{p}{2(p-2)}+\cdots+\frac{p}{(\frac{p-1}{2})^2})$$

as $p-(\frac{p-1}{2})=\frac{p+1}{2}\equiv-(\frac{p-1}{2})\ (\mod p)$. Then the above equality is equal to

$=-p(1+2^2+3^2+\cdots+(\frac{p-1}{2})^2)$ when it is considered in the multiplicative group $\mathbf{Z}_p^*$

For the above equality we consider $\mathbf{Z}_p^*$ as a cyclic group with respect to multiplication with $p-1$ elements. The square of the elements forms a subgroup of $\mathbf{Z}_p$ with respect to multiplication and so inverse of every element is again contained in this subgroup and inverse of each element is unique and appears in the above sum only once Hence the above sum

$$1+2^2+\cdots+(\frac{p-1}{2})^2=\frac{(\frac{p-1}{2})(\frac{p+1}{2})(p)}{6}$$

since $p>3$, and p is a prime and $(p,6)=1$.

Hence the sum becomes $-p^2(\frac{p-1}{2})(\frac{p+1}{2})=\frac{a}{b}$. Then $-p^2\frac{(p^2-1)}{4}=\frac{a}{b}$ and $-p^2(p^2-1)b=4a$. Now we observe that $p^2|a$.

2.65. *Prove that the non-zero integers* $\mod p$ *under multiplication form a cyclic group if p is a prime.*

Solution: The non-zero integers modulo p forms a field and the multiplicative group of a finite field is cyclic.

2.66. *Give an example of a non-abelian group in which $(xy)^3=x^3y^3$ for all x and y.*

Compare this question with question 2.17.

Solution: Let $G = \{ \begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & z & 1 \end{bmatrix} \Big| x, y, z \in \mathbf{Z}_3 \}$

$$\begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & z & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & z & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 2x & 1 & 0 \\ 2y + zx & 2z & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 2x & 1 & 0 \\ 2y + zx & 2z & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & z & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Hence every element of G is of order 3. But

$$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix}$$

Hence G is not abelian.
It is clear that $|G| = 27$

2.67. *If G is a finite abelian group, prove that the number of solutions of $x^n = e$ in G, where $n|o(G)$ is a multiple of n.*

Solution: Let G be a finite abelian group. The set S of solutions of the equation $x^n = e$ in G forms a subgroup of G. Indeed, let g, h be two elements from S. Then $g^n = e$ and $h^n = e$. We obtain $(gh)^n = g^n h^n = e$ and $(g^{-1})^n = (g^n)^{-1} = e$.

Since G is abelian and $n|o(G)$ so G has a subgroup H of order n. Then every element in H is a solution for $x^n = e$. Hence H is a subgroup of S, then by Lagrange Theorem $|H|$ divides $|S|$. i.e. n divides the number of solutions in G of $x^n = e$.

A group G is said to be **soluble** if there is a finite sequence $H_0, H_1, \cdots, H_n$ of subgroups of G such that $H_i < H_{i+1}$ and H_i is a normal subgroup of H_{i+1} with $H_0 = \{e\}$ and $H_n = \{G\}$, and all factor groups H_{i+1}/H_i are abelian.

2.68. *Prove that a subgroup of a soluble group and the homomorphic image of a soluble group must be soluble.*

Solution: Let G be a soluble group and K be a subgroup of G. Since G is soluble there exists subgroup $H_0 \leq H_1 \leq \cdots \leq H_n = G$ such that H_i is normal in H_{i+1} and H_{i+1}/H_i is abelian.

Now take the intersection of K with H_i we obtain

$$\{e\} = H_0 \cap K \leq H_1 \cap K \leq \ldots \leq H_n \cap K = K$$

since H_i is normal in H_{i+1} we have $H_i \cap K$ is normal in $H_{i+1} \cap K$. In order to say K is soluble it is enough to show

$(H_{i+1} \cap K)/(H_i \cap K)$ is abelian. But

$$(H_{i+1} \cap K)/(H_i \cap K) \cong (H_{i+1} \cap K)H_i/H_i \leq H_{i+1}/H_i$$

Since H_{i+1}/H_i is abelian subgroup of an abelian group is abelian. Hence by the isomorphism theorem $(H_{i+1} \cap K)/(H_i \cap K)$ is abelian.

For the second part of the question, let M be a homomorphic image of G and let N be the kernel of the homomorphism ψ from G onto M. Hence by isomorphism theorem $G/N \cong M$. We show G/N is soluble.

Let $H_0 = \{e\} \leq H_1 < \cdots < H_n = G$ be the subgroups of G such that H_i is normal in H_{i+1} and H_{i+1}/H_i is abelian, $1 = 1, 2, \ldots, n-1$.

Now consider $H_0N = \{N\} \leq H_1N/N \leq H_2N/N \leq \cdots \leq H_nN/N = G/N$

Since H_i is normal in H_{i+1} we have H_iN/N normal in $H_{i+1}N/N$. Indeed if $gN \in H_{i+1}N/N$, then

$(gN)^{-1}(H_iN/N)gN = g^{-1}N(H_iN/N)gN = H_iN/N$ as $g^{-1}H_ig = H_i$ for all $g \in H_{i+1}$.

Moreover $(H_{i+1}N/N)/(H_iN/N) \cong H_{i+1}N/H_iN = H_{i+1}H_iN/H_iN$

$\cong H_{i+1}/(H_{i+1} \cap H_iN) \cong H_{i+1}/H_i(H_{i+1} \cap N)$

Since H_{i+1}/H_i is abelian and homomorphic image of an abelian group is abelian question 2.34 we get $H_{i+1}/H_i(H_{i+1} \cap N)$ is abelian. Hence the group G/N is soluble.

2.69. *If G is a group and N is a normal subgroup of G such that both N and G/N are soluble, prove that G is soluble.*

Solution: Let N be a normal subgroup of G. Since G/N is soluble there exist subgroups $N = H_0 < H_1/N < \cdots H_n/N = G/N$ such that $H_i/N \lhd H_{i+1}/N$. (i.e. $H_i \lhd H_{i+1}$) and $(H_{i+1}/N)/(H_i/N) \cong H_{i+1}/H_i$ is abelian.

Since N is soluble, there exist $T_0 = \{e\} \lhd T_1 \lhd \cdots \lhd T_k = N$ such that T_{j+1}/T_j is abelian. Now

$\{e\} = T_0 \lhd \cdots \lhd T_k = N = H_0 \lhd \cdots \lhd H_n = G$ are subgroups of G such that each subgroup is normal in the next one and the quotient group is abelian. Hence G is soluble.

2.70. *If G is a group, A a subgroup of G and N a normal subgroup of G, prove that if both A and N are soluble, then so is AN.*

Solution: Since $N \lhd G$, AN is a subgroup of G and $N \lhd AN$. Now $AN/N \cong A/(A \cap N)$. Since A is soluble, by question 2.68 homomorphic image $A/(A \cap N)$ is also soluble. Now by question 2.69 we obtain AN is soluble.

2.71. *If G is a group, define the sequence of subgroups $G^{(i)}$ of G by*

(1) $G^{(1)}$ = commutator subgroup of G which is a subgroup of G generated by all $aba^{-1}b^{-1}$ where $a, b \in G$.

(2) $G^{(i)}$ = commutator subgroup of $G^{(i-1)}$ if $i > 1$.

Prove

(a) Each $G^{(i)}$ is a normal subgroup of G.

b) Let $H \trianglelefteq G$. Then $G^{(1)} \leq H$ if and only if G/H is abelian. ($G/G^{(1)}$ is the largest abelian factor group of G.)

(c) G is soluble if and only if $G^{(k)} = \{e\}$ for some $k \geq 1$.

Solution: (a) We prove this by induction on i.

For $i = 1$

$$G^{(1)} = \langle\ g^{-1}h^{-1}gh \mid g, h \in G\ \rangle$$

Let x be an element of G, and $g^{-1}h^{-1}gh$ be an arbitrary generator of $G^{(1)}$. Then

$$\begin{aligned} x^{-1}g^{-1}h^{-1}ghx &= x^{-1}g^{-1}xx^{-1}h^{-1}xx^{-1}gxx^{-1}hx \\ &= (g^{-1})^x(h^{-1})^x g^x h^x \in G^{(1)} \end{aligned}$$

Since x normalizes an arbitrary generator of $G^{(1)}$, the element x normalizes every element of $G^{(1)}$. Hence $G^{(1)} \trianglelefteq G$.

Now assume that $G^{(i-1)} \trianglelefteq G$ and let

$g^{-1}h^{-1}gh$ be an arbitrary generator of $G^{(i)}$ and let x be an arbitrary element of G. Then

$x^{-1}g^{-1}h^{-1}ghx = (g^{-1})^x(h^{-1})^x g^x h^x$ since g and $h \in G^{(i-1)}$ and $G^{i-1} \trianglelefteq G$ we have g^x and $h^x \in G^{(i-1)}$ hence $(g^{-1})^x(h^{-1})^x g^x h^x \in G^{(i)}$ and $G^{(i)} \trianglelefteq G$.

(b) Assume that $G^{(1)} \leq H$. Then for any $xH, yH \in G/H$ we have $x^{-1}y^{-1}xyH = H$ as every generator of $G^{(1)}$ is an element of H. It follows that $xyH = yxH$. i.e The group G/H is abelian.

Conversely assume that G/H is abelian. Then for any $xH, yH \in G/H$ we have $xyH = yxH$. It follows that $x^{-1}y^{-1}xyH = H$. Hence every generator of $G^{(1)}$ is in H. Hence $G^{(1)} \leq H$.

(c) Assume that G is soluble, then there exists subgroups $H_0 = \{e\} \lhd H_1 \lhd \cdots \lhd H_n = G$ such that H_{i+1}/H_i is abelian. Hence $H_{n-1} \geq G^{(1)}$ as $g^{-1}h^{-1}gh \in H_{n-1}$. Continuing like this we get $G^{(i)} \leq H_{n-i}$, in particular $G^{(n)} \leq H_0 = \{e\}$.

Conversely assume that $G^{(k)} = \{e\}$ for some $k \geq 1$. By (a) each $G^{(i)}$ is normal in G, in particular each $G^{(i+1)} \lhd G^{(i)}$ and observe that $G^{(i)}/G^{(i+1)}$ is abelian for all i. Hence G is soluble.

2.72. *Prove that a soluble group $G \neq \{e\}$ always has an abelian normal subgroup $M \neq \{e\}$.*

Solution: Let $G \neq \{e\}$ be a soluble group. Then by question 2.71 we have $G^{(k)} = \{e\}$ for some k. Let k be the least integer satisfying $G^{(k)} = \{e\}$. Hence $G^{(k-1)} \neq \{e\}$. Here if $h^k = 1$, $G^{(0)} = G$ By question

2.71, $G^{(k-1)}$ is a normal subgroup of G and moreover it is abelian as for any $g, h \in G^{(k-1)}$ we have $g^{-1}h^{-1}gh \in G^{(k)} = \{e\}$. Hence $g^{-1}h^{-1}gh = e$ implies $gh = hg$. i.e. $G^{(k-1)}$ is the required group.

If G is a group, define the sequence of subgroups $\gamma_i(G)$ by

(a) $\gamma_1(G) = G'$ commutator subgroup of G.

(b) $\gamma_i(G)$ = subgroup of G generated by all $aba^{-1}b^{-1}$ where $a \in G$, $b \in \gamma_{i-1}(G)$.

G is said to be **nilpotent** if $\gamma_k(G) = \{e\}$ for some $k \geq 1$.

2.73. *(a) Show that each $\gamma_i(G)$ is a normal subgroup of G and $\gamma_i(G) \geq G^{(i)}$.*

(b) If G is nilpotent, prove it must be soluble.

(c) Give an example of a group which is soluble but not nilpotent.

Solution: We prove this by induction on i.

For $i = 1, \gamma_1(G)$ is the commutator subgroup of G and we showed in 2.71 that commutator subgroup is normal.

Now assume that $\gamma_{i-1}(G)$ is normal in G.

Let $h \in \gamma_{i-1}(G)$ and $x, g \in G$, then a generator of $\gamma_i(G)$ is of the form $h^{-1}g^{-1}hg$. So for any $x \in G$, $x^{-1}h^{-1}g^{-1}hgx = (h^{-1})^x(g^{-1})^x h^x g^x$

Since $\gamma_{i-1}(G) \lhd G$ and $h \in \gamma_{i-1}(G)$ we have $(h^{-1})^x \in \gamma_{i-1}(G)$ and $g^x \in G$, hence $(h^{-1})^x(g^{-1})^x h^x g^x \in \gamma_i(G)$ and therefore $\gamma_i(G) \lhd G$.

$G^{(i)} \lhd \gamma_i(G)$ as every generator of $G^{(i)}$ is contained in $\gamma_i(G)$. by induction on i.

(b) Let's assume that G is nilpotent. Hence there exists $k \geq 1$ such that $\gamma_k(G) = \{e\}$. But then $G^{(k)} \leq \gamma_k(G) = \{e\}$. Hence $G^{(k)} = \{e\}$. Now by question 2.71 (b) G is soluble.

(c) $G = S_3$ is soluble as $G^{(1)} = A_3$ and $G^{(2)} = \{e\}$. G is not nilpotent as $Z(G) = \{e\}$.

2.74. *Show that any subgroup and homomorphic image of a nilpotent group must be nilpotent.*

Solution:) Let G be a nilpotent group and H be a subgroup of G. Then $\gamma_1(H) \leq \gamma_1(G)$ and $\gamma_2(H) \leq \gamma_2(G)$ and so on. Then by induction

k we have $\gamma_k(H) \leq \gamma_k(G) = \{e\}$. Hence H is nilpotent.

Now let G be nilpotent and N be a normal subgroup of G. Then $\gamma_1(G/N) = \gamma_1(G)N/N$ and $\gamma_2(G/N) = \gamma_2(G)N/N$ and by induction we observe that $\gamma_i(G/N) = \gamma_i(G)N/N$.

Since $\gamma_k(G) = \{e\}$ we get $\gamma_k(G) = \{e\}$. Hence G/N is nilpotent.

2.75. *Show that every homomorphic image, different from* $\{e\}$*, of a nilpotent group has a nontrivial center.*

Solution: Let G be a nilpotent group. We show that G has a nontrivial center, whenever $G \neq \{e\}$. This will be enough for the question because by question 2.74 every homomorphic image of a nilpotent group is nilpotent.

Let G be nilpotent and k be the smallest positive integer such that $\gamma_k(G) = \{e\}$. Then $\gamma_{k-1}(G) \neq \{e\}$ and for any $z \in \gamma_{k-1}(G)$ and $g \in G$. $z^{-1}g^{-1}zg \in \gamma_k(G) = \{e\}$. Hence $z^{-1}g^{-1}zg = e$ i.e. $z \in Z(G)$. Therefore $\{e\} \neq \gamma_{k-1}(G) \leq Z(G)$.

2.76. *(a) Show that any group of order* p^n, p *a prime, must be nilpotent.*
(b) If G *is nilpotent, and* $H \neq G$ *is a subgroup of* G*, prove that* $N_G(H) \neq H$ *where* $N_G(H) = \{x \in G \mid xHx^{-1} = H\}$.

Solution: (a) We first show that if $G/Z(G)$ is nilpotent, then G is nilpotent.
To prove this, $\gamma_1(G/Z(G)) = \gamma_1(G)Z(G)/Z(G)$ $\gamma_2(G/Z(G)) = \gamma_2(G)Z(G)/Z(G)$ and by induction $\gamma_k(G/Z(G)) = \gamma_k(G)Z(G)/Z(G)$.

Since $G/Z(G)$ is nilpotent, there exists $k \geq 1$ such that $\gamma_k(G/Z(G)) = \{e\}$ i.e.

$\gamma_k(G)Z(G)/Z(G) = Z(G)$. Hence $\gamma_k(G) \leq Z(G)$.

Therefore $\gamma_{k+1}(G) = \{e\}$. Hence G is nilpotent.

Now for the solution of the question for a p-group G, we know that $Z(G) \neq \{e\}$. We make induction on the order of G.

Assume that all p-groups of order $< p^n$ are nilpotent and let $|G| = p^n$. Since G is a p-group we have $Z(G) \neq \{e\}$. Hence $|G/Z(G)| < |G|$ and so $G/Z(G)$ nilpotent, then by the above proof G is nilpotent.

(b) Let G be a nilpotent group and $H \neq G$ be a subgroup of G. By question 2.75 $Z(G) \neq \{e\}$. In fact we have a central series

$G = \gamma_0(G) \rhd \gamma_1(G) \rhd \gamma_2(G) \rhd \cdots \rhd \gamma_k(G) = \{e\}$

Let i be the smallest integer such that $\gamma_{i+1}(G) < H$ but $\gamma_i(G) \not\leq H$. Then

$$[\gamma_i(G), H] \leq [\gamma_i(G), G] \leq \gamma_{i+1}(G) \leq H.$$

Hence $\gamma_i(G)$ is contained in the normalizer of H. But $\gamma_i(G) \not\leq H$ implies $N_G(H) \neq H$

2.77. *(a) If G is a finite group and if P is a p-Sylow subgroup of G, prove that P is the only p-Sylow subgroup in $N_G(P)$.*

(b) If P is a p-Sylow subgroup of G and if $a^{p^k} = e$ then, if $a \in N(P), a$ must be in P.

(c) Prove that $N_G(N_G(P)) = N_G(P)$.

Solution: (a) Let P and Q be two Sylow p-subgroups of G contained in $N(P)$. Then they are two Sylow p-subgroups of $N_G(P)$. So they are conjugate in $N_G(P)$ i.e. there exists an element $x \in N_G(P)$ such that $P^x = Q$. But $x \in N_G(P)$ implies $P^x = P = Q$.

(b) Since $a^{p^k} = e$, the element a is a p-element hence it is contained in a Sylow p-subgroup because every p-element is contained in a Sylow p-subgroup. But it is given that $a \in N(P)$, now by (a) there is only one Sylow p-subgroup in $N(P)$ namely P. Hence a must be in P.

(c) It is clear that $N_G(P) \leq N_G(N_G(P))$. Now let $g \in N_G(N_G(P))$. Then $P^g \leq N_G(P^g) = g^{-1}N_G(P)g = N_G(P)$. So P and P^g are Sylow p-subgroups of $N_G(P)$. Hence they are equal by (a), i.e. $P = P^g$ and $g \in N_G(P)$. This implies $N_G(N_G(P)) \leq N_G(P)$ and so we have the equality.

2.78. *If G is a finite group, prove that G is nilpotent if and only if G is the direct product of its Sylow subgroups.*

Solution: Let G be a nilpotent group and let P be a Sylow p-subgroup of G. Then by question 2.76 (b) $P < N_G(P)$. Now consider $N_G(P)$. By question 2.77 (c) we have $N_G(N_G(P)) = N_G(P)$. Now question 2.76 implies that $N_G(P) = G$. i.e. P is a normal subgroup of G.

Let $P_1, P_2, \cdots, P_n$ be the Sylow p_i-subgroups of G, each normal in G. It is clear that $G = P_1P_2 \cdots P_n$ and for any $i \neq j$ $P_i \cap P_j = \{e\}$. Hence the elements of P_i and P_j commute for all $i \neq j$.

Now let $x \in P_i \cap P_1 \cdots P_{i-1}P_{i+1} \cdots P_n$. Then x is a p_i-element, and $x = y_1y_2 \ldots y_{i-1}y_{i+1} \ldots y_n$ where y_j is a p_j element of G, for all $i \neq j$, and $j = 1 \cdots n$. Let m be the least common multiple of the orders of y_i's and $x^{p_i^t} = e$. Then $(m, p_i^t) = 1$ and so we have $l, s \in \mathbf{Z}$ such that $ml + p_i^t s = 1$. Now

$x = x^{ml+p_i^t s} = x^{ml}(x^{p_i^t})s = x^{ml}$. Hence $x = x^{ml} = (y_1y_2 \cdots y_iy_{i+1} \cdots y_n)^{ml}$
$= y_1^{ml} \cdots y_{i-1}^{ml} y_{i+1}^{ml} \cdots y_n^{ml} = e$

Conversely assume that G is a direct product of its Sylow p-subgroups. By question 2.76 (a) each Sylow p-subgroup is nilpotent. Now it is enough to show that direct product of two nilpotent group is nilpotent.

Let N and M be nilpotent groups and $G = N \times M$. Then $\gamma_1(G) = \gamma_1(N) \times \gamma_1(M)$, $\gamma_2(G) = \gamma_2(N) \times \gamma_2(M)$ and so on. If $\gamma_k(N) = \{e\}$ and $\gamma_l(M) = \{e\}$ and $k \geq l$, then $\gamma_k(G) = \gamma_k(N) \times \gamma_k(M) = \{e\}$. Hence G is nilpotent.

2.79. *Let G be a finite group and H a subgroup of G. For A, B subgroups of G, define A to be conjugate to B relative to H if $B = x^{-1}Ax$ for some $x \in H$. Prove*

(a) This defines an equivalence relation on the set of subgroups of G.

(b) The number of subgroups of G conjugate to A relative to H equals the index of $N_G(A) \cap H$ in H.

Solution: a) (i) $A \sim A$ since $e \in H$ and $A = eAe$

(ii) $A \sim B$, then there exists $x \in H$ such that $B = x^{-1}Ax$. Therefore $xBx^{-1} = A$. i.e. $B \sim A$. This is because $x^{-1} \in H$ as H is a subgroup and $x \in H$.

(iii) $A \sim B$ and $B \sim C$, then there exists $x, y \in H$ such that $B = x^{-1}Ax$ and $C = y^{-1}By$. We have $C = y^{-1}x^{-1}Axy = (xy)^{-1}Axy$. Since H is a subgroup, $xy \in H$ and we obtain $A \sim C$.

(b) Let Ω be the set of right cosets of $N_G(A) \cap H$ in H and Y be the set of subgroups of G conjugate to A relative to H. Define a map $\alpha : \Omega \to Y$ such that $\alpha(N_G(A) \cap H)h = h^{-1}Ah$. The map α is one to one and onto. Indeed if $\alpha((N_G(A) \cap H)h) = \alpha((N_G(A) \cap H)v)$, then $h^{-1}Ah = v^{-1}Av$, multiplying from left by h and from right by h^{-1} we obtain $hv^{-1}Avh^{-1} = A$. i.e. $vh^{-1} \in N_G(A)$. Since $v, h \in H$ we have $vh^{-1} \in H$ and hence $vh^{-1} \in N_G(A) \cap H$. i.e. $(H_G(A) \cap H)v = (N_G(A) \cap H)h$. Clearly α is onto.

2.80. *Show that a group cannot be written as the set-theoretic union of two proper subgroups.*

Solution: Let $G = HUK$ and assume that $H \not\subseteq K$ and $K \not\subseteq H$. Let $h \in H \setminus K$ and $k \in K \setminus H$. G is a group, implies that $hk \in G$. So either $hk \in H$ or $hk \in K$. If $hk \in H$, then $k \in H$ which is not the case. If $hk \in K$, then $h \in K$ which is not the case. Hence one should have either $H \subseteq K$ or $K \subseteq H$.

2.81. *Suppose G is the group defined by the following Cayley table*

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
2	*2*	*1*	*8*	*7*	*6*	*5*	*4*	*3*
3	*3*	*4*	*5*	*6*	*7*	*8*	*1*	*2*
4	*4*	*3*	*2*	*1*	*8*	*7*	*6*	*5*
5	*5*	*6*	*7*	*8*	*1*	*2*	*3*	*4*
6	*6*	*5*	*4*	*3*	*2*	*1*	*8*	*7*
7	*7*	*8*	*1*	*2*	*3*	*4*	*5*	*6*
8	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*

(a) Find the centralizer of 5 in G.
(b) Find the centralizer of 3 in G.
(c) Find center of G.
(d) Find the order of each element of G.
(e) Is the above group abelian?
(f) Find a proper normal subgroup of G and verify why it is normal.

Solution: (a) $C_G(5) = \{1, 2, 3, 4, 5, 6, 7, 8\}$. This shows that $5 \in Z(G)$.

(b) $C_G(3) = \{1, 3, 5, 7\}$.

(c) Since $Z(G) \leq C_G(3)$ we need only to check that 7 is in the center or not. But 7 does not commute with 2. Then we have $Z(G) = \{1, 5\}$.

(d) $o(1) = 1 \quad o(2) = 2 \quad o(3) = 4 \quad o(4) = 2 \quad o(5) = 2 \quad o(6) = 1 \quad o(7) = 4 \quad o(8) = 2$.

(e) No, since $Z(G) = \{1, 5\}$.

(f) $C_G(3) = \{1, 3, 5, 7\}$ is a normal subgroup of G, since $|G| = 8$, and $|C_G(3)| = 4$. Hence $|G : C_G(3)| = 2$. Every group of index 2 in G is a normal subgroup.

2.82. *Find an example of a noncyclic group, all of whose proper subgroups are cyclic.*

Solution: Consider the symmetric group S_3 on 3 letters. .All proper non-trivial subgroups of S_3 are the followings
$H_1 = \{1, (12)\}, \quad H_2 = \{1, (13)\}, \quad H_3 = \{1, (23)\}, \quad H_4 = \{1, (123), (132)\}$.
Hence they are all cyclic groups of order 2 or 3. Hence S_3 is the required example.

2.83. *List all the elements of order 8 in* $\mathbf{Z}_{8000000}$. *How do you know your list is complete?*

Solution: Let $G = \mathbf{Z}_{800000}$ and let x be an element of order 8 in G, then $|\langle x \rangle| = 8$. Since G is a cyclic group and a cyclic group has a unique subgroup for each divisor of its order we have a unique subgroup of order 8. Then all the elements of order 8 is contained in $\langle x \rangle$. Hence the question reduces to find the number of elements of order 8 in $\mathbf{Z}_8$. They are $\{1, 3, 5, 7\}$.Therefore we have 4 elements of order 8 in $\mathbf{Z}_{8000}$.The list is complete as up to isomorphism there exists a unique cyclic group of order 8 namely $\mathbf{Z}_8$.

2.84. *Explain why* $\mathbf{Z}_8 \oplus \mathbf{Z}_4$ *and* $\mathbf{Z}_{8000000} \oplus \mathbf{Z}_{4000000}$ *must have the same numbers of elements of order* 4.

Solution: Recall that in a group $A \oplus B$ the orders of elements $|(a,b)| = lcm(|a|,|b|)$. Hence we need to find the number of pairs (a,b) such that $lcm(|a|,|b|) = 4$. Hence $|a| = 1,2,4$ or $|b| = 1,2,4$ such that satisfying $lcm(|a|,|b|) = 4$. We need to exclude $|a| = |b| = 2$ as $lcm(|a|,|b|) = 2$. In order to find the number of elements of order 4 in $\mathbf{Z}_8$ we consider the following: any element of order 4 is contained in the unique subgroup of $\mathbf{Z}_8$ of order 4. Hence we need to find the number of generators of that subgroup of order 4 which is 2 namely the elements relatively prime to 4.

Because of the above observation any element of order 4 in $\mathbf{Z}_{800000}$ generates a subgroup of order 4. But $\mathbf{Z}_{800000}$ is cyclic and by the above explanation it has a unique subgroup of order 4. Hence it is isomorphic to $\mathbf{Z}_4$. Therefore the number of elements of order 4 is the number of generators of that group of order 4 which is 2.

$(|a|,|b|) = (4,1)$ the number of (a,b) is $2 \cdot 1 = 2$
$(|a|,|b|) = (4,2)$ the number of (a,b) is $2 \cdot 1 = 2$
$(|a|,|b|) = (4,4)$ the number of (a,b) is $2 \cdot 2 = 4$
$(|a|,|b|) = (2,4)$ the number of (a,b) is $1 \cdot 2 = 2$
$(|a|,|b|) = (1,4)$ the number of (a,b) is $1 \cdot 2 = 2$
Hence totally we have 12 elements of order 4.

2.85. . *How many elements of order* 4 *does* $\mathbf{Z}_4 \oplus \mathbf{Z}_4$ *have? (Do not do this exercise by checking each member of* $\mathbf{Z}_4 \oplus \mathbf{Z}_4$.)

Solution: Recall that in a group $A \oplus B$ the order of elements $|(a,b)| = lcm(|a|,|b|)$. Hence we need to find the number of elements $(a,b) \in \mathbf{Z}_4 \oplus \mathbf{Z}_4$ such that $lcm(|a|,|b|) = 4$.

The number of elements of order 4 in $\mathbf{Z}_4$ is 2. The number of elements of order 2 in $\mathbf{Z}_4$ is 1

The number of (a,b) such that $|a| = 4 \quad |b| = 2$ is $2 \cdot 1 = 2$
$|a| = 4 \quad |b| = 4$ is $2 \cdot 2 = 4$
$|a| = 2 \quad |b| = 4$ is $1 \cdot 2 = 2$
$|a| = 2 \quad |b| = 4$ is $1 \cdot 2 = 2$
So we have all together 12 elements of order 4. in $\mathbf{Z}_4 \oplus \mathbf{Z}_4$.

2.86. *Let* M *be the group of all real* 2×2 *matrices under addition. Let* $N = \mathbf{R} \oplus \mathbf{R} \oplus \mathbf{R} \oplus \mathbf{R}$ *under componentwise addition. Prove that*

M and N are isomorphic. What is the corresponding theorem for the group of $n \times n$ matrices under addition?

Solution: Define a map $f : M \to M$
$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to (a, b, c, d)$ It is easy to see that f is an isomorphism of additive abelian groups.

b) For the group M of $n \times n$ matrices with respect to addition $N = R \oplus \cdots \oplus R$ n-copies of R are isomorphic. The map defined similar to the above and the addition on the right hand side is componentwise addition.

2.87. *Any group of order 12 is isomorphic to one of $\mathbf{Z}_{12}, \mathbf{Z}_6 \oplus \mathbf{Z}_2, A_4$ or D_6. To which of these is isomorphic to $S_3 \oplus \mathbf{Z}_2$?*

Solution: The group $S_3 \oplus \mathbf{Z}_2$ cannot be isomorphic to $\mathbf{Z}_{12}$ and $\mathbf{Z}_6 \oplus \mathbf{Z}_2$ as they are abelian but $S_3 \oplus \mathbf{Z}_2$ is not abelian as the group S_3 in the first component is not abelian. Hence $S_3 \oplus \mathbf{Z}_2$ either isomorphic to A_4 or D_6.The group $S_3 \oplus \mathbf{Z}_2$ has a subgroup of order 6 but A_4 does not have a subgroup of order 6 moreover the group$S_3 \oplus \mathbf{Z}_2$ has a unique subgroup of order 3 but A_4 has 4 subgroups of order 3 . Hence $S_3 \oplus \mathbf{Z}_2$ is isomorphic to D_6.

Solution: Consider $n = p_1^2 p_2^2 p_3 \cdots p_k$ where p_i are distinct primes. Then any group of order n is isomorphic to
$\mathbf{Z}_{p_1^2} \oplus \mathbf{Z}_{p_2^2} \oplus \mathbf{Z}_{p_3} \oplus \cdots \oplus \mathbf{Z}_{p_k}$.
$\mathbf{Z}_{p_1} \oplus \mathbf{Z}_{p_1} \oplus \mathbf{Z}_{p_2^2} \oplus \mathbf{Z}_{p_3} \oplus \cdots \oplus \mathbf{Z}_{p_k}$.
$\mathbf{Z}_{p_1} \oplus \mathbf{Z}_{p_1} \oplus \mathbf{Z}_{p_2} \oplus \mathbf{Z}_{p_2} \oplus \mathbf{Z}_{p_3} \oplus \cdots \oplus \mathbf{Z}_{p_k}$
$\mathbf{Z}_{p_1^2} \oplus \mathbf{Z}_{p_2} \oplus \mathbf{Z}_{p_2} \oplus \mathbf{Z}_{p_3} \oplus \cdots \mathbf{Z}_{p_k}$

2.88. *Prove that the center of a group is characteristic.*

Solution: Let φ be an automorphism of G and let z be any element of $\mathbf{Z}(G)$. Then we need to show that
$(z)\varphi \in Z(G)$.
Let $g \in G$. Since φ is an automorphism so φ is bijective hence for any $g \in G$ there exists $x \in G$ such that $(x)\varphi = g$. Then
$(xz)\varphi = (zx)\varphi = (xz)\varphi$

$(x)\varphi(z)\varphi = (z)\varphi(x)\varphi$. Then we have

$g(z)\varphi = (z)\varphi g$. for all $g \in G$.Hence we have

$(z)\varphi \in Z(G)$. Then

$(Z(G))\varphi \subset Z(G)$. using the fact that φ is one-to-one and onto we obtain $Z(G)\varphi = Z(G)$. i.e. $Z(G)$ is a characteristic subgroup of G.

2.89. *The commutator subgroup G' of a group G is the subgroup generated by the set $\{x^{-1}y^{-1}xy \mid x, y \in G\}$. (That is, every element of G' has the form $a_1^{i_1}a_2^{i_2}\cdots a_k^{i_k}$ where each a_j has the form $x^{-1}y^{-1}xy$, each $i_j = \pm 1$ and k is any positive integer.) Prove that G' is a characteristic subgroup of G. This important subgroup was first introduced by G.A. Miller.*

Solution: The commutator $u = x^{-1}y^{-1}xy$ is an arbitrary generator of G^1.

Let φ be an automorphism of G. Then

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

$= ((x)\varphi)^{-1}((y)\varphi)^{-1}(x)\varphi(y)\varphi \in G^1$. Then for any generator $u \in G^1$ $(u)\varphi$ is also a generator of G^1.

$(u)\varphi \in G^1$. $(G^1)\varphi \subseteq G^1$. Moreover for

$x^{-1}y^{-1}xy \in G^1$ where $x, y \in G$ there exists $x^1, y^1 \in G$ such that $(x_1)\varphi = x$ and $(y_1)\varphi = y$. Then

$(\ (x_1)^{-1}(y_1)^{-1}x_1y_1)\varphi = (x^{-1})y^{-1}xy$. This implies that $G^1 \leq (G^1)\varphi$. Hence we have $G^1 = \varphi(G')$

2.90. *Prove that $\mathbf{R}$ under addition is not isomorphic to $\mathbf{R}^*$ under multiplication.*

Solution: *Assume that there exists and isomorphism from $(\mathbf{R}, +)$ onto $R^*, \cdot)$ Then for $-1 \in R^*$ there exists an element $y \in R$ such that $f(y) = -1$.*

Let $f(\frac{y}{2}) = a$ in $\mathbf{R}$. Then $f(y) = f(\frac{y}{2}+\frac{y}{2}) = f(\frac{y}{2})f(\frac{y}{2}). = a^2 = -1$. But this is impossible in real numbers.

One can argue the same question also as follows. The group $\mathbf{R}$ under addition has no element of finite order it is a torsion free group but $\mathbf{R}^*$ under multiplication has an element -1 hence these two groups cannot be isomorphic.

2.91. *Show that* $\mathbf{Q}^+$ *(the set of positive rational numbers) under multiplication is not isomorphic to* $\mathbf{Q}$ *under addition.*

Solution: Let $f : (\mathbf{Q}, +) \to (\mathbf{Q}^+, \cdot)$
$f(a+b) = f(a) \cdot f(b)$. Then there exists
$y \in \mathbf{Q}$ such tthat $f(y) = 2$. Then we have
$f(y) = f(\frac{y}{2} + \frac{y}{2}) = f(\frac{y}{2})\ f(\frac{y}{2}) = a^2 = 2$ for some $a \in \mathbf{Q}$.
But this is impossible in $\mathbf{Q}$.

2.92. *Suppose* $G = \{e, x, x^2, y, yx, yx^2\}$ *is a non-abelian group with* $|x| = 3$ *and* $|y| = 2$. *Show* $xy = yx^2$.

Solution: Observe first that $xy \neq yx$. Otherwise G is abelian.
Since $|x| = 3$, we have $x \neq e$,
$x^2 \neq e$. and $y \neq e$
So the only possibilities for xy are x, x^2, yx^2
If $xy = x$ then $y = e$.
If $xy = x^2$ then $y = x$ this implies $y^2 = x^2 = e$ which is impossible
$xy = y$ implies $x = e$ Hence the only remaining element is yx^2.

2.93. *(i) The set*

$$G = \left\{ \left[\begin{array}{ccc} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{array} \right] \middle| \quad a, b, c \in \mathbf{Z}_3 \right\}$$

is a group under multiplication if addition and multiplication of the entries are done modulo 3.
(ii) How many elements does G *have?*
(iii) Find three subgroups of G *of order* 9.
(iv) Are these subgroups of order 9 *abelian?*
(v) Is G *abelian?*

Solution: One can see that G is a group under multiplication by checking the group axioms.
(ii) There are 3 possibilities for each of a, b or c. Hence $|G| = 27$.
(iii)

$$H_1 = \left\{ \left[\begin{array}{ccc} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right] \mid \ a, b \in \mathbf{Z}_3 \right\}$$

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a'+a & b'+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & a' & b' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & b+b' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Since $\mathbf{Z}_3$ is a commutative group with respect to addition modulo 3 and $a, b, a^1, b^1 \in \mathbf{Z}_3$ we have

$a+a' = a'+a, \qquad b+b' = b+b'$. Hence H_1 is an abelian subgroup of G of order 9. Recall that for any prime p the group of order p^2 is abelian.

$$H_2 = \left\{ \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid \ b, c \in \mathbf{Z}_3 \right\}$$

$$\begin{bmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & b'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & b+b' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{bmatrix}$$

By the above explanation H_2 is an abelian subgroup of G of order 9.

$$H_3 = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} \mid \ a, b \in \mathbf{Z}_3 \right\}$$

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & a' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a'+a & b'+aa'+b \\ 0 & 1 & a'+a \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & a' & b' \\ 0 & 1 & a' \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & b+a'+b' \\ 0 & 1 & a+a' \\ 0 & 0 & 1 \end{bmatrix}$$

Since for any $a, a' \in \mathbf{Z}_3$ we have $a'a = aa'$ we get H_3 is an abelian subgroup of order 9.

G is not abelian since $x = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$, $y = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$ $xy \neq yx$.

2.94. *Find the centralizer of* $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ *in* $GL(2, \mathbf{R})$.

Solution:

$C_{GL(2,\ \mathbf{R})}\left(\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\right) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbf{R}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right\}$

So $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ gives the equality $\begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix}$. Hence we get

$a + b = a$

$c + d = a + c$

$b + d = d$

Then $b = 0$ and $d = a$. Hence

$$C_{GL(2,\mathbf{R})}\left(\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\right) = \left\{ \begin{bmatrix} a & 0 \\ c & a \end{bmatrix} \mid a \neq 0, \quad a,\ c \in \mathbf{R} \right\}.$$

2.95. *Let* $K = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in \mathbf{Q} \quad ab \neq 0 \right\}$. *Prove*

(a) K is a subgroup of $GL(2,\ \mathbf{Q})$. (The elements of K are called ***diagonal matrices.)***

(b) $Z(K) = K$.

(c) Are your proofs for (a) and (b) valid when $\mathbf{Q}$ *is replaced by* $\mathbf{R}$ *the field of real numbers? Are they valid when* $\mathbf{Q}$ *is replaced by* $\mathbf{Z}_p$*? the finite field with p-elements*

Solution: Let $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ and $\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ be elements of K. Then $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}$ since $ab \neq 0$ and $cd \neq 0$ we get $acbd \neq 0$. Hence $\begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in K$

$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}^{-1} = \begin{bmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix} \in K$ since $ab \neq 0$ we obtain $a^{-1}b^{-1} \neq 0$.

Hence K is a subgroup of $GL(2, \mathbf{Q})$. Observe that as $a, b \in \mathbf{Q}$ we have $a^{-1}, b^{-1} \in \mathbf{Q}$.

b) $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}$

and $\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} ca & 0 \\ 0 & db \end{bmatrix}$

Since $\mathbf{Q}$ is a commutative group with respect to multiplication we get that K is a commutative group. Hence $Z(K) = K$

c) Yes.

2.96. *Let* G *be a group. Show that* $Z(G) = \bigcap_{a \in G} C_G(a)$.

Solution: Let $x \in \bigcap_{a \in G} C_G(a)$. Then $xa = ax$ for all $a \in G$. This means $x \in Z(G)$.

Conversely if $x \in Z(G)$, then $xa = ax$ for all $a \in G$. Hence $x \in C_G(a)$ for all $a \in G$, that implies $x \in \bigcap_{a \in G} C_G(a)$.

2.97. *Let* $G = SL(2, \mathbf{R})$*. For any positive integer* n *and any angle* θ *show that*

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}.$$

Use this formula to find the order of

$$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix} \text{ and } \begin{bmatrix} \cos\sqrt{2^\circ} & -\sin\sqrt{2^\circ} \\ \sin\sqrt{2^\circ} & \cos\sqrt{2^\circ} \end{bmatrix}.$$

(Geometrically, $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ *represents a rotation of the plane* θ *degrees).*

Solution: By induction on n. For $n = 1$, it is clear.

Assume $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$

Then

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^{n+1} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n$$

$$= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$$

$$= \begin{bmatrix} \cos\theta\cos n\theta - \sin\theta\sin n\theta & -\cos\theta\sin n\theta - \sin\theta\cos n\theta \\ \sin\theta\cos n\theta + \cos\theta\sin n\theta & -\sin\theta\sin n\theta + \cos\theta\cos n\theta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(n+1)\theta & -\sin(n+1)\theta \\ \sin(n+1)\theta & \cos(n+1)\theta \end{bmatrix}$$

Now to find the order of the matrices consider

$$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60 & \cos 60^\circ \end{bmatrix}^6 = \begin{bmatrix} \cos 360^\circ & -\sin 360^\circ \\ \sin 360^\circ & \cos 360^\circ \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

For any number $1 \leq k < 6$ we can not get the identity because of the above formula. Hence the order of the above matrix is 6.

$\begin{bmatrix} \cos\sqrt{2^\circ} & -\sin\sqrt{2^\circ} \\ \sin\sqrt{2^\circ} & -\cos\sqrt{2^\circ} \end{bmatrix}$ has infinite order, since for any n, $n\sqrt{2^\circ} \neq 360^\circ$ as $\sqrt{2}$ is an irrational number.

2.98. *Consider the set* $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$. *Suppose there is a group operation* $\star$ *on* G *that satisfies the following two conditions:*

(a) $a \star b \leq a + b$ *for all* a, b *in* G.

(b) $a \star a = 0$ *for all* a *in* G.

Construct the multiplication table for G. *(This group is sometimes called the Nim group.)*

Solution:

$\star$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

2.99. *Let* G *be a finite group.*

(i) Show that there are an odd number of elements x *of* G *such that* $x^3 = e$.

(ii) Show that there are an even number of elements x *of* G *such that* $x^2 \neq e$.

Solution: (i) For each $e \neq x \in G$ with $x^3 = e$ we have $(x^2)^3 = x^6 = e$. Hence x and x^2 are elements of order 3 and certainly $x \neq x^2 = x^{-1}$. This implies every non trivial element x of order 3 gives another element x^2 of order 3. Hence the set of non-trivial elements of order 3 are paired as $(x, x^2), (y, y^2), \cdots$ and so on. Since identity also satisfies $e^3 = e$, we get the number of elements satisfying $x^3 = e$ is an odd number.

(ii) For the second part each non-trivial element x such that $x^2 \neq e$ gives $(x^{-1})^2 \neq e$ and $x \neq x^{-1}$. So the set of elements satisfying $x^2 \neq e$ are the pairs (x, x^{-1}) $(y, y^{-1}), \cdots$. Hence their number is even when G is a finite group.

2.100. *Let x belong to a group. If $x^2 \neq e$ while $x^6 = e$, prove that $x^4 \neq e$ and $x^5 \neq e$. What can we say about the order of x?*

Solution: We have $x^2 \neq e$ and $x^6 = e$. So $x^4 = x^{-2}$. Since $x^2 \neq e$ we obtain $x^{-2} \neq e$. Then we get $x^4 = x^{-2} \neq e$. Now multiplying by x^{-1} both sides of the equation $x^6 = e$ we have $x^5 = x^{-1} \neq e$ since $x^2 \neq e$ then we have $x^{-1} \neq x \neq e$. The order of x is either 3 or 6.

2.101. *Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G.*

Solution: $a^{-1}b^{-1} = (ab)^{-1} = b^{-1}a^{-1}$. Now take the inverse of both sides we obtain $ba = ab$ for all $a, b \in G$. Hence G is abelian. Converse is clear.

2.102. *(i) Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40.*
(ii) What is the identity element of this group?
(iii) Can you see any relationship between this group and $U(8)$ the group consisting of invertible elements in $\mathbf{Z}_8$?

Solution: The group table of the multiplication modulo 40 is the following table.

$\cdot$	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

(ii) Observe that 25 is the identity element of the above group.

(iii) The group table of $U(8) = \{1, 3, 5, 7\}$ is the following table

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Both groups are abelian of order 4 and in both groups every element x satisfies $x^2 = e$. Hence they are isomorphic to $Z_2 \oplus Z_2$.

2.103. *Suppose the table given below is a group table. Fill in the blank entries.*

Solution:

	e	a	b	c	d
e	e	-	-	-	-
a	-	b	-	-	e
b	-	c	d	e	-
c	-	d	-	a	b
d	-	-	-	-	-

To find the entries in the table, we may look at the table as a 5×5 matrix. First consider the entry x_{41}. Since the table is a group table each symbol should appear in each row and in each column once. The the only possibility for x_{41} is c. Then $x_{43} = e$ Then the table becomes

	e	a	b	c	d
e	e	-	-	-	-
a	-	b	-	-	e
b	-	c	d	e	-
c	c	d	e	a	b
d	-	-	-	-	-

Since by Lagrange Theorem any group of order 5 is a cyclic group because every non-trivial element generate the group our group table must be symmetric with respect to diagonal. Then the table becomes

	e	a	b	c	d
e	e	-	-	c	-
a	-	b	c	d	e
b	-	c	d	e	-
c	c	d	e	a	b
d	-	-	-	b	-

Now $x_{21} = a$ and the only possibility for $x_{31} = b$ and for $x_{35} = a$

Now it is easy to complete the table with the above information using commutativity.

Note: Every symbol should appear at most and at least once in each row and in each column.

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

2.104. *(i) Show that* $U(14) = \langle 3\rangle = \langle 5\rangle$. *(Hence* $U(14)$ *is cyclic.)*
(ii) Is $U(14) = \langle 11\rangle$?

Solution: $U(14) = \{1, 3, 5, 9, 11, 13\}$
$3 \equiv 3(\mod 14)$, $3^2 \equiv 9(\mod 14)$, $3^3 \equiv 13(\mod 14)$, $3^4 \equiv 11(\mod 14)$, $3^5 \equiv 5(\mod 14)$, $3^6 \equiv 1(\mod 14)$
Hence $U(14) = \langle 3\rangle$.
Now we will do similar calculation for 5. Indeed $5 \equiv 5(\mod 14), 5^2 \equiv 11(\mod 14)$, $5^3 \equiv 13(\mod 14)$, $5^4 \equiv 9(\mod 14)$, $5^5 \equiv 3(\mod 14)$, $5^6 \equiv 1(\mod 14)$.
Hence $U(14) = \langle 5\rangle$ i.e. $U(14)$ is a cyclic group.
$\langle 11\rangle = \{1, 11, 9\}$. So $5 \notin \langle 11\rangle$. Hence $\langle 11\rangle \neq U(14)$

2.105. *Let* $G = \{1, -1, i, -i\}$ *be the group of four complex numbers under multiplication.*
(a) Is $\{1, -1\}$ *a subgroup of* G*? Why?*
(b) Is $\{1, i\}$ *a subgroup of* G*? Why?*

Solution: i) Yes. Since G is a finite group it is enough show $ab \in \{1, -1\}$, for all $a, b \in \{1, -1\}$ which is obviously true.

ii) No. Since $i^2 \notin \{1, i\}$.

2.106. *List the elements of the subgroups* $\langle 20\rangle$ *and* $\langle 10\rangle$ *in* $\mathbf{Z}_{30}$.

Solution: $\langle 20\rangle = \{0, 20, 10\}$ and $\langle 10\rangle = \{0, 10, 20\}$
Hence $\langle 20\rangle = \langle 10\rangle$ in $\mathbf{Z}_{30}$.

2.107. *List the elements of the subgroups* $\langle 3\rangle$ *and* $\langle 15\rangle$ *in* $\mathbf{Z}_{18}$.

Solution: $\langle 3\rangle = \{0, 3, 6, 9, 12, 15\}$
$\langle 15\rangle = \{0, 15, 12, 9, 6, 3\}$
Hence $\langle 3\rangle = \langle 15\rangle$ in $\mathbf{Z}_{18}$.

2.108. *List the elements of the subgroups* $\langle 3\rangle$ *and* $\langle 7\rangle$ *in* $U(20)$.

Solution: $\langle 3\rangle = \{1, 3, 9, 7\}$
$\langle 7\rangle = \{1, 7, 9, 3\}$
Hence $\langle 3\rangle = \langle 7\rangle$ in $U(20)$

2.109. *If* $|a| = n$, *show that* $|a^t| = \frac{n}{\gcd(n,t)}$.

Solution: Let $|a| = n$. Then $(a^t)^{\frac{n}{\gcd(n,t)}} = (a^n)^{\frac{t}{\gcd(n,t)}} = e$ as we know that $\frac{t}{\gcd(n,t)}$ is an integer. If $|a^t| = s$, then by above $s|\frac{n}{\gcd(n,t)}$. The equality $|a^t| = s$, implies that $a^{ts} = e$. This implies that $n|ts$ and $n \leq ts$.

Let $k = \gcd(n, t)$. Then $\gcd(\frac{t}{k}, \frac{n}{k}) = 1$. Let $ts = nm$ for some $m \in \mathbf{Z}$. Then $\frac{t}{k}s = \frac{n}{k}m$. So $\frac{t}{k}|m$ as $\frac{t}{k}$ and $\frac{n}{k}$ are relatively prime. Hence by cancelling the $\frac{t}{k}$ in the above equation we have $s = \frac{n}{k}m_1 = \frac{n}{\gcd(n,t)}m_1$ for some $m_1 \in \mathbf{Z}$. Then $\frac{n}{\gcd(n,t)}|s$

So m_1 must be 1 and we obtain $s = \frac{n}{\gcd(n,t)} = |a^t|$.

3. RINGS

3.1. *If R is a ring and $a, b, c, d \in R$, evaluate $(a+b)(c+d)$.*

Solution: $(a+b)(c+d) = a(c+d) + b(c+d)$ by distributive law

$$\begin{aligned} &= (ac+ad) + (bc+bd) \\ &= ac + ad + bc + bd \end{aligned}$$

3.2. *Prove that if $a, b \in R$, then $(a+b)^2 = a^2 + ab + ba + b^2$ where by x^2 we mean xx.*

Solution: $(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b)$
$= a^2 + ab + ba + b^2$

Note that if R is not a commutative ring $ab \neq ba$.

3.3. *If in a ring R every $x \in R$ satisfies $x^2 = x$, prove that R must be commutative*

*(A ring in which $x^2 = x$ for all elements is called a **Boolean ring**).*

Solution: Let $x, y \in R$. Then $(x+y)^2 = (x+y)(x+y) = x^2 + xy + yx + y^2$

Since $x^2 = x$ and $y^2 = y$ we have $x + y = x + xy + yx + y$.

Hence $xy = -yx$.

But for every $x \in R$

$(-x) = (-x)^2 = (-x)(-x) = x^2 = x$.

Hence $-yx = yx$ i.e. we obtain $xy = yx$.

3.4. *Prove that any field is an integral domain.*

Solution: Let $a \neq 0$ and b be two elements in the field F and $ab = 0$. Since F is a field and $a \neq 0$. we have $a^{-1} \in F$. Hence $a^{-1}ab = a^{-1}0 = 0$. So we obtain $b = 0$.

Hence there exists no zero divisor in F.

3.5. *If U is an ideal of R and $1 \in U$, prove that $U = R$.*

Solution: Since for any $r \in R$ and $u \in U$, $ru \in U$ we have for any $r \in R$, $r1 = r \in U$. Hence $R = U$.

3.6. *If F is a field, prove that its only ideals are (0) and F itself.*

Solution: Let I be an ideal of a field F. Assume that $(0) \neq I$ and let $0 \neq a \in I$. Then as F is a field, there exists $a^{-1} \in F$ such that $a^{-1}a = 1$. Hence $1 \in I$. Now by exercise 3.5, $I = F$. So every non-zero ideal of F is equal to F.

3.7. *If D is an integral domain and if $na = 0$ for some $a \neq 0$ in D and some integer $n \neq 0$, prove that D is of finite characteristic.*

Solution: Let $b \in D$. Consider nab. Since $(na) = 0$ we have $nab = 0$. On the other hand $nab = nba$ as integral domain is a commutative ring. So $0 = nab = nba$. But $a \neq 0$ implies $nb = 0$ for all $b \in D$.

3.8. *D is an integral domain and D is of finite characteristic, prove that the characteristic of D is a prime number.*

Solution: Let a be any non zero element of D. Then $a^2 \neq 0$ as D is an integral domain. Since D is of positive characteristic q, then $qa^2 = 0$ for all $a \in D$.

If q is a composite number, let p_1 be a prime number dividing q and let $q = p_1q_1$.

Now

$$qa^2 = p_1q_1a^2 = p_1aq_1a = 0.$$

since D is integral domain either $p_1a = 0$ or $q_1a = 0$. By exercise 3.7, either of these equations gives a contradiction to the assumption that q is the smallest positive integer such that $qx = 0$ for all $x \in D$. Thus q is not composite, it is a prime.

3.9. *Show that the commutative ring D is an integral domain if and only if for $a, b, c \in D$ with $a \neq 0$ the relation $ab = ac$ implies that $b = c$.*

Solution: If D is a commutative ring and $a \neq 0$, then $ab = ac$ implies $a(b - c) = 0$. Since $a \neq 0$ we obtain $b = c$

Conversely assume that $ab = ac$ and $a \neq 0$ implies that $b = c$. Assume if possible that $a \neq 0$ and $ab = 0$ Then $ab = a0$ and hence $b = 0$

3.10. *If U, V are ideals of R, let $U+V = \{u+v \mid u \in U, v \in V\}$. Prove that $U+V$ is also an ideal.*

Solution: Let u_1+v_1 and u_2+v_2 be two elements of $U+V$. Then $u_1+v_1-(u_2+v_2) = (u_1-u_2)+(v_1-v_2)$. Since $u_1-u_2 \in U$ and $v_1-v_2 \in V$, we have $(u_1-u_2)+(v_1-v_2) \in U+V$. For any $r \in R$ we have

$r(u+v) = ru+rv \in U+V$ as $ru \in U$ and $rv \in V$ for any $u \in U, v \in V$.

Similarly $(u+v)r = ur+vr \in U+V$ as $ur \in U$ and $vr \in V$.

3.11. *If U is an ideal of R, let $r(U) = \{x \in R \mid xu = 0$ for all $u \in U\}$*

Prove that $r(U)$ is an ideal of R.

Solution: Let $x_1, x_2 \in r(U)$ and let $u \in U$. Then $(x_1-x_2)u = x_1u - x_2u = 0$ as $x_1u = 0$ and $x_2u = 0$. Hence $x_1 - x_2 \in r(U)$. Now let $r \in R$ and $x \in r(U)$. Then

$(rx)u = r(xu) = 0$

$(xr)u = x(ru) = 0$ as U is an ideal, $ru \in U$.

Hence $r(U)$ is an ideal of R.

3.12. *If R is a commutative ring and $a \in R$,*

a) Show that $aR = \{ar \mid r \in R\}$ is a two sided ideal of R.

b) Show by an example that this may be false if R is not commutative.

Solution: a) Clearly $0 \in aR$ so aR is non-empty. For any $ax, ay \in aR$

$$ax - ay = a(x-y) \in aR \text{ as } x-y \in R$$

Now for any $r \in R$ $rax = axr$ as R is commutative. Hence $axr \in aR$. So aR is a two sided ideal of R.

b) Consider the ring R of 2×2 matrices over real numbers.

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} R = \{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & t \end{bmatrix} \mid x, y \in \mathbf{R}\}$$

$$= \{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \mid x, y \in \mathbf{R}\}$$

this is not a two sided ideal as

$$\begin{bmatrix} x & y \\ z & t \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & 0 \\ z & 0 \end{bmatrix} \notin \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} R$$

for any $z \neq 0$.

3.13. *If R is a ring with unit element 1 and ϕ is a homomorphism of R into an integral domain R' such that kernel of ϕ is different from R, prove that $\phi(1)$ is the unit element of R'.*

Solution: Observe first that if $\phi(1) = 0$, then for any element $a \in R$ we have $\phi(a) = \phi(a.1) = \phi(a)\phi(1) = 0$. But by assumption we have $ker\phi \neq R$ so we obtain $\phi(1) \neq 0$. Then for any $y \in R'$ we have $\phi(1)y = \phi(1.1)y = \phi(1)\phi(1)y$. Then we have $\phi(1)y = \phi(1)\phi(1)y$ and so $\phi(1)(y - \phi(1)y) = 0$. Since R' is an integral domain and $\phi(1) \neq 0$ we obtain $\phi(1)y = y$ for all $y \in R'$. Hence $\phi(1)$ is an identity element of R'.

3.14. *If R is a ring with identity the element 1 and ϕ is a homomorphism of R onto R', then prove that $\phi(1)$ is the unit element of R'.*

Solution: Since ϕ is onto for any $w \in R'$ there exists $x \in R$ such that $\phi(x) = w$.

Now

$$\phi(x) = \phi(1x) = \phi(1)\phi(x) = \phi(x)\phi(1)$$

so $w = \phi(1)w = w\phi(1)$ for any $w \in R'$.

Hence $\phi(1)$ is the multiplicative identity element of R'.

3.15. *Prove that any homomorphism of a field is either a monomorphism or takes each element into 0.*

Solution: Let F be a field and α be a homomorphism of F to F. Assume that α is a non-zero homomorphism. If $\alpha(a) = 0$ for some $a \in F$, then $\alpha(1) = \alpha(aa^{-1}) = \alpha(a)\alpha(a^{-1}) = 0$. Then for any $b \in F$,

$\alpha(b) = \alpha(1)\alpha(b) = 0$.

But this is impossible as α is a non-zero map. Therefore α is a one to one homomorphism.(See also exercise 3.6.)

3.16. *If U is an ideal of R, let $[R : U] = \{x \in R \mid rx \in U$ for all $r \in R\}$. Prove that $[R : U]$ is an ideal of R and that it contains U.*

Solution: $[R : U] = \{x \in R \mid rx \in U \text{ for all } r \in R\}$

Let $x, y \in [R : U]$ so for any $r \in R$, $rx \in U$ and $ry \in U$. Then $r(x - y) = rx - ry \in U$ as U is an ideal. So $x - y \in [R : U]$. Now for any $s \in R$, and any $x \in [R : U]$, $r(sx) \in U$ for any $r \in R$ as $sx \in U$ and U is an ideal. Thus $sx \in [R : U]$. Similarly $(rx)s = r(xs) \in U$ for any $r \in R$, i.e. $xs \in [R : U]$ for any $s \in R$.

3.17. *Let R be a ring with unit element, R not necessarily commutative, such that the only right ideals of R are (0) and R. Prove that R is a division ring.*

Solution: Now consider aR for any $a \neq 0$. $aR = \{ar | r \in R\}$ is a right ideal of R. Indeed if ar_1 and ar_2 be two elements in aR, then $ar_1 - ar_2 = a(r_1 - r_2) \in aR$. Moreover for any $r \in R$ and $ax \in aR$, $(ax)r = axr \in aR$. Hence aR is a right ideal and $aR \neq \{0\}$ as $a \in aR$. Hence $aR = R$, this means that there exists $y \in R$ such that $ay = 1$. But then for every $a \neq 0$ there exists $y \in R$ such that $ay = 1$. Now consider $ya = y(ay)a$. So $ya = (ya)(ya) = (ya)^2$. Since there exists $t \in R$ such that $(ya)t = 1$, we get $yat = (ya)^2 t$, $1 = ya$ as required.

3.18. *If U, V are ideals of R let UV be the set of all elements that can be written as finite sums of elements of the form uv where $u \in U$ and $v \in V$. Prove that UV is an ideal of R.*

Solution:

$$UV = \{\ u_1v_1 + u_2v_2 + \cdots + u_nv_n \mid u_i \in U, v_i \in V\ i = 1, \ldots, n,\ n \in \mathbf{N}\ \}$$

Let $x = u_1v_1 + \cdots + u_nv_n$, where $u_i \in U$, $v_i \in V$ and let $y = t_1s_1 + \cdots + t_ms_m$, where $t_i \in U, s_i \in V$. Then $x - y = u_1v_1 + \cdots + u_nv_n - t_1s_1 - t_2s_2 \cdots - t_ms_m$. Hence $x - y \in UV$. Moreover for any $r \in R$ and any $x \in UV$.

$rx = ru_1v_1 + ru_2v_2 + \cdots + ru_nv_n \in UV$, since U is an ideal and so $ru_i \in U$, similarly $xr = u_1v_1r_1 + \cdots + u_nv_nr_n \in UV$. Now we use V is an ideal to conclude that $xv \in UV$. Hence UV is an ideal of R.

In questions 3.19, 3.20, 3.21, 3.22. Let D be an integral domain and define a relation $'' \sim''$ on $D \times D$ such that $b \neq 0$ and $d \neq 0$ $(a, b) \sim (c, d)$ if and only if $ad = bc$.

Let F be the set of equivalence classes $[a,b], (a,b) \in D \times D, b \neq 0$. The equivalence class $[ax,x]$ for some $x \neq 0$ is denoted by $[a,1]$. The product and addition of $[a,c]$ and $[b,d]$ is defined by $[a,b][c,d] := [ac,bd]$ and $[a,b]+[c,d] := [ad+bc,bd]$ respectively.

3.19. *Prove that if* $[a,b] = [a',b']$ *and* $[c,d] = [c',d']$, *then* $[a,b][c,d] = [a',b'][c',d']$.

Solution: The equivalence classes $[a,b] = [a',b']$ implies that $ab' = ba'$ and $[c,d] = [c',d']$ implies that $cd' = dc'$. In order to show that $[a,b][c,d] = [a',b'][c',d']$ we need to show that $[ac,bd] = [a'c',b'd']$ equivalently, $acb'd' = bda'c'$. So let's start from the left hand side.

$$\begin{aligned} acb'd' &= ab'cd' \quad \text{by commutativity} \\ &= ba'cd' \\ &= ba'dc' \\ &= bda'c' \end{aligned}$$

by commutativity. This is the required equality.

3.20. *Prove that if* $[a,b] = [a',b']$ *and* $[c,d] = [c',d']$, *then* $[a,b] + [c,d] = [a',b'] + [c',d']$.

Solution: The equivalence classes $[a,b] = [a',b']$ implies that $ab' = ba'$ and similarly $[c,d] = [c',d']$ implies that $cd' = dc'$.

To show that $[a,b]+[c,d] = [a',b']+[c',d']$ we need to show that

$$[ad+bc,bd] = [a'd'+b'c',b'd'].$$

Equivalently

$(ad+bc)b'd' = (a'd'+b'c')bd$ if and only if

$adb'd' + bcb'd' = a'd'bd + b'c'bd$. We start from the left hand side

$$\begin{aligned} adb'd' + bcb'd' &= ab'dd' + bb'cd' \\ &= a'bdd' + bb'dc' \\ &= a'd'bd + b'c'bd \end{aligned}$$

as required.

3.21. *Prove the distributivity law in F.*

Solution: Let $X = [a, b], \quad Y = [c, d]$ and $Z = [e, f]$ in F. Then $(X + Y)Z = ([a, b] + [c, d])([e, f])$

$$\begin{aligned} &= [ad + bc, bd][e, f] \\ &= [(ad + bc)e, bdf] \quad \text{by distributivity in D} \\ &= [ade + bce, bdf] \end{aligned}$$

$$\begin{aligned} XZ + YZ &= [a, b][e, f] + [c, d][e, f] \\ &= [ae, bf] + [ce, df] \\ &= [aedf + bfce, bfdf] \end{aligned}$$

But $[ade+bce, bdf] = [aedf+bfce, bfdf]$ equivalently $(ade+bce)bfdf = (bdf)(aedf + bfce)$

$adebfdf + bcebfdf = bdfaedf + bdfbfce$. Hence $(X + Y)Z = XZ + YZ$.

3.22. *Prove that the mapping $\phi : D \to F$ defined by $\phi(a) = [a, 1]$ is a monomorphism of D to F.*

Solution: The function $\phi : D \to F$.

$$\phi(a) = [a, 1]$$

$$\begin{aligned} \phi(ab) = [ab, 1] &= [abx^2, x^2] = [ax(bx), x^2] = [ax, x][bx, x] = [a, 1][b, 1] \\ &= \phi(a)\phi(b) \\ \phi(a + b) = [a + b, 1] &= [a, 1] + [b, 1] \\ &= \phi(a) + \phi(b). \\ K_\phi &= \{\ a \in D \mid \phi(a) = [0, 1]\ \} \end{aligned}$$

$a \in K_\phi$ if and only if $[a, 1] = [ax, x] = [0, 1] = [0y, y]$ if and only if $axy = 0yx = 0$. Since $x \neq 0 \neq y$ and D is an integral domain we have $a = 0$. So $K_\phi = \{0\}$ and ϕ is a monomorphism.

3.23. *Let Z be the ring of integers, p a prime number and (p) the ideal of Z consisting of all multiples of p. Prove*

a) $Z/(p)$ is isomorphic to Z_p the ring of integers mod p.

b) Prove that Z_p is a field. (Hint: use (p) is a maximal ideal and Z is a commutative ring with unit element.)

Solution: a) Define a homomorphism $\varphi : Z \to Z_p$ by $\varphi(a) = a \ (mod\ p)$. It is easy to check that this is a ring homomorphism, which is onto.

$$\begin{aligned} Ker(\varphi) &= \{a \in Z \mid a \equiv 0 \ (mod\ p)\ \} \\ &= \{a \in Z \mid a = kp \text{ for some } k \in Z\} \\ &= (p) \end{aligned}$$

This implies by the isomorphism theorem that $Z/(p) \cong Z_p$

b) Since Z is an integral domain, it is enough to show that (p) is a maximal ideal (which implies that $Z/(p)$ is a field).

Assume that I is another ideal of Z such that $I \neq (p)$ and $(p) \subset I$. Then there exists $a \in I \setminus (p)$. Since p is prime and p does not divide a, the greatest common divisor $(a, p) = 1$. Therefore $1 = ax + py$ for some $x, y \in Z$. Thus $1 \in I$, since $ax, py \in I$, i.e. $I = Z$.

Hence (p) is maximal and $Z/(p)$ is a field.

3.24. *Prove that the units in a commutative ring with unit element form an abelian group.*

Solution: Let x and y be units in R. Then there exists x^{-1} and $y^{-1} \in R$ such that $xx^{-1} = x^{-1}x = 1$ and $yy^{-1} = y^{-1}y = 1$.

Now $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1$ and $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = 1$.

Hence xy is invertible. Since $(x^{-1})^{-1} = x$ the element x^{-1} is also a unit. So the set of all units in R is closed with respect to the multiplication in R and taking inverses.

Since the associativity is inherited from the ring axioms, the set of units in R is a group with respect to the multiplication in R.

Since the ring is commutative, the group is also commutative.

3.25. *Prove that if K is any field which contains an integral domain D, then K contains a subfield isomorphic to the field F of the fractions of D. (In this sense F is the smallest field containing D).*

Solution: Let F be the field of fractions of the integral domain D. Let K be any field containing D. Every element in D is contained in K and has an inverse in K. Define a map

$\varphi : F \to K$.

$[a, b] \to ab^{-1}$ since $a \in D$, $0 \neq b \in D$ and K is a field $b^{-1} \in K$ and the product $ab^{-1} \in K$.

φ is well defined. Indeed

$[a, b] = [c, d]$, then $ad = bc$ and hence $ab^{-1} = cd^{-1}$ i.e. $\varphi([a, b]) = \varphi([c, d])$. Moreover

$\varphi([a, b][c, d]) = \varphi([ac, bd]) = (ac)(bd)^{-1} = (ab^{-1})(cd^{-1}) = \varphi([a, b])$ $\varphi([c, d])$ and

$\varphi([a, b] + [c, d]) = \varphi([ad + bc, bd]) = (ad + bc)(bd)^{-1} = ab^{-1} + cd^{-1} = \varphi([a, b]) + \varphi([c, d])$. For the kernel of the map φ we have

$K_\varphi = \{\ [a, b] \mid ab^{-1} = 0\ \} = [0, b]$

Hence K contains subfield $\varphi(F)$ which is isomorphic to F.

3.26. *Let D be an integral domain, $a, b \in D$. Suppose that $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n. Prove that $a = b$.*

Solution: We may embed the integral domain into a field.

If a is zero then b must be zero.

Assume that a is non-zero then a has inverse in the field. Since m and n are relatively prime there exists

x and y in $\mathbf{Z}$ such that $mx + ny = 1$. Since one of the integers may be negative we may need to use the fact that we can embed D into its field of fractions. Then

$a = a^{mx+ny} = a^{mx}a^{ny} = b^{mx}b^{ny} = b^{mx+ny} = b$ as required.

Remark: The above equation makes sense in the field but does not make sense in the domain as the negative power of an element does not make sense in D.

3.27. *Let R be a ring, possibly non commutative, in which $xy = 0$ implies $x = 0$ or $y = 0$. If $a, b \in R$ and $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n, prove that $a = b$.*

Solution: $(m,n)=1$, implies that, there exists $u,k \in \mathbf{Z}$ such that $mu+nk=1$. Since $m,n \geq 0$ either $u \geq 0$ or $k \geq 0$. Assume that $u>0$. Then $mu-nk=1$ where $k>0$. Hence $mu=nk+1$. Now, let

$a^{mu}=(a^m)^u=(b^m)^u=b^{mu}$

$b^{nk+1}=a^{mu}=a^{nk+1}=aa^{nk}=a(a^n)^k=a(b^n)^k=ab^{nk}$.

Hence

$bb^{nk}=ab^{nk}$ implies that $(b-a)b^{nk}=0$. Then either $b^{nk}=0$ or $b=a$. The first possibility $b^{nk}=0$ is impossible if $b \neq 0$. One can see this easily that, if t is the smallest positive integer such that $b^{t-1} \neq 0$, but $b^t=0$, then $0=b^t=b^{t-1}.b \neq 0$. This implies that the assumption $b^t=0$ is impossible, whenever $b \neq 0$. Hence $b=a$.

(In the above solution we assume $u>0$, if $k>0$, then we can continue the solution by changing the symbols u and k, in the above solution.)

3.28. *In a commutative ring with unit element, prove that the relation "a is an associate of b" is an equivalence relation.*

Solution: $a \sim b$ if and only if a is associate of b.

(1) $a \sim a$ as $a=1a$.

(2) $a \sim b$, then $b=ua$ for some unit u. Then $a=u^{-1}b$. Hence $b \sim a$.

(3) $a \sim b$ and $b \sim c$, then there exist units u and v such that $b=ua$ and $c=vb$

Now $c=vb=vua$ since product of two units in a commutative ring is again a unit, we have vu unit and so $a \sim c$

3.29. *Prove that if an ideal U of a ring R contains a unit of R, then $U=R$.*

Solution: Let U be an ideal of R and x be a unit in U. Then the exists $y \in R$ such that $xy=1_R \in U$. This implies $U=R$ as for any $r \in R \quad r1_R=r \in U$.

3.30. *Prove that in a Euclidean ring, the greatest common divisor (a,b) can be found as follows:*

$$\begin{aligned} b &= q_0 a + r_1 \ \ where \ \ d(r_1) < d(a) \\ a &= q_1 r_1 + r_2 \ \ where \ \ d(r_2) < d(r_1) \\ r_1 &= q_2 r_2 + r_3 \ \ where \ \ d(r_3) < d(r_2) \\ r_2 &= q_3 r_3 + r_4 \ \ where \ \ d(r_4) < d(r_3) \\ &\vdots \\ r_{n-2} &= q_{n-1} + r_{n-1} + r_n \\ r_{n-1} &= q_n r_n \end{aligned}$$

and $r_n = (a, b)$

Solution: First we show that r_n divides a and b.Indeed

$r_{n-1} = q_n r_n$

$r_{n-2} = q_{n-1} r_{n-1} + r_n$ substitute $r_{n-1} = q_n r_n$, hence r_n divides r_{n-1}.

$r_{n-2} = q_{n-1} q_n r_n + r_n = (q_{n-1} q_n + 1) r_n$

Hence r_n divides $r_n - 2$

$r_{n-3} = q_{n-2} r_{r-2} + r_{n-1} = q_{n-2}(q_{n-1} q_{n+1}) r_n + q_n r_n$

Hence r_n divides $r_{n-3} = (q_{n-2}(q_{n-1} q_{n+1}) + q_n) r_n$ going up like this we reach a and b. Hence r_n divides a and b.

Assume there exists t in the Euclidean ring which divides both a and b

$b = q_0 a + r_1$ the assumption t divides b and a implies that t divides $b - q_0 a$, hence t divides r_1. As $a = p_1 r_1 + r_2$ we have t divides a, and t divides r_1 implies that t divides $a - q_1 r_1 = r_2$. Continuing like this, we show from the equation $r_{n-2} = q_{n-1} r_{n-1} + r_n$ that t divides r_n.

3.31. *Find the greatest common divisor of the following polynomials over F, the field of rational numbers.*

a) $x^2 + x - 2$ *and* $x^5 - x^4 - 10x^3 + 10x^2 + 9x - 9$

b) $x^2 + 1$ *and* $x^6 + x^3 + x + 1$.

Solution: a) $x^5 - x^4 - 10x^3 + 10x^2 + 9x - 9 = (x^3 - 2x^2 - 6x + 12)(x^2 + x - 2) + (-15x + 15)$ and

$x^2 + x - 2 = (-15x + 15)(-\frac{1}{15}x - \frac{2}{15})$.

Hence $-15x+15$ is a greatest common divisor of $x^5-x^4-10x^3+10x^2+9x-9$ and x^2+x-2. Since any associate of a greatest common divisor is again a greatest common divisor we may say that $x-1$ is also o greatest common divisor of the above polynomials.

b) $x^6+x^3+x+1=(x^4-x^2+x+1)(x^2+1)$. Hence greatest common divisor is x^2+1.

3.32. *Prove that*
(a) x^2+x+1 *is irreducible over* F, *the field of integers mod 2.*
(b) x^2+1 *is irreducible over the integers mod 7.*
(c) x^3-9 *is irreducible over the integers mod 31.*
(d) x^3-9 *is reducible over the integers mod 11.*

Solution: In this question all the polynomials are either of degree 2 or 3. Therefore if it is reducible, then one of the factors should be linear i.e. this polynomial has a root in the given field. Hence it is enough to check whether the given polynomial has a root in this field or not.

a) $f(x)=x^2+x+1$ where F has two elements 0 and 1.
$f(0)=1 \ (mod\ 2)$

$f(1)=1 \ (mod\ 2)$. Hence $f(x)$ is irreducible.

b) $f(x)=x^2+1$ where $F=Z_7$.
$f(0)=1$, $f(1)=2$, $f(2)=5$, $f(3)=3$, $f(4)=3$
$f(5)=5$, $f(6)=2$.
Hence $f(x)$ has no root in Z_7.

c) $f(x)=x^3-9$, $f(0)=-9$, $f(1)=-8$, $f(2)=-1$, $f(3)=18$, $f(4)=24$, $f(5)=23$, $f(6)=21$, $f(7)=24$.
$f(8)=7$, $f(9)=7$, $f(10)=30$, $f(11)=21$, $f(12)=14$.
$f(13)=18$, $f(14)=7$, $f(15)=18$, $f(16)=26$.
$f(17)=6$, $f(18)=26$, $f(19)=30$, $f(20)=24$, $f(21)=14$.
$f(22)=6$, $f(23)=6$, $f(24)=20$, $f(25)=23$, $f(26)=21$.

$f(27) = 20,\ \ f(28) = 26,\ \ f(29) = 14,\ \ f(30) = 21.$

d) $f(x) = x^3 - 9\ \ F = Z_{11}$
$f(0) = 2,\ \ f(1) = 3,\ \ f(2) = 10,\ \ f(3) = 7,\ f(4) = 0$

$f(5) = 6,\ \ f(6) = 9,\ \ f(7) = 4,\ \ f(8) = 9,\ \ f(9) = 5,\ \ f(10) = 1.$
$x^3 - 9 = (x - 4)(x^2 + 4x + 5)$

3.33. *Let F be the field of real numbers. Prove that $F[x]/\langle(x^2+1)\rangle$ is a field isomorphic to the field of complex numbers.*

Solution: $x^2 + 1$ is irreducible polynomial in $F[x]$. Hence the ideal generated by
$x^2 + 1$ is a maximal ideal in $F[x]$. Since $F[x]$ is a commutative ring with unit element $F[x]/\langle(x^2 + 1)\rangle$ is a field. Moreover every element in $F[x]/\langle(x^2 + 1)\rangle$ can be written in the form: $a_0 + a_1x + \langle(x^2 + 1)\rangle$ for some $a_0, a_1 \in F$: Any element of $F[x]/\langle(x^2 + 1)\rangle$ is of the form $f(x) + \langle(x^2 + 1)\rangle$ for some $f(x) \in F[x]$. Using the division algorithm we can write $f(x) = g(x)(x^2 + 1) + h(x),\ g(x), h(x) \in F[x]$ and either $h(x) = 0$ or $deg\ h(x) \leq 1$. We obtain $f(x) + \langle(x^2 + 1)\rangle = g(x)(x^2 + 1) + h(x) + \langle(x^2 + 1)\rangle = h(x) + \langle(x^2 + 1)\rangle$ where $deg\ (h(x)) \leq 1$.

Hence every element of $F[x]/\langle(x^2 + 1)\rangle$ is of the form $a_0 + a_1x + \langle(x^2 + 1)\rangle$. Then

$F[x]/\langle(x^2 + 1)\rangle = \{a_0 + a_1x + \langle(x^2 + 1)\rangle \mid a_0, a_1 \in \mathbf{R}\ \}$.

Let $x + \langle(x^2 + 1)\rangle = t, \qquad 1 + \langle(x^2 + 1)\rangle = 1$. Observe that $1 + \langle(x^2 + 1)\rangle$ is the multiplicative identity of $F[x]/\langle(x^2 + 1)\rangle$, so this notation is not misleading.)

$t^2 = x^2+\langle(x^2 + 1)\rangle = x^2+1-1+\langle(x^2 + 1)\rangle = -1+\langle(x^2 + 1)\rangle = -1$ every element can be written uniquely of the form $F[x]/\langle(x^2 + 1)\rangle = \{a_0+a_1t \mid a_0, a_1 \in \mathbf{R},\ \ t^2 = -1\}$ addition and multiplication is defined as

$(a + bt) + (c + dt) = (a + c) + (b + d)t$
$(a + bt)(c + dt) = (ac - bd) + (ad + bc)t$
Define a homomorphism
$\varphi : \mathbf{C} \to F[x]/\langle(x^2 + 1)\rangle$
$a + bi \to a + bt.$

$(a+bi)+(c+di)=(a+c)+(b+d)i$

$$\begin{aligned}\varphi(a+bi)+(c+di))=\varphi(a+c)+(b+d)i) &= a+c+(b+d)t\\ &= a+bt+c+dt\\ &= \varphi(a+bi)+\varphi(c+di)\end{aligned}$$

$\varphi(a+bi)(c+di)=\varphi((ac-ba)+(ad+bc)i)$

$$\begin{aligned}&= (ac-bd)+(ad+bc)t\\ &= (a+bt)(c+dt)\\ &= \varphi(a+bi)\varphi(c+di)\end{aligned}$$

$Ker(\varphi)=\{a+bi\in\mathbf{C}\mid \varphi(a+bi)=a+bt=0\}=\{0\}$:

By the uniqueness of the writing in $F[x]/\langle(x^2+1)\rangle$ we have

$a+bt=0$ if and only if $a=0$ and $b=0$. Hence $Ker(\ \varphi)=\{0\}$

φ is onto as for any $a+bt\in F[x]/\langle(x^2+1)\rangle$, there exists $a+bi\in\mathbf{C}$ such that $\varphi(a+bi)=a+bt$. Hence φ is an isomorphism.

3.34. *If $f(x)$ is in $F[x]$, where F is the field of integers mod p, p a prime, and $f(x)$ is irreducible over F of degree n, prove that $F[x]/\langle$f(x)$\rangle$ is a field with p^n elements.*

Solution: The polynomial $f(x)$ is irreducible implies that the ideal generated by $f(x)$ is a maximal ideal and hence $F[x]/\langle f(x)\rangle$ is a field. Since $f(x)$ has degree n, for any $g(x)\in F[x]$ we have

$g(x)=f(x)h(x)+r(x)$ where $r(x)=0$ or $\deg r(x)<\deg f(x)$. By using similar methods we have

$F[x]/\langle f(x)\rangle=\{a_0+a_1x+\cdots+a_{n-1}x^{n-1}+\langle f(x)\ \rangle\ \mid\ a_i\in Z_p\}$ every element can be written uniquely in this form. Now it is easy to see that $F[x]/\langle f(x)\rangle$ has p^n elements.

3.35. *Prove that the polynomial $1+x+\cdots+x^{p-1}$ where p is a prime number, is irreducible over the field of rational numbers.*

Hint: Consider the polynomial

$$1+(x+1)+(x+1)^2+\cdots+(x+1)^{p-1}$$

Solution: First observe that $f(x) = 1 + x + \cdots + x^{p-1}$ reducible, if and only if $g(x) = 1 + (x+1) + \cdots + (x+1)^{p-1} = f(x+1)$ is reducible.

$$1 + (x+1) + \cdots + (x+1)^{p-1} = \frac{(x+1)^p - 1}{(x+1) - 1}$$

(in the field of fractions of $F[x]$).

$$\frac{(x+1)^p-1}{x} = \frac{x^p + \binom{p}{1} x^{p-1} + \binom{p}{2} x^{p-2} + \cdots + \binom{p}{p-1} x}{x}$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{p-1}$$

$\binom{p}{p-1} = p$. The constant term of $f(x+1)$ is p and is not divisible by p^2, also p does not divide the leading coefficient of this polynomial but divides each of the remaining coefficients. By Eisenstein Criterion the polynomial $1 + x + \cdots + x^{p-1}$ is an irreducible polynomial.

3.36. *If R is an integral domain, prove that for $f(x), g(x)$ in $R[x]$*

$$deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$$

Solution: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ where $a_n \neq 0$ and $b_m \neq 0$. Then $f(x)g(x) = a_n b_m x^{n+m} + \cdots + a_0 b_0$

Since R is an integral domain and a_n and b_m are non-zero we have $a_n b_m \neq 0$. Hence

$$\begin{aligned} n + m = \deg(f(x)g(x)) &= \deg f(x) + \deg(g(x)) \\ &= n + m \end{aligned}$$

3.37. *If R is an integral domain with unit element, prove that any unit in $R[x]$ must already be a unit in R.*

Solution: Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ and let $g(x) = b_m x^m + \cdots + b_1 x + b_0 \in R[x]$ be the inverse of $f(x)$ in $R[x]$. We need to show that $f(x) \in R$.

This is equivalent to say that $\deg f(x) = 0$. Since $\deg(f(x)g(x)) = \deg 1 = 0$ But by question 3.36 in an integral domain

$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

Since $\deg f(x), \deg g(x) \geq 0$ we have $\deg f(x) = 0$ and $\deg g(x) = 0$. Hence $f(x) \in R$ and $g(x) \in R$.

3.38. *Prove that $R[x]$ is a commutative ring with an identity element whenever R is.*

Solution: Let R be a commutative ring with an identity element and $f(x)$ and $g(x)$ be two elements in $R[x]$ say $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + \cdots + b_1 x + b_0$. Then

$f(x)g(x) = a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0$. since R is commutative we have

$= b_m a_n x^{n+m} + (b_{m-1} a_n + b_m a_{n-1}) x^{n+m-1} + \cdots + (b_0 a_1 + b_1 a_0)x + b_0 a_0$

$= g(x)f(x)$

Let 1 be the identity element of R. Then for any $f(x) \in R[x]$ $f(x) \cdot 1 = 1 \cdot f(x) = f(x)$. Hence 1 is also the unit element in $R[x]$.

3.39. *If R is a commutative ring, let $N = \{x \in R \mid x^n = 0$ for some integer $n\}$*

Prove:

a) N is an ideal of R.

b) In $\overline{R} = R/N$ if $(\overline{x})^m = 0$ for some m, then $\overline{x} = 0$.

Solution: Let $N = \{x \in R | x^n = 0$ for some integer n $\}$

Observe that n cannot be a negative integer because in order to talk negative power, x must be an invertible element, but if $(x^{-1})^n = x^{-n} = 0$, then multiplying by x^{n+1} we obtain that $x = 0$ which is impossible since x is invertible (i.e. zero and has an inverse is impossible).

Let $x, y \in N$. Then there exists $n, m > 0$ such that $x^n = 0$, $y^m = 0$. Since R is a commutative ring $(x-y)^{n+m} = \sum_{i=0}^{n+m} (-1)^i \begin{pmatrix} n+m \\ i \end{pmatrix} x^{n+m-i} y^i$

$$= x^{n+m} - \begin{pmatrix} n+m \\ 1 \end{pmatrix} x^{n+m-1} y + \cdots + (-1)^m \begin{pmatrix} n+m \\ m \end{pmatrix} x^n y^m + (-1)^{m+1} \begin{pmatrix} n+m \\ m+1 \end{pmatrix}$$

$$x^{n-1} y^{m+1} + \cdots + (-1)^{n+m} y^{n+m}$$

all powers $x^{n+j} = 0$, $j = 0 \cdots m$ and all powers $y^{m+k} = 0$, $k = 0, \cdots n$.

So we obtain $(x-y)^{n+m}=0$ i.e. $x-y\in N$

For any $r\in R, x\in N$ we have $(rx)^n=r^nx^n=0$ since $x^n=0$. Hence $rx\in N$. As R is a commutative ring $rx=xr\in N$. Hence N is an ideal of R.

b) By (a) $\overline{R}=R/N$ is a ring. Let $\overline{x}\in\overline{R}$. Then $(\overline{x})^m=0$ implies $x^m\in N$, but this implies there exists, n, such that $(x^m)^n=x^{mn}=0$. Therefore $x\in N$ i.e. $\overline{x}=0$.

3.40. *If A and B are ideals in a ring R such that $A\cap B=(0)$, prove that for every $a\in A, b\in B,\ ab=0$.*

Solution: Let $a\in A$ and $b\in B$. Then

$ab\in A$ as A is an ideal

$ab\in B$ as B is an ideal

Hence $ab\in A\cap B=\{0\}$

3.41. *Find all $c\in\mathbf{Z}_3$ such that $\mathbf{Z}_3[x]/\langle x^3+cx^2+1\rangle$ is a field.*

Solution: $Z_3[x]/\langle x^3+cx^2+1\rangle$ is a field if and only if the ideal generated by x^3+cx^2+1 is maximal ideal if and only if x^3+cx^2+1 is irreducible in $Z_3[x]$. Let $f(x)=x^3+cx^2+1$ since $f(x)$ has degree 3, if $f(x)$ is reducible then one of the factor should have degree one i.e $f(x)$ should have a root in Z_3.

$f(0)=1\neq 0\ (\mod 3)$

$f(1)=2+c$

$f(2)=9+c\equiv c\ (\mod 3)$

So, if $c\not\equiv 0$ and $c\not\equiv 1$ in Z_3, then $f(x)$ is irreducible. So for $c\equiv 2$, $f(x)$ is irreducible.

3.42. *Show that if F is a field, then $\langle(x)\rangle$ is a maximal ideal in $F[x]$, but it is not the only maximal ideal.*

Solution: Let F be a field. Define a map ψ from $F[x]$ to F such that

$$\psi(a_nx^n+\cdots+a_1x+a_0)=a_0$$

ψ is a ring homomorphism

Let $f(x)=a_nx^n+\cdots+a_1x+a_0$ and $g(x)=b_mx^m+\cdots+b_1x+b_0$.

Then $\psi(f(x)+g(x))=\psi(f(x))+\psi(g(x))=a_0+b_0$

$\psi(f(x)g(x)) = \psi(f(x))\psi(g(x)) = a_0b_0$.
$Ker\psi = \{f(x) \in F[x] \mid \psi(f(x)) = 0\}$
= The set of all polynomials with constant term zero.
$= \langle(x)\rangle$.

Since $F[x]/\langle(x)\rangle \cong F$ we see that $\langle(x)\rangle$ is a maximal ideal. But $\langle(x)\rangle$ is not the only maximal ideal because every ideal generated by an irreducible polynomial is a maximal ideal, for example the ideal $\langle(x+a)\rangle$ is also maximal for all $a \in F$.

3.43. *Let R be a ring containing $\mathbf{Z}$ as a subring. Prove that if integers m, n are contained in a proper ideal of R, then they have a common factor > 1.*

Solution: Let R be a ring containing $\mathbf{Z}$ as a subring. Let I be a proper ideal of R and $m, n \in I$. Assume if possible that m and n do not have a common factor greater than 1. Then they are relatively prime. Hence there exist $x, y \in \mathbf{Z}$ such that $xm + ny = 1$. Since $n, m \in I$ we have xm and $ny \in I$. But this implies $1 \in I$, which is a contradiction, since I is a proper ideal.

3.44. *Let R be a commutative ring; an ideal P of R is said to be a* prime ideal *of R if $ab \in P$, for $a, b \in R$ implies that $a \in P$ or $b \in P$. Prove that P is a prime ideal of R if and only if R/P is an integral domain.*

Solution: Assume that P is a prime ideal and consider R/P. Let $a + P$ and $b + P$ be two elements in R/P and $(a + P)(b + P) = P$ i.e. $ab + P = P$. This implies $ab \in P$, then either $a \in P$ or $b \in P$. Therefore either $a + P = P$ or $b + P = P$. Hence R/P is an integral domain.

Conversely assume that R/P is an integral domain and $ab \in P$. Then $(a + P)(b + P) = ab + P = P$. Since R/P is an integral domain either $a + P = P$ or $b + P = P$. Hence either $a \in P$ or $b \in P$.

3.45. *Let R be a commutative ring with unit element; prove that every maximal ideal of R is a prime ideal.*

Solution: Let R be a commutative ring with unit element and let M be a maximal ideal. Then R/M is a field in particular it is an integral domain. Hence by question 3.44 M is a prime ideal.

3.46. *Give an example of a ring in which some prime ideal is not a maximal ideal.*

Solution: Let $R = \mathbf{Z} + \mathbf{Z}$ be the direct sum of the ring of integers. Let $I = 0 + \mathbf{Z}$ be an ideal of R. Now R/I is a prime ideal since R/I is isomorphic to $\mathbf{Z}$ which is an integral domain. But I is not a maximal ideal since R/I is isomorphic to $\mathbf{Z}$. Since $\mathbf{Z}$ is not a field we obtain I is not a maximal ideal.

An integral domain R is said to be a **Euclidean ring** if for every $a \neq 0$ in R there is defined a non-negative integer $d(a)$ such that
(1) For all $a, b \in R$ both non-zero, $d(a) \leq d(ab)$.
(2) For any $a, b \in R$ both non-zero, there exists $t, r \in R$ such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.

3.47. *Prove that a necessary and sufficient condition that the element a in the Euclidean ring be a unit is that $d(a) = d(1)$.*

Solution: Assume that a is a unit then there exist $b \in R$ such that $ab = ba = 1$. Since R is a Euclidean ring for any $a \in R$, we have $d(a) \leq d(ab) = d(1)$. Conversely $d(1) \leq d(1a) = d(a)$ Hence $d(a) = d(1)$.

Now assume that $d(a) = d(1)$. Since 1 and a are elements of R there exists $b, r \in R$ such that $1 = ab + r$ where $d(r) < d(a)$ or $r = 0$. So either $r = 0$ or $d(r) < d(a) = d(1)$. But $d(1) \leq d(r)$. Hence we must have $r = 0$, this implies that $1 = ab$ and a is a unit as R is a commutative ring $ab = ba = 1$.

3.48. *Let R be a commutative ring and suppose that A is an ideal of R. Let $N(A) = \{x \in R \mid x^n \in A \text{ for some } n\}$. Prove*
(a) $N(A)$ is an ideal of R which contains A.
(b) $N(N(A)) = N(A)$.
*The ideal $N(A)$ is often called the **radical of** A.*

Solution: (a) Let x and y be two elements of $N(A)$. Then there exists n and m such that $x^n \in A$ and $y^m \in A$. Consider $(x - y)^{n+m}$. Since R is a commutative ring we have

$$(x-y)^{n+m} = \sum_{i=0}^{n+m} \begin{pmatrix} n+m \\ i \end{pmatrix} (-1)^i x^{n+m-i} y^i$$

$$= x^{n+m} + \begin{pmatrix} n+m \\ 1 \end{pmatrix} (-1)^1 x^{n+m-1} y + \cdots + \begin{pmatrix} n+m \\ m \end{pmatrix}$$
$$(-1)^m x^n y^m + \cdots + \begin{pmatrix} n+m \\ n+m \end{pmatrix} (-1)^{n+m} y^{n+m}.$$

$x^n \in A$ and A is an ideal implies $x^n y^i \in A$ for all i and by the same property $y^m \in A$ implies $x^j y^m \in A$. Since A is an ideal the sum of the elements in A is again in A. Hence $x - y \in N(A)$.

Let r be any element in R. Then $(rx)^n = r^n x^n \in A$ as $x^n \in A$ and A is an ideal.

Therefore $N(A)$ is an ideal of R. For any $a \in A$, $a^1 \in A$. Hence $N(A) \supseteq A$.

(b) It is clear that $N(A) \subseteq N(N(A))$. Let $x \in N(N(A))$. Then there exists n such that $x^n \in N(A)$. Then there exists m such that $x^{nm} \in A$. Hence $x \in N(A)$. i.e. $N(N(A)) \subseteq N(A)$. Therefore we have the equality.

3.49. *If R is a ring, let $Z(R) = \{x \in R \mid xy = yx \text{ all } y \in R\}$. Prove that $Z(R)$ is a subring of R.*

Solution: Clearly $0 \in Z(R)$, so $Z(R) \neq \emptyset$. Let $x, y \in Z(R)$ and let $r \in R$.

$(x - y)r = xr - yr$. Since x and y are in the center this is equal to $rx - ry = r(x - y)$. So $x - y \in Z(R)$. Now $(xy)r = x(yr) = x(ry) = (xr)y = r(xy)$ for all $r \in R$.

Hence $xy \in Z(R)$.

3.50. *If R is a division ring, prove that $Z(R)$ is a field.*

Solution: We have shown in question 3.49 that $Z(R)$ is a subring of R. It is clear that $Z(R)$ is a commutative ring. So it is enough to show that every non-zero element in $Z(R)$ has an inverse in $Z(R)$.

But this follows from the given fact that R is a division ring. Hence every non-zero element in R has an inverse in R. We show if $0 \neq x \in Z(R)$, then x^{-1} is also in $Z(R)$. For any $r \in R$ we have $xr = rx$. Since x^{-1} exists for any $r \in R$ we multiply this equation from left and right by x^{-1}. We have $rx^{-1} = x^{-1}r$. Hence $x^{-1} \in Z(R)$.

3.51. *Find a polynomial of degree* 3 *irreducible over the ring of integers,* $\mathbf{Z_3}$, mod 3. *Use it to construct a field having* 27 *elements.*

Solution: $f(x) = x^3 + x^2 + 2$ is an irreducible polynomial in $\mathbf{Z}_3[x]$. Since $f(x)$ is of degree 3, if $f(x)$ is reducible, then one of the factors must be of degree 1. This implies that $f(x)$ has a root in $\mathbf{Z}_3$. But
$f(0) = 2$
$f(1) = 1$
$f(2) = 1$

Let $I = \langle (x^3 + x^2 + 2) \rangle$ be an ideal of $\mathbf{Z}_3[x]$. Since $f(x)$ is irreducible I is a maximal ideal in $\mathbf{Z}_3[x]$ and hence $\mathbf{Z}_3[x]/I$ is a field. Every element in $\mathbf{Z}_3[x]/I$ can be written uniquely in the form $a_0 + a_1 x + a_2 x^2 + I$, for some $a_0, a_1, a_2 \in \mathbf{Z}_3$. Now it is easy to see that there are 27 elements in this form.

3.52. *Construct a field having 625 elements.*

Solution: All we need to find is an irreducible polynomial $f(x)$ of degree 4 over $\mathbf{Z}_5$ and as in question 3.51 the field $\mathbf{Z}_5[x]/\langle f(x) \rangle$ will be a field with 625 elements. Existence of such a polynomial is well known as for any prime power, there exists a unique (up to isomorphism) finite field of that given prime power order.

3.53. *Prove that the polynomial* $f(x) = 1 + x + x^3 + x^4$ *is not irreducible over any field* F.

Solution: $f(x) = 1 + x + x^3 + x^4$ is not irreducible because $f(-1) = 1 - 1 - 1 + 1 = 0$. Hence $x + 1$ is a factor of $1 + x + x^3 + x^4$ in any $F[x]$, for any field F.

3.54. *Prove that the polynomial* $f(x) = x^4 + 2x + 2$ *is irreducible over the field of rational numbers.*

Solution: $f(x) = x^4 + 2x + 2$ is irreducible by Eisenstein criterion.

3.55. *Prove that any nonzero ideal in the Gaussian integers* $\mathbf{Z}[i]$ *must contain some positive integer.*

Solution: Let I be a non zero ideal in $\mathbf{Z}[i]$ and let $m + ni \in I$ for some $m, n \in \mathbf{Z}$. Since I is an ideal $(m + ni)(m - ni) \in I$. Hence $m^2 + n^2 \in I$ and $m^2 + n^2 \in \mathbf{Z}$ and positive as either m or n is nonzero.

3.56. *In a Euclidean ring prove that any two greatest common divisors of a and b are associates.*

Solution: Assume that d_1 and d_2 are greatest common divisors of a and b. Since d_1 is a greatest common divisor and d_2 divides both a and b, d_2 divides d_1 similarly d_1 divides d_2 Hence $d_1 = d_2x$ and $d_2 = d_1y$. We obtain $d_1 = d_1yx$.

Since R is a Euclidean ring it has an identity and it is an integral domain. $d_1(1 - yx) = 0$ implies $yx = 1$. So x is unit and $d_1 = d_2x$. Hence d_1 and d_2 are associates.

4. FIELDS

4.1. *Prove that the mapping $\psi : F[x] \to F(a)$ defined by $\psi(h(x)) = h(a)$ is a homomorphism.*

Solution: Let $f(x), h(x)$ be two elements in $F[x]$. Then $\psi(f(x) + h(x)) = \psi(f + g)(x) = (f + g)(a) = f(a) + g(a) = \psi(f(x)) + \psi(h(x))$. Moreover $\psi(f(x)h(x)) = \psi(f+g)(x) = (fg)(a) = f(a)g(a) = \psi(f(x))\psi(h(x))$.

Hence ψ is a homomorphism.

4.2. *Let F be a field and let $F[x]$ be the ring of polynomials in x over F. Let $g(x)$ of degree n, be in $F[x]$ and let $I = \langle g(x)\rangle$ be the ideal generated by $g(x)$ in $F[x]$. Prove that $F[x]/I$ is an $n-$dimensional vector space over F.*

Solution: $F[x]/I = \{f(x) + I \ \mid \ f(x) \in F[x] \ \}$.

I is the ideal generated by the polynomial $g(x)$ of degree n. Since $F[x]$ is a Euclidean ring there exists $h(x)$ and $r(x) \in F[x]$ such that

$f(x) = g(x)h(x)+r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Group structure of $F[x]/I$ is already known. For any $\lambda \in F$, and $f(x) + I \in F[x]/I$ define $\lambda(f(x) + I) = \lambda f(x) + I$, with this addition and multiplication by an element of F, the set $F[x]/I$ forms a vector space over the field F. Every element of $F[x]/I$ can be written uniquely as a linear combination of the elements $1 + I, x + I, \cdots, x^{n-1} + I$

Indeed let

$$f(x) + I = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + I = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + I$$

Then $(a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1} \in I$.

But every non-zero element in I has degree $\geq n$. Hence $a_0-b_0+(a_1-b_1)x+\cdots+(a_{n-1}-b_{n-1})x^{n-1} = 0$. Then $a_i = b_i$ for all $i = 0, \cdots, n-1$.

Therefore the set $\{1+I, x+I, \cdots, x^{n-1}+I\}$ forms a basis for the vector space $F[x]/I$ of dimension n.

On the other hand, it is clear that every element in $F[x]/I$ can be written as a linear combination of the above elements.

4.3. *(a) Let* $\mathbf{R}$ *be the field of real numbers and* $\mathbf{Q}$ *the field of rational numbers. In* $\mathbf{R}$, $\sqrt{2}$ *and* $\sqrt{3}$ *are both algebraic over* $\mathbf{Q}$. *Exhibit a polynomial of degree* 4 *over* $\mathbf{Q}$ *satisfied by* $\sqrt{2}+\sqrt{3}$.

(b) What is the degree of $\sqrt{2}+\sqrt{3}$ *over* $\mathbf{Q}$? *Prove your answer.*

(c) What is the degree of $\sqrt{2}\sqrt{3}$ *over* $\mathbf{Q}$?

Solution: Let $x = \sqrt{2}+\sqrt{3}$ then $x^2 = 2+3+2\sqrt{6}$ and

$$x^2 - 5 = 2\sqrt{6}$$

$$(x^2-5)^2 = 4 \cdot 6$$

$$x^4 - 10x^2 + 25 = 24$$

$$x^4 - 10x^2 + 1 = 0$$

$f(x) = x^4 - 10x^2 + 1 \in \mathbf{Q}[x]$ has $\sqrt{2}+\sqrt{3}$ as a root.

(b) $f(x)$ is an irreducible polynomial in $\mathbf{Q}[x]$. Firstly $f(x)$ does not have any root in $\mathbf{Q}$ because the only possible roots in $\mathbf{Q}$ are ∓ 1 but $f(\pm 1) \neq 0$. On the other hand $f(x)$ cannot be factored as a product of polynomials of degree 2. One can see this by substituting $t = x^2$ in the above equation.

Hence $[\mathbf{Q}(\sqrt{2}+\sqrt{3}) : \mathbf{Q}] = 4$.

(c) Let $x = \sqrt{2}\sqrt{3}$ then $x^2 = 2 \cdot 3$. Hence $f(x) = x^2 - 6$ is satisfied by $\sqrt{2}\sqrt{3}$ and by Eisenstein criterion $f(x)$ is irreducible. Hence

$$[\mathbf{Q}(\sqrt{2}\sqrt{3}) : \mathbf{Q}] = 2$$

4.4. *With the same notation as in Question 4.3 show that* $\sqrt{2}+\sqrt[3]{5}$ *is algebraic over* $\mathbf{Q}$ *of degree 6.*

Solution: Let $a = \sqrt{2}+\sqrt[3]{5}$. Then $(a-\sqrt{2})^3 = 5$. We get

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

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

So

$a^6 - 6a^4 - 10a^3 + 12a^2 - 60a + 17 = 0$

Now if one goes backwards finds that the polynomial $p(x) = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$ satisfies a.

Now we need to show that $[\mathbf{Q}(a) : \mathbf{Q}] = 6$. We will show that the possibilities $[\mathbf{Q}(a) : \mathbf{Q}) = 3$ or $[\mathbf{Q}(a) : \mathbf{Q}] = 2$ cannot occur. Then we conclude that $[\mathbf{Q}(a) : \mathbf{Q}] = 6$.

Let $F = \mathbf{Q}(\sqrt[3]{5}, \sqrt{2})$.

$[\mathbf{Q}(a, \sqrt{2}), \mathbf{Q}] = [\mathbf{Q}(a, \sqrt{2}) : \mathbf{Q}(\sqrt{2})]\ [\mathbf{Q}(\sqrt{2}), \mathbf{Q}] = 6$. If $[\mathbf{Q}(a) : \mathbf{Q}] = 3$, then $[\mathbf{Q}\underbrace{(a, \sqrt[3]{5}) : \mathbf{Q}(a)}_{2}]\ \underbrace{[\mathbf{Q}(a) : \mathbf{Q}]}_{3} = 6$

There exists $p(x) \in \mathbf{Q}(a)[x]$ such that $p(\sqrt[3]{5}) = 0$ The polynomial $p(x)$ is irreducible and of degree 2. But $p(x)$ must divide $x^3 - 5$, since $x^3 - 5$ satisfies $\sqrt[3]{5}$. This implies the polynomial $x^3 - 5$ must have a root in $\mathbf{Q}(a) \subseteq \mathbf{R}$, but $x^3 - 5$ has only one real root in $\mathbf{R}$, namely $\sqrt[3]{5}$. This implies $\sqrt[3]{5} \in \mathbf{Q}(a)$, this is impossible as $\mathbf{Q}(a, \sqrt[3]{5}) = F$ and $[F : \mathbf{Q}] = 6$. Hence the possibility $[\mathbf{Q}(a) : \mathbf{Q}] = 3$ cannot occur.

If $[\mathbf{Q}(a) : \mathbf{Q}] = 2$, then

$$[\mathbf{Q}(a, \sqrt{2}) : \mathbf{Q}(a)][\mathbf{Q}(a) : \mathbf{Q}] \leq 4$$

$x^2 - 2 \in \mathbf{Q}(a)[x]$ and satisfies $\sqrt{2}$. Then either $\sqrt{2} \in \mathbf{Q}(a)$ or $[\mathbf{Q}(a, \sqrt{2}) : \mathbf{Q}(a)] = 2$ certainly $\sqrt{2} \notin \mathbf{Q}(a)$, otherwise $\sqrt[3]{5} \in \mathbf{Q}(a)$ and hence $\mathbf{Q}(a) = \mathbf{Q}(\sqrt[3]{5}, \sqrt{2}) = F$ and this is impossible as $[F : \mathbf{Q}] = 6$. Hence $[\mathbf{Q}(a, \sqrt{2}) : \mathbf{Q}] = 4$ which is impossible.

Hence $[\mathbf{Q}(a) : \mathbf{Q}] = 6$ and $\mathbf{Q}(a) = F$.

4.5. *Suppose that F is a field having a finite number of elements, q and K is an extension of F.*

(a) Prove that there is a prime number p such that $pa = \underbrace{a + a + \cdots + a}_{p-times} = 0$ for all $a \in F$.

(b) Prove that $q = p^n$ for some integer n.

(c) If $a \in F$, prove that $a^q = a$.

(d) If $b \in K$ is algebraic over F, prove $b^{q^m} = b$ for some $m > 0$.

An algebraic number a is said to be an **algebraic integer** if it satisfies an equation of the form $a^m + \alpha_1 a^{m-1} + \cdots + \alpha_m = 0$, where $\alpha_1, \cdots, \alpha_m$ are integers.

Solution: Let F be a finite field with q elements.

Since q is the order of F with respect to addition, for any $a \in F$, $q.a = 0$. In particular $q.1 = 0$.

If q is not a prime say $q = m.n$ then $q.1 = m.1n.1 = 0$. Since F is a field either $m.1 = 0$ or $n1 = 0$. Continuing like this we will reach the smallest number n such that $n.1 = 0$ and n is not a composite. i.e. n is a prime number and for any $a \in F \quad n.a = (n.1)a = 0$

(b) Every finite field is a vector space over the field $\mathbf{Z}_p$ with p elements for some prime p. If the dimension is n, then every element in F can be written uniquely in the form $a_1u_1 + \cdots + a_nu_n$ where $a_i \in Z_p$, and $\{u_1, \ldots, u_n\}$ be a basis for F over $\mathbf{Z}_p$

Hence the number of elements in F is p^n.

(c) We know that every finite field forms a cyclic group with respect to multiplication. Hence for any non-zero element $a^{q-1} = 1$. Hence $a^q = a$. This is true for zero element as well. Hence $a^q = a$ for all $a \in F$.

(d) Let b be an algebraic element over F. Then there exists an irreducible polynomial $f(x)$ in $F[x]$ such that b is a root of $f(x)$. If $\deg f(x) = m$, then $F(b)$ is a finite extension of F and $|F(b)| = |F|^m = q^m$. Hence by (c) $b^{q^m} = b$.

4.6. *If α is any algebraic number, prove that there is a positive integer n such that $n\alpha$ is an algebraic integer.*

Solution: Let α be an algebraic number. Let $f(x) = a_kx^k + \cdots + a_1x + a_0$ be a polynomial in $\mathbf{Q}[x]$ such that

$$f(\alpha) = a_k\alpha^k + \cdots + a_1\alpha + a_0 = 0$$

since $a_i \in \mathbf{Q}$ multiplying by a_k^{-1} we may assume that $a_k = 1$

Now let $a_i = \frac{m_i}{n_i}$, where $m_i, n_i \in \mathbf{Z}$ and $i = 0, 1, \cdots, k-1$. Let $s = lcm(n_i; i = 0, 1, \cdots k-1)$. Then multiply both side of $f(x)$ by $s^k = n$. we get

$$s^k\alpha^k + a_{k-1}s.s^{k-1}\alpha^{k-1} + \cdots + a_1s^{k-1}s\alpha + a_0s^k = 0$$

i.e

$$(s\alpha)^k + a_{k-1}s(s\alpha)^{k-1} + \ldots + a_1s^{k-1}(s\alpha) + a_0s^k = 0$$

Observe that $a_i s \in \mathbf{Z}$ as s is the least common multiple of n_i, $\quad i = 0, \cdots, k-1$. Hence $s\alpha$ satisfies the polynomial $x^k + a_{k-1}sx^{k-1} + \ldots a_1 s^{k-1}x + a_0 s^k$.

4.7. *If the rational number r is also an algebraic integer, prove that r must be an ordinary integer.*

Solution: Let $r \in \mathbf{Q}$ and let r be an algebraic integer as well. Then $r = m/k$ where $m, k \in \mathbf{Z}$. Since r is an algebraic integer, there exists an equation $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$ where

$a_i \in \mathbf{Z}, \quad i = 0, \cdots a_{n-1}$. Substitute $r = \frac{m}{k}$ and by cancelling out the common multiplies of m and k we may assume that $(m, k) = 1$.

$$\frac{m^n}{k^n} + a_{n-1}\frac{m^{n-1}}{k^{n-1}} + \cdots + a_1\frac{m}{k} + a_0 = 0$$

$$m^n + a_{n-1}m^{n-1}k + \cdots + a_1 mk^{n-1} + a_0 k^n = 0$$

Let p be a prime which divides k. Then

$m^n = k(a_{n-1}m^{n-1} + \cdots + a, mk^{n-2} + a_0 k^{n-1})$. Then p divides m^n, hence p divides m. But then $1 = (m, k) > p$. Hence $k = 1$ and r becomes an integer.

4.8. *If a is an algebraic integer and m is an ordinary integer, prove*

(a) $a + m$ is an algebraic integer.

(b) ma is an algebraic integer.

Solution: (a) Let a be an algebraic integer. Then there exists a polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $\mathbf{Z}[x]$ such that $f(a) = 0, \quad a_i \in \mathbf{Z}, \quad i = 0, 1, 2, \ldots, n-1$. Consider the polynomial $g(x) = f(x - m)$.

Since m is an integer $f(x - m) \in \mathbf{Z}[x]$ and substitute for $x = a + m$ we get $g(a + m) = f(x) = 0$. Hence $a + m$ is an algebraic integer.

b) $a^n + a_{n-1}a^{n-1} + \cdots + a_1 a + a_0 = 0 \qquad$ where $\quad a_i \in \mathbf{Z}, \quad i = 0, \cdots, n-1$, multiply now both side by m^n we obtain

$$m^n a^n + a_{n-1}mm^{n-1}a^{n-1} + \cdots + a_1 m^{n-1}ma + a_0 m^n = 0$$

$$(ma)^n + a_{n-1}m(ma)^{n-1} + \cdots + a_1m^{n-1}(ma) + a_0m^n = 0$$

Hence ma is an algebraic integer.

4.9. *If E is an extension of F and if $f(x) \in F[x]$ and if ψ is an automorphism of E leaving every element of F fixed, prove that ψ must take a root of $f(x)$ lying in E into a root of $f(x)$ in E.*

Solution: Let $a \in E$ and $f(x) = a_nx^n + \cdots + a_1x + a_0$ be a polynomial in $F[x]$ such that $f(\alpha) = 0$. Then $\psi(f(\alpha)) = \psi(a_n\alpha^n + \cdots + a_1\alpha + a_0) = \psi(0) = 0 = a_n\psi(\alpha^n) + \cdots + a_1\psi(\alpha) + a_0$ since ψ fixes a_i and ψ is an automorphism, we have $\psi(f(\alpha)) = a_n\psi(\alpha)^n + \cdots + a_1\psi(\alpha) + a_0 = 0$.

Therefore $f(\psi(\alpha)) = 0$

Hence $\psi(\alpha)$ as a root of $f(x)$ and is $\alpha \in E$ and since ψ an automorphism of E we have $\psi(\alpha) \in E$.

4.10. *Prove that $F(\sqrt[3]{2})$, where F is the field of rational numbers, has no automorphisms other than the identity automorphism.*

Solution: Observe first that the only field automorphism of $\mathbf{Q}$ is the trivial automorphism. Indeed let ψ be a field automorphism of $\mathbf{Q}$. Then $\psi(1) = 1$ and $\psi(n) = n$ for all $n \in \mathbf{Z}$. As ψ is a field automorphism

$$\begin{aligned}
\psi(\frac{m}{n}) &= \psi(m)\psi(\frac{1}{n}) \\
&= \psi(m)\psi(n^{-1}) \\
&= \psi(m)\psi(n)^{-1} \\
&= mn^{-1} = \frac{m}{n}
\end{aligned}$$

Hence ψ is the identity automorphism. Now let $E = F(\sqrt[3]{2})$. Then $\sqrt[3]{2}$ satisfies the polynomial $x^3 - 2 \in F[x]$. Let ψ be an automorphism of E. Then by Question 4.9 $\psi(\sqrt[3]{2})$ is also a root of $x^3 - 2$. But $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{2^2})$. But the roots of the second polynomial of degree two are complex. Hence they are not contained in E. Therefore $\psi(\sqrt[3]{2}) = \sqrt[3]{2}$. Therefore ψ fixes every element in E. i.e. ψ is identity.

4.11. *Prove that if the complex number α is a root of the polynomial $p(x)$ having* real *coefficients then $\overline{\alpha}$, the complex conjugate of α, is also a root of $p(x)$.*

Solution: Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ where $a_i \in \mathbf{R}$. Then $p(\alpha) = 0$ implies

$p(\alpha) = a_n\alpha^n + a_{n-1} + \alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$

Take conjugate of both sides we get,

$$\overline{p(\alpha)} = \overline{a_n}\overline{\alpha}^n + \overline{a_{n-1}}\overline{\alpha}^{n-1} + \cdots + \overline{a_1}\overline{\alpha} + \overline{a_0} = 0$$

using $(\overline{\alpha^n}) = (\overline{\alpha})^n$ and sum of the conjugates is conjugate of the sums and $a_i \in \mathbf{R}$ we have

$\overline{p(\alpha)} = a_n\overline{\alpha}^n + \cdots + a_1\overline{\alpha} + a_0 = 0.$

Hence $p(\overline{\alpha}) = \overline{p(\alpha)} = 0$. i.e. $\overline{\alpha}$ is a root of the polynomial $p(x)$.

4.12. *Prove that if m is an integer which is not a perfect square and if $\alpha + \beta\sqrt{m}$ $(\alpha, \beta$ rational) is the root of a polynomial $p(x)$ having* rational coefficients, *then $\alpha - \beta\sqrt{m}$ is also a root of $p(x)$.*

Solution: Let $p(x) = a_n x^n + \cdots + a_n x + a_0 \in \mathbf{Q}[x]$ and let $p(\alpha + \beta\sqrt{m}) = 0$

Since $\alpha, \beta \in \mathbf{Q}$ and m is not a perfect square $\sqrt{m} \notin \mathbf{Q}$. Now consider $\mathbf{Q}(\sqrt{m})$. Define a map ψ from $\mathbf{Q}(\sqrt{m})$ to $\mathbf{Q}(\sqrt{m})$ such that

$\psi : \mathbf{Q}(\sqrt{m}) \to \mathbf{Q}(\sqrt{m})$

$a + b\sqrt{m} \to a - b\sqrt{m}$

ψ is a field automorphism of $\mathbf{Q}(\sqrt{m})$ and ψ fixes every element of $\mathbf{Q}$. Indeed

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

$$\begin{aligned} &= a + c - (b + d)\sqrt{m} \\ &= a - b\sqrt{m} + c - d\sqrt{m} \\ &= \psi(a + b\sqrt{m}) + \psi(c + d\sqrt{m}) \end{aligned}$$

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

$= ac + bdm - (ad + bc)\sqrt{m}$

$= (a - b\sqrt{m})(c - d\sqrt{m}) = \psi(a + b\sqrt{m})\psi(c + d\sqrt{m})$. Moreover

$Ker\ \psi = \{a + b\sqrt{m} \mid \ a - b\sqrt{m} = 0\} = \{0\}$

Clearly ψ is onto. Hence ψ is an automorphism of $\mathbf{Q}(\sqrt{m})$.

Now by question 4.9 if $\alpha + \beta\sqrt{m}$ is a root of a polynomial $p(x)$ and ψ is an automorphism of $\mathbf{Q}(\sqrt{m})$ then $\psi(\alpha+\beta\sqrt{m}) = \alpha - \beta\sqrt{m}$ is also a root of $p(x)$.

4.13. *Let R be a commutative ring and let A be any subset of R. Show that the annihilator of A, namely $Ann(A) = \{r \in R \mid ra = 0$ for all $a \in A\}$, is an ideal.*

Solution: Let $r, s \in Ann(A)$ and let a be any element of A. We have $ra = 0$ and $sa = 0$. Then $(r - s)a = ra - sa = 0$ and for any $x \in R, \quad (rx)a = (xr)a = x(ra) = 0$. Since R is commutative we have $Ann(A)$ is an ideal.

4.14. *Let*

$$R = \left\{ \left[\begin{array}{cc} a & b \\ c & d \end{array} \right] \middle| \ a, b, c, d \in \mathbf{Z}_2 \right\}$$

with ordinary matrix addition and multiplication modulo 2. Show that

$$\left\{ \left[\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right] r \ \middle| \ \ r \in R \right\}$$

is not an ideal of R.

Solution : $S = \{ \left[\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right] r \ \mid \ r \in R\}$

$$= \left\{ \left[\begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right] \left[\begin{array}{cc} a & b \\ c & d \end{array} \right] \mid \ \ a, b, c, d \in \mathbf{Z}_2 \right\} = \left\{ \left[\begin{array}{cc} a & b \\ 0 & 0 \end{array} \right] | a, b, \in \mathbf{Z}_2 \right\} \Bigg\}$$

For any $s_1, s_2 \in S$ we have $s_1 - s_2 \in S$ but for any $\left[\begin{array}{cc} x & y \\ z & w \end{array} \right]$ in R

$$\left[\begin{array}{cc} x & y \\ z & w \end{array} \right] \left[\begin{array}{cc} a & b \\ 0 & 0 \end{array} \right] = \left[\begin{array}{cc} ax & bx \\ az & wb \end{array} \right]$$

choose $a = 1, \ \ b = 1, \ \ x = 1, \ \ y = 1 \ \ z = 1, \ \ w = 1$ then

$$\left[\begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \right] \left[\begin{array}{cc} 1 & 1 \\ 0 & 0 \end{array} \right] = \left[\begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \right] \notin S.$$

Hence S is not an ideal.

4.15. *a) Show that the homomorphic image of a principal ideal ring is a principal ideal ring.*

b) Let R and S be commutative rings with unity. If ψ is a homomorphism from R onto S and the characteristic of R is nonzero, prove that the characteristic of S divides the characteristic of R.

Solution: (a) Let R be a principal ideal ring and S be a homomorphic image of R. Let ψ be the homomorphism, and let J be an ideal of S. Then $\psi^{-1}(J) = I$ is an ideal of R. Since R is a principal ideal ring, there exists $a \in I$ such that $I = (a)$. Let $s \in J$. Since ψ is onto there exists $r \in R$ such that $\psi(r) = s$, and so $r \in I$. Then $r = ax$ for some $x \in R$. Hence $s = \psi(r) = \psi(ax) = \psi(a)\psi(x)$. Hence every element of J is a product of an element from S with the element $\psi(a)$. Hence $J = \langle \psi(a) \rangle$.

(b) Let n be a characteristic of R. Let s be any element of S. Then there exists $r \in R$ such that $\psi(r) = s$. But then $0 = \psi(n.r) = \psi((n.1) \cdot r) = \psi(n.1)\psi(r) = n.s$ We used here that $\psi(1_R) = 1_S$ as ψ is onto. Hence for any $s \in S, ns = 0$ i.e. Characteristic of S divides characteristic of R as characteristic of S is the minimal positive integer satisfying $na = 0$ for all $a \in S$.

4.16. *Let S be a set, R a ring and $f : S \to R$ a bijective mapping. For each $x, y \in S$ define*

$$x + y = f^{-1}(f(x) + f(y)) \quad \textit{and} \quad xy = f^{-1}(f(x)f(y))$$

Do these sum and product define a ring structure on S? Prove your answer.

Yes they do define an abelian group and a multiplication on S and so a ring structure on S. We will show only $f^{-1}(0)$ is the identity element of S with respect to addition and S is abelian with respect to addition.

Indeed let x be an arbitrary element of S. Then there exists an element $r \in R$ such that $f^{-1}(r) = x$. Then $x + f^{-1}(0) = f^{-1}(f(x) + 0) =$

$f^{-1}(r+0) = f^{-1}(r) = x$. Similarly one can show that $f^{-1}(0) + x = x$. Now for $x, y \in S$. we have $x + y = f^{-1}(f(x) + f(y)) = f^{-1}(f(y) + f(x)) = y + x$. Hence S is an abelian group.

The other properties can be shown similarly.

4.17. *Let R be a commutative ring. A map $D : R \to R$ is called a derivation if $D(x+y) = D(x) + D(y)$ and $D(xy) = D(x)y + xD(y)$ for all $x, y \in R$. If D_1, D_2 are derivations, define the bracket product $[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$. Show that $[D_1, D_2]$ is a derivation.*

Solution: For the solution just apply the definition and show that $[D_1, D_2](x+y) = D_1 \circ D_2 - D_2 \circ D_1(x+y) = [D_1, D_2](x) + [D_1, D_2](y)$ and $[D_1, D_2](xy) = [D_1, D_2](x)y + x[D_1, D_2](y)$.

4.18. *Let K be a field and $f : \mathbf{Z} \to K$ the homomorphism of integers into K.*

a) Show that the kernel of f is a prime ideal. If f is an embedding, then we say that K has characteristic zero.

b) If $kerf \neq \{0\}$, show that $kerf$ is generated by a prime number p. In this case we say that K has characteristic p.

Solution: Recall that kernel of any ring homomorphism is an ideal. Hence $Ker(f)$ is an ideal of $\mathbf{Z}$. Then the ideal $Ker(f)$ is a prime ideal if and only if $\mathbf{Z}/Ker(f)$ is an integral domain. Indeed if $xKer(f), yKer(f)$ are in $\mathbf{Z}/Ker(f)$ and $xKer(f)yKer(f) = Ker(f)$. Then $xy \in Ker(f)$, then $f(xy) = f(x)f(y) = 0$. But K is a field either $f(x) = 0$ or $f(y) = 0$. i.e. either $x \in Ker(f)$ or $y \in Ker(f)$. Hence $\mathbf{Z}/Ker(f)$ is an integral domain.

On the other hand if $Ker(f) = \{0\}$, then $f(n) \neq 0$ for any $n \neq 0$. In particular $0 \neq f(1) = f(1)f(1)$ and $f(1)$ is an element of the field implies multiplying from right by its inverse we have $f(1)$ is the multiplicative identity of the field K. Hence for any integer n and any non-zero element $a \in K$ we have $na = f(n)a \neq 0$ as product of two non-zero element in a field is non-zero. Hence characteristic of the field K is zero.

(b) On the other hand since $\mathbf{Z}/Ker(f)$ is an integral domain when $Ker(f) \neq 0$, the ideal $Ker(f)$ must be a prime ideal. But the only prime ideals of the ring $\mathbf{Z}$ are the ones generated by prime numbers. Hence $\mathbf{Z}/Ker(f) \cong \mathbf{Z}_p$ Hence K has a smallest subfield isomorphic to $\mathbf{Z}_p$. It follows that K has characteristic p for the prime p.

4.19. *In a ring R if $x^3 = x$ for all $x \in R$, then show that R is commutative.*

Solution: The assumption $x^3 = x$ for all $x \in R$ implies that $(x + x)^3 = (x + x)$ for all $x \in R$. This means $(2x)^3 = 8x = 2x$. Thus $6x = 0$ for all $x \in R$. Also $(x^2 - x)^3 = x^2 - x$ implies that $3x^2 = 3x$ after simplifications. Consider $S = \{3x \mid x \in R\}$. It can be easily checked that S is a subring of R and for $y \in S$

$y^2 = (3x)^2 = 9x^2 = 6x^2 + 3x^2 = 3x^2 = 3x = y$ as $6x^2 = 0$. Thus $y^2 = y$ for all $y \in S$ implies that S is a commutative ring and so $(3x)(3y) = (3y)(3x)$, i.e. $9xy = 9yx$ which implies $3xy = 3yx$. Now $(x + y)^3 = x + y$ implies

(i) $xy^2 + x^2y + xyx + yx^2 + yxy + y^2x = 0$ and $(x - y)^3 = x - y$ implies

(ii) $xy^2 - x^2y - xyx - yx^2 + yxy + y^2x = 0$ By adding (i) and (ii) we obtain

$2xy^2 + 2yxy + 2y^3x = 0$

Multiply last equation by y on right and then by y on left we have

(iii) $2xy + 2yxy^2 + 2y^2xy = 0$

(iv) $2yxy^2 + 2y^2xy + 2yx = 0$ subtract (iii) and (iv) to get

$2xy = 2yx$

since $3xy = 3yx$, we have $xy = yx$ for all $x, y \in R$. Hence R is commutative.

Exercises I

1. Let a and b be elements of a group. If $|a| = n, |b| = m$, and m and n are relatively prime, show $\langle a \rangle \cap \langle b \rangle = \{e\}$.

2. Bertrand's Postulate from number theory says that for any integer $N > 1$ there is always a prime between N and $2N$. Use this fact to prove that $\mathbf{Z}_n$ has more that two generators whenever $n > 6$.

3. Prove that in any group, $|ab| = |ba|$.

4. (Conjugation preserves order.). Prove that in any group $|x^{-1}ax| = |a|$.

5. Prove that if a is the only element of order 2 in a group, then a lies in the center of the group.

6. Let $\mathbf{R}^+$ be the group of positive real numbers under multiplication. Show the mapping $x\phi = \sqrt{x}$ is an automorphism of $\mathbf{R}^+$.

7. Let

$$G = \{a + b\sqrt{2} \mid a, b \text{ rational}\}$$

and

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a, b \text{ rational} \right\}$$

Show that G and H are isomorphic under addition. Prove that G and H are closed under multiplication. Does your isomorphism preserve multiplication as well as addition? (G and H are examples of ring - a topic we will take up later.)

8. Let $\mathbf{R}^\#$ denote the group of all nonzero real numbers under multiplication. Let $\mathbf{R}^+$ denote the subgroup of $\mathbf{R}^\#$ of positive real numbers. Prove that $\mathbf{R}^\#$ is the internal direct product of $\mathbf{R}^+$ and the subgroup $\{1, -1\}$,

9. Prove that $\mathbf{Z}_8 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_{25} \approx \mathbf{Z}_{50} \oplus \mathbf{Z}_{40}$.

10. How many Abelian groups (up to isomorphism) are there

(a) of order 6?

(b) of order 15?

(c) of order 42?

(d) of order pq where p and q are distinct primes?

(e) of order pqr where p, q, and r are distinct primes?

(f) Generalize parts a, b, c, d, e.

11. How does the number (up to isomorphism) of Abelian groups of order n compare with the number (up to isomorphism) of Abelian groups of order m where

(a) $n = 3^2$ and $m = 5^2$?

(b) $n = 2^4$ and $m = 5^4$?

(c) $n = p^r$ and $m = q^r$ where p and q are prime?

(d) $n = p^r$ and $m = p^r q$ where p and q are distinct primes?

(e) $n = p^r$ and $m = p^r q^2$ where p and q are distinct primes?

12. Characterize those integers n such that the only Abelian groups of order n are cyclic.

13. Characterize those integers n which correspond to exactly four isomorphism classes of Abelian groups.

14. Show that an Abelian group of odd order cannot have an element of order 2

15. Suppose G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.

16. Suppose G is a finite Abelian group. Prove that G has order p^n where p is prime if and only if the order of every element of G is a power of p.

17. A subgroup N of a group G is called a *characteristic subgroup if* $N\psi = N$ for all automorphisms ψ of G. (The term "characteristic" was coined by G. Frobenius in 1895.) Prove that every subgroup of a cyclic group is characteristic.

18. Prove that the characteristic property is transitive. That is, if N is a characteristic subgroup of K and K is a characteristic subgroup of G, then N is a characteristic subgroup of G.

19. Let $G = \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$ and let H be the subgroup of $SL(2, \mathbf{Z}_3)$ consisting of

$$\left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbf{Z}_3 \right\}.$$

Determine the number of elements of each order in G and H. Are G and H isomorphic?

EXERCISES II

1. Describe all the subrings of the ring of integers.

2. Show that if n is an integer and a is an element from a ring then $n(-a) = -(na)$

3. Prove that the intersection of any collection of subrigns of a ring R is a subring of R.

4. Let a belong to a ring R. Let $S = \{x \in R \mid ax = 0\}$. Show that S is a subring of R.

5. Let m and n be positive integers and let k be the least common multiple of m and n. Show that $m\mathbf{Z} \cap n\mathbf{Z} = k\mathbf{Z}$.

6. Show that $2\mathbf{Z} \cup 3\mathbf{Z}$ is not a subring of $\mathbf{Z}$.

7. Determine the smallest subring of $\mathbf{Q}$ that contains $1/2$.

8. Suppose that there is a positive even integer n such that $a^n = a$ for all elements a of some ring. Show that $-a = a$ for all a in the ring.

9. Show that a commutative ring with the cancellation property (under multiplication) has no zero-divisors.

10. Give an example of a commutative ring without zero-divisors that is not an integral domain.

11. Let a belong to a ring R and $a^n = 0$ for some positive integer n. (Such an element is called nilpotent.) Prove that $1 - a$ has a multiplicative inverse in R. (Hint: Consider $(1-a)(1+a+a^2+\cdots+a^{n-1})$.)

12. Show that the nilpotent elements of a commutative ring form a subring.

13. A ring element a is called an idempotent if $a^2 = a$. Prove that the only idempotents in an integral domain are 0 and 1.

14. Let R be a ring with unity 1. If the product of any pair of nonzero elements of R is nonzero, prove that $ab = 1$ implies $ba = 1$.

15. Formulate the appropriate definition of a subdomain (that is, a "sub" integral domain). Let D be an integral domain with unity 1. Show that $P = \{n \mid n \in \mathbf{Z}\}$ (that is, all integral multiples of 1) is a subdomain of D. Show that P is contained in every subdomain of D. What can we say about the order of P?

16. Prove that there is no integral domain with exactly six elements. Can your argument be adapted to show that there is no integral domain with exactly four elements? What about 15 elements?

Use these observations to guess a general result about the number of elements in a finite integral domain.

17. Is $\mathbf{Z} \oplus \mathbf{Z}$ an integral domain?

18. Suppose a and b belong to an integral domain.

(a) If $a^5 = b^5$ and $a^3 = b^3$, prove that $a = b$.

(b) If $a^n = b^n$ and $a^m = b^m$, where n and m are positive integers that are relatively prime, prove that $a = b$.

19. Find an example of an integral domain and distinct positive integers m and n such that $a^m = b^m$ and $a^n = b^n$, but $a \neq b$.

20. Show that a finite commutative ring with no zero-divisors has a unity.

21. Let x and y belong to an integral domain of prime characteristic p.

(a) Show that $(x + y)^p = x^p + y^p$.

(b) Show that for all positive integers $n, (x + y)^{p^n} = x^{p^n} + y^{p^n}$.

(c) Find elements x and y in a ring of characteristic 4 such that $(x + y)^4 \neq x^4 + y^4$.

22. Consider the equation $x^2 - 5x + 6 = 0$

a) How many solutions does this equation have in $\mathbf{Z}_7$?

b) Find all solutions of this equation in $\mathbf{Z}_8$

c) Find all solutions of this equation in $\mathbf{Z}_{12}$.

d) Find all solutions of this equation in $\mathbf{Z}_{14}$.

23. Let R be the ring of all functions from $\mathbf{R}$ to $\mathbf{R}$ with pointwise addition and pointwise multiplication as the operations. Show that every element of R is either a unit or a zero-divisor.

24. If A and B are ideals of a commutative ring R with unity and $A + B = R$, show that $A \cap B = AB$.

25. Show that $\mathbf{R}[x]/\langle x^2 + 1\rangle$ is a field.

26. Show that $A = \{(3x, y) \mid x, y \in \mathbf{Z}\}$ is a maximal ideal of $\mathbf{Z} \oplus \mathbf{Z}$.

27. Let R be the ring of continuous functions from $\mathbf{R}$ to $\mathbf{R}$. Show that $A = \{f \in R \mid f(0) = 0\}$ is a maximal ideal of R.

28. Show that $\mathbf{Z}_3[x]/\langle x^2 + x + 1\rangle$ is not a field.

29. Let R be the ring of continuous functions from $\mathbf{R}$ to $\mathbf{R}$. Let $A = \{f \in R \mid f(0)$ is an even integer $\}$. Show that A is a subring of R, but not an ideal of R.

30. If R is a principal ideal domain and I is an ideal of R, prove that every ideal of R/I is principal.

31. If R is an integral domain and A is a proper ideal of R, must R/A be an integral domain?

32. Let $\mathbf{Z}(\sqrt{2}) = \{a + b\sqrt{2} \quad | \ a, b \in \mathbf{Z}\}$. Let

$$H = \left\{ \left[\begin{array}{cc} a & 2b \\ b & a \end{array} \right] \middle| \ a, b \in \mathbf{Z} \right\}.$$

Show that $\mathbf{Z}(\sqrt{2})$ and H are isomorphic as rings.

33. Determine all ring homomorphisms from $\mathbf{Z}_6$ to $\mathbf{Z}_6$. Determine all ring homomorphisms from $\mathbf{Z}_{20}$ to $\mathbf{Z}_{30}$.

34. Let R be a commutative ring of prime characteristic p. Show that the Frobenius map $x \to x^p$ is a ring homomorphism from R to R.

35. Let ψ be a ring homomorphism from R onto S and A be an ideal of S.

(a) If A is prime in S, show that $A\psi^{-1} = \{x \in R \mid x\psi \in A\}$ is prime in R.

(b) If A is maximal in S, show that $A\psi^{-1}$ is maximal in R.

36. Show that if n and m are distinct positive integers, then $n\mathbf{Z}$ is not ring isomorphic to $m\mathbf{Z}$.

37. Show that the only automorphism of the real numbers is the identity mapping.

38. Suppose $\psi : R \to S$ is a ring homomorphism and the image of ψ is not $\{0\}$. If R has a unity and S is an integral domain, show that ψ carries the unity of R to the unity of S. Given an example to show that the previous statement need not be true if S is not an integral domain.

EXERCISES III

1. Show that $x^2 + 3x + 2$ has 4 zeros in $\mathbf{Z}_6$.

2. In $\mathbf{Z}_3[x]$, show that x^4+x and x^2+x determine the same function from $\mathbf{Z}_3$ to $\mathbf{Z}_3$.

3. List all the polynomials of degree 2 in $\mathbf{Z}_2[x]$.

4. If $\phi : R \to S$ is a ring homomorphism, define $\overline{\phi} : R[x] \to S[x]$ by $(a_n x^n + \cdots + a_0)\phi = a_n\phi x^n + \cdots + a_0\phi$. Show that ϕ is a ring homomorphism.

5. Let R be a commutative ring. Show that $R[x]$ has a subring isomorphic to R.

6. Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1$ in $\mathbf{Z}_7[x]$. Determine the quotient and remainder upon dividing $f(x)$ by $g(x)$.

7. Show that the polynomial $2x + 1$ in $\mathbf{Z}_4[x]$ has a multiplicative inverse in $\mathbf{Z}_4[x]$.

8. Are there any nonconstant polynomials in $\mathbf{Z}[x]$ that have multiplicative inverses? Explain your answer.

9. Prove that the ideal $\langle x \rangle$ in $\mathbf{Z}[x]$ is prime and maximal in $\mathbf{Q}[x]$, but not maximal in $\mathbf{Z}[x]$.

10. Let F be an infinite field and $f(x), g(x) \in F[x]$. If $f(a) = g(a)$ for infinitely many elements a of F, show that $f(x) = g(x)$.

11. Prove that $\mathbf{Z}[x]$ is not a principal ideal domain.

12. Let F be a field and let

$I = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \mid \quad a_n, a_{n-1}, \cdots, a_0 \in F$ and $a_n + a_{n-1} + \cdots + a_0 = 0\}$.

Show that I is an ideal of $F[x]$ and find a generator for I.

13. For every prime p, show that

$$x^{p-1} - 1 = (x-1)(x-2)\cdots[x-(p-1)] \qquad \text{in } \mathbf{Z}_p[x].$$

14. Let p be a prime. Show that $x^n - p$ is irreducible over the rational numbers.

15. Let F be a field and let a be a nonzero element of F.

a) If $af(x)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

b) If $f(ax)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

c) If $f(x+a)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

16. Show that x^4+1 is irreducible over $\mathbf{Q}$ but reducible over $\mathbf{R}$.

17. Construct a field of order 25.

18. Determine which of the polynomials below are irreducible over $\mathbf{Q}$.

a) $x^5+9x^4+12x^2+6$ b) x^4+x+1 c) x^4+3x^2+3

d) x^5+5x^2+1 e) $(5/2)x^5+(9/2)x^4+15x^3+(3/7)x^2+6x+3/14$.

19. Let $f(x)=x^3+6 \in \mathbf{Z}_7[x]$. Write $f(x)$ as a product of irreducible polynomials over $\mathbf{Z}_7$.

20. Let $f(x)=x^3+x^2+x+1 \in \mathbf{Z}_2[x]$. Write $f(x)$ as a product of irreducible polynomials over $\mathbf{Z}_2$.

21. Let p be a prime

a) Show that the number of reducible polynomials over $\mathbf{Z}_p$ of the form x^2+ax+b is $p(p+1)/2$.

b) Determine the number of reducible quadratic polynomials over $\mathbf{Z}_p$.

22. Show that x^4+1 is reducible over $\mathbf{Z}_p$ for every prime p.

23. Prove that the irreducible factorization of $x^6+x^5+x^4+x^3+x^2+x$ over $\mathbf{Z}$ is
$x(x+1)(x^2+x+1)(x^2-x+1)$,

24. If p is a prime, prove that $x^{p-1}-x^{p-2}+x^{p-3}-\cdots-x+1$ is irreducible over $\mathbf{Q}$.

25. In an integral domain, show that the product of an irreducible and a unit is an irreducible.

26. Show that the union of a chain $I_1 \subset I_2 \subset \cdots$ of ideals of a ring R is an ideal of R.

27. Suppose a and b belong to an integral domain, $b \neq 0$, and a is not a unit. Show that $\langle ab \rangle$ is a proper subset of $\langle b \rangle$.

28. Let D be a principal ideal domain. Show that every proper ideal of D is contained in a maximal ideal of D.

29. In $\mathbf{Z}[\sqrt{-5}]$, show that 21 does not factor uniquely as a product of irreducibles.

30. Show that $1-i$ is an irreducible in $\mathbf{Z}[i]$.

31. Show that $\mathbf{Z}[\sqrt{-6}]$ is not a unique factorization domain. (Hint: Factor 10 in two ways.)

32. In $\mathbf{Z}[i]$, show that 3 is irreducible but 2 and 5 are not.

33. Show that $3x^2 + 4x + 3 \in \mathbf{Z}_5[x]$ factors as $(3x + 2)(x + 4)$ and $(4x + 1)(2x + 3)$.

34. Let D be a principal ideal domain and let $p \in D$. Prove that $\langle p \rangle$ is a maximal ideal in D if and only if p is irreducible.

35. Suppose F is a field and there is a ring homomorphism from $\mathbf{Z}$ onto F. Show that F is isomorphic to $\mathbf{Z}_p$ for some prime p.

36. Let $\mathbf{Q}[\sqrt{2}] = \{r + s\sqrt{2} \mid r, s \in \mathbf{Q}\}$. Determine all ring automorphisms of $\mathbf{Q}[\sqrt{2}]$.

37. Prove that the set of all polynomials with even coefficients is a prime ideal in $\mathbf{Z}[x]$.

38. Let $R = \mathbf{Z}[\sqrt{-5}]$ and let $I = \{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}.\ a - b$ is even $\}$. Show that I is a maximal ideal of R.

39. Show that $\mathbf{Z}[i]/\langle 2 + i \rangle$ is a field. How many elements does it have?

40. In $[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$. Show that every element of the form $(3 + 2\sqrt{2})^n$ is a unit.

41. Recall, a is an idempotent if $a^2 = a$. Show that if $1 + k$ is an idempotent in $\mathbf{Z}(n)$, then $n - k$ is an idempotent in $\mathbf{Z}(n)$.

42. Prove that $x^4 + 15x^3 + 7$ is irreducible over $\mathbf{Q}$.

Exercise IV

1. Describe the elements of $\mathbf{Q}(\sqrt[3]{5})$.

2. Show $\mathbf{Q}(\sqrt{2},\sqrt{3}) = \mathbf{Q}(\sqrt{2}+\sqrt{3})$.

3. Find the splitting field of x^3-1 over $\mathbf{Q}$. Express your answer in the form $\mathbf{Q}(a)$.

4. Find the splitting field of x^4+1 over $\mathbf{Q}$.

5. Find the splitting field of $x^4+x^2+1 = (x^2-x+1)(x^2-x+1)$ over $\mathbf{Q}$.

6. Find a polynomial $p(x)$ in $\mathbf{Q}[x]$ so that $\mathbf{Q}(\sqrt{1+\sqrt{5}})$ is isomorphic to $\mathbf{Q}[x]/\langle p(x)\rangle$.

7. Let $F = \mathbf{Z}_2$ and let $f(x) = x^3+x+1 \in F[x]$. Suppose a is a zero of $f(x)$ in some extension of F. How many elements does $F(a)$ have? Express each member of $F(a)$ in terms of a. Write out a complete multiplication table for $F(a)$.

8. Express $(3+4\sqrt{2})^{-1}$ in the form $a+b\sqrt{2}$ where $a,b \in \mathbf{Q}$.

9. Show that $\mathbf{Q}(4-i) = \mathbf{Q}(1+i)$ where $i = \sqrt{-1}$.

10. Prove that $\mathbf{Q}(\sqrt{2},\sqrt[3]{2},\sqrt[4]{2},\cdots)$ is an algebraic extension of $\mathbf{Q}$ but not a finite extension on $\mathbf{Q}$.

11. Let E be the algebraic closure of F, show that every polynomial in $F[x]$ splits in E.

12. Let E be an algebraic extension of F. If every polynomial in $F[x]$ splits in E, show that E is algebraically closed.

13. Suppose $f(x)$ and $g(x)$ are irreducible over F and deg $f(x)$ and deg $g(x)$ are relatively prime. If a is a zero of $f(x)$ in some extension of F, show that $g(x)$ is irreducible over $F(a)$.

14. Let a and b belong to $\mathbf{Q}$ with $b \neq 0$. Show that $\mathbf{Q}(\sqrt{a}) = \mathbf{Q}(\sqrt{b})$ if and only if there exists some $c \in \mathbf{Q}$ such that $a = bc^2$.

15. Find the degree and a basis for $\mathbf{Q}(\sqrt{3}+\sqrt{5})$ over $\mathbf{Q}(\sqrt{15})$. Find the degree and a basis for $\mathbf{Q}(\sqrt{2},\sqrt[3]{2},\sqrt[4]{2})$ over $\mathbf{Q}$.

16. Suppose E is an extension of F of prime degree. Show that for every a in E, $F(a) = F$ or $F(a) = E$.

17. Suppose α is algebraic over $\mathbf{Q}$. Show that $\sqrt{\alpha}$ is algebraic over $\mathbf{Q}$.

18. Suppose E is an extension of F and $a,b \in E$. If a is algebraic over F of degree m and b is algebraic over F of degree n where m and n are relatively prime, show that $[F(a,b):F] = mn$.

19. Find the minimal polynomial for $\sqrt{-3}+\sqrt{2}$ over $\mathbf{Q}$.

20. Find the minimal polynomial for $\sqrt[3]{2}+\sqrt[3]{4}$ over $\mathbf{Q}$.

21. Let a be a complex zero of x^2+x+1. Express $(5a^2+2)/a$ in the form $c+ba$, where c and b are rational

22. Describe the elements of the extension $\mathbf{Q}(\sqrt[4]{2})$ over the field $\mathbf{Q}(\sqrt{2})$.

23. If $[F(a):F]=5$, find $[F(a^3):F]$.

24. If $p(x)\in F[x]$ and $\deg p(x)=n$, show that the splitting field for $p(x)$ over F has degree at most $n!$.

25. Let α be a nonzero algebraic element over F of degree n. Show that a^{-1} is also algebraic over F of degree n.

26. Prove that π^2-1 is algebraic over $\mathbf{Q}(\pi^3)$.

27. If ab is algebraic over F, prove that a is algebraic over $F(b)$.

28. Squaring the circle. With a straightedge and compass, show that it is impossible to construct a square whose area equals that of a circle of radius 1.

29. Show that a regular 9-gon cannot be constructed with a straightedge and a compass.

30. Find $[GF(729):GF(9)]$ and $[GF(64):GF(8)]$.

31. If n divides m, show that $[GF(p^m):GF(p^n)]=m/n$.

32. Let K be a finite extension field of a finite field F. Show that there is an element a in K such that $K=F(a)$.

33. Show that any finite subgroup of the multiplicative group of a field is cyclic.

34. Suppose m and n are positive integers and m divides n. If F is any field, show that x^m-1 divides x^n-1 in $F[x]$.

35. If $g(x)$ is irreducible over $GF(p)$ and $g(x)$ divides $x^{p^n}-x$, prove that $\deg g(x)$ divides n.

36. Draw the subfield lattice of $GF(3^{18})$ and $GF(2^{30})$.

37. Show that the Frobenius mapping $\phi: GF(p^n)\to GF(p^n)$, given by $a\to a^p$ is an automorphism of order n. (That is, ϕ^n is the identity mapping.)

38. Suppose F is a field of order 1024 and $F^{\#}=\langle\alpha\rangle$. List the elements of each subfield of F.

39. Suppose F is a field of order 125 and $F^{\#}=\langle\alpha\rangle$. Show that $\alpha^{62}=-1$.

40. Show that no finite fields is algebraically closed.

1) Let G be a group and let $T = G \times G$

a) Show that $D = \{(g, g) \in G \times G \mid g \in G\}$ is isomorphic to G.

b) Prove that D is normal in T if and only if G is abelian.

2. Let F be a field of characteristic p.

(a) Show that the map $x \to x^{p^n}$ is an automorphism of the field F.

(b) Find elements x and y in a ring of characteristic 4 such that $(x + y)^4 \neq x^4 + y^4$.

3. Let $G = \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$ and let H be the subgroup of $SL(2, \mathbf{Z}(3))$ consisting of

$$\left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbf{Z}_3 \right\}.$$

Determine the number of elements of each order in G and H. Are G and H isomorphic?

4. Find the set of all automorphisms of the field $\mathbf{Q}$ $(\sqrt{7})$.

5 Let G be the symmetric group on four letters and A_4 be the alternating group in G consisting of even permutations. Find the smallest normal subgroup N of A_4 that contain the element (12)(34).

b)Write the cosets of N in A_4.

MATH 370, Final Exam: 1.6.1994

1) If a cyclic group T of G is normal in G, then show that every subgroup of T is a normal subgroup in G.

2) D is an integral domain and D is of finite characteristic, prove that the characteristic of D is a prime number.

3) If E is an extension of F and if $f(x) \in F[x]$ and if ψ is an automorphism of E leaving every element of F fixed, prove that ψ must take a root of $f(x)$ lying in E into a root of $f(x)$ in E.
4) Show $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

5) In a finite field $\mathbf{F}$ with char $\mathbf{F} = p$. Show that for any $\alpha \in \mathbf{F}$, there exists $\beta \in \mathbf{F}$ such that $\beta^p = \alpha$.
6) Find a polynomial $p(x)$ in $\mathbf{Q}[x]$ so that $\mathbf{Q}(\sqrt{1 + \sqrt{5}})$ is isomorphic to $\mathbf{Q}[x]/\langle p(x) \rangle$.