# GRADUATE ALGEBRA PROBLEMS WITH SOLUTIONS

Mahmut Kuzucuoğlu

November 21, 2011

# TABLE OF CONTENTS

# PREFACE

These notes were prepared in 1993 when we gave the graduate algebra course. Our intention was to help the students by giving them exercises and get them familiar with how to use the theory to solve problems. These notes are the outcome of request from old-new postgraduate students who constantly requested a copy of the solutions.

I am grateful to Prof.Dr. C. Koç for a thorough critical reading of the solutions. I would also like to thank to Dr. A. Berkman for her contribution in reading the manuscript. Of course the remaining errors belongs to me. If you find any errors, I should be grateful to hear from you. I also thank to Mathematics Foundation for making this book possible . Finally I would like to thank Aynur Bora for her typing the manuscript in LATEX.

Mahmut Kuzucuoğlu

July 1999, METU, ANKARA

In 2010 I had a bright student in my Graduate Algebra course Barış Kartal. He took this course when he was a Freshman and go through all the exercises in the previous version. Therefore I had to correct or change some of the questions. For this new version, I would like to thank him for all his efforts and making the course, one of the most enjoyable one.

Mahmut Kuzucuoğlu

November 2011, METU, ANKARA

# Graduate algebra, problems with solutions

M. Kuzucuoğlu

# GROUPS

(1) If $G$ is a group and $f : G \to G$ is defined by $f(x) = x^{-1}$, all $x \in G$, show that $f$ is a homomorphism if and only if $G$ is abelian.

**Solution:** Assume that $f$ is a homomorphism. Then

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

Hence $y^{-1}x^{-1} = x^{-1}y^{-1}$, and $xy = (y^{-1}x^{-1})^{-1} = (x^{-1}y^{-1})^{-1} = yx$ for all $x, y \in G$. This implies that $G$ is abelian. Conversely assume that $G$ is abelian. Then

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

Hence $f$ is a homomorphism.

(2) If a group $G$ has a unique element $x$ of order 2, show that $x \in Z(G)$.

**Solution:** Assume that $x$ is the unique element of order 2 in $G$. Then it is easy to see that for any $g \in G, g^{-1}xg$ is also an element of order 2. By uniqueness, $g^{-1}xg = x$. Hence, $x \in Z(G)$.

(3) Suppose $G$ is finite, $K \lhd G, H \leq G$ and $|K|$ is relatively prime to $[G : H]$. Show that $K \leq H$.

**Solution:** Since $K \lhd G, KH$ is a subgroup of $G$. $[G : H] = [G : KH][KH : H]$. By assumption $(|K|, [G : H]) = 1$. This implies $(|K|, [G : KH]) = 1$ and $([KH : H], |K|) = 1$. Since $G$ is finite, $[KH : H] = \frac{|KH|}{|H|}$ and since $\frac{KH}{H} \cong \frac{K}{K \cap H}$

$$(\frac{|KH|}{|H|} = \frac{|K|}{|K \cap H|}\ , \quad |K|) = 1$$

This implies $\frac{|K|}{|K \cap H|} = 1$. Hence $K \cap H = K$, and consequently $K \leq H$.

(4) If $G$ is not abelian show that $Z(G)$ is properly contained in an abelian subgroup of $G$.

**Solution:** Since $G$ is not abelian, $G \neq Z(G)$. So there exists an element $x \in G \setminus Z(G)$. Now consider the group generated by $x$

and $Z(G)$. This group is an abelian subgroup of $G$ containing $Z(G)$ properly. This group is not equal to $G$ as $G$ is not abelian. Hence $\langle Z(G), x\rangle$ is the required subgroup of $G$.

(5) If $G$ is a group and $|x| = 2$ for all $x \neq 1$ in $G$, show that $G$ is abelian. Can you say more?

**Solution:** For any $x \in G, x^2 = 1$. Hence $x = x^{-1}$. Now, let $x, y \in G$. Then, $(xy)^2 = (xy) \cdot (xy) = 1$. This gives $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Hence $G$ is abelian. Such a group must be a 2-group and all such groups are called elementary abelian 2-groups.

(6) Suppose $G$ is a group, $H \leq G$, and $K \leq G$. Show that $H \cup K$ is not a group unless $H \leq K$ or $K \leq H$.

**Solution:** Assume that $H \not\leq K$ and $K \not\leq H$, and $H \cup K$ is a group. Let $h \in H \setminus K$ and $k \in K \setminus H$. Then, $hk \in H \cup K$. Therefore, either $hk \in H$ or $hk \in K$. If $hk \in H$, then $h^{-1}hk = k \in H$ which is impossible. If $hk \in K$, then $hkk^{-1} = h \in K$ which is also impossible. This contradiction gives the result.

(7) Suppose that $S$ and $T$ are two subsets of a finite group $G$, with $|S| + |T| > |G|$. If $ST$ is defined to be $\{st \ : \ s \in S, t \in T\}$, show that $G = ST$.

**Solution:** Let $g$ be an arbitrary element in $G$. Then $|gT| = |T| = |gT^{-1}|$ and $|G| \geq |S \cup gT^{-1}| = |S| + |gT^{-1}| - |S \cap gT^{-1}| > |G| - |S \cap gT^{-1}|$. Hence $|S \cap gT^{-1}| > 0$, i.e $S \cap gT^{-1} \neq \emptyset$. Thus there exists $s \in S$ and $t^{-1} \in T^{-1}$ such that $s = gt^{-1}$ which implies that $g = st$. This proves that $g \in ST$ and $G = ST$.

(8) Suppose $S$ is a subset of a finite group $G$, with $|S| > \frac{|G|}{2}$. If $S^2$ is defined to be $\{xy : x, y \in S\}$, show that $S^2 = G$.

**Solution:** Assume that $S^2 \neq G$. Then there exists $x \in G \setminus S^2$. Consider the table of $G$ :

| $\star$ | $s_1$ | $s_2$ | $s_3$ | $\cdots$ | $s_k$ | | | |
|---|---|---|---|---|---|---|---|---|
| $s_1$ | $s_1^2$ | $s_1s_2$ | $s_1s_3$ | $\vdots$ | $s_1s_k$ | $x$ | | |
| $s_2$ | $s_2s_1$ | $s_2^2$ | $s_2s_3$ | $\vdots$ | $s_2s_k$ | | | |
| $s_3$ | $s_3s_1$ | $s_3s_2$ | $s_3^2$ | $\vdots$ | $s_3s_k$ | | | |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $s_k$ | $s_ks_1$ | $s_ks_2$ | $s_ks_3$ | $\cdots$ | $s_k^2$ | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Recall that $x$ must appear in each row and in each column of the table only once. Hence $x$ appears $|G|$ times in the table. Assume that $|S| = k$. Each row contains $x$ implies that, we need $k$ more columns to place $x$'s to each row. That implies the order of the group $G$ is greater than or equal to $2k$. But this is impossible by the assumption that $k = |S| > \frac{|G|}{2}$.

**Remark** Observe that it is possible to argue this question as in the previous question $S = T$.

(9) If $A, B \leq G$ and both $[G : A]$ and $[G : B]$ are finite. Show that $[G : A \cap B] \leq [G : A][G : B]$ with equality if and only if $G = AB$.

**Solution:** Let $\Omega_A = \{Ax \mid x \in G\}$, $\Omega_B = \{Bx \mid x \in G\}$ and $\Omega_{A\cap B} = \{(A \cap B)x \mid \ x \in G\}$ be the sets of right cosets of $A, B$ and $A \cap B$ in $G$ respectively. Define a map

$$\alpha : \Omega_{A\cap B} \to \Omega_A \times \Omega_B$$

by $\alpha((A \cap B)y) = (Ay, By)$. Clearly $\alpha$ is well-defined.

$$\alpha((A \cap B)y) = \alpha((A \cap B)t)$$

implies

$$(Ay, By) = (At, Bt).$$

Then $Ay = At$ and $By = Bt$. Hence $yt^{-1} \in A \cap B$. This implies $(A \cap B)y = (A \cap B)t$. Hence the map $\alpha$ is one to one. This gives

$$[G : A \cap B] \leq [G : A][G : B].$$

If $G = AB$, then $[AB : A \cap B] = [AB : A][A : A \cap B]$

Claim: $[A : A \cap B] = [AB : B]$. Let

$$\begin{aligned} \Omega &= \{(A \cap B)x \mid x \in A\} \\ \Sigma &= \{By \mid y \in AB\} \end{aligned}$$

Define a map $\beta : \Omega \to \Sigma$ by $\beta((A \cap B)y) = By$. For $x, y \in A, Bx = By$ implies $xy^{-1} \in A \cap B$. So

$(A \cap B)x = (A \cap B)y$. So $\beta$ is 1-1. Since $G = AB = BA$ every coset of $B$ in $G$ is of the form $Ba$ for some $a \in A$. It is clear that $\beta$ is onto. Hence the result.

Conversely assume that

$$[G : A \cap B] = [G : A][G : B]$$

$$[G : A \cap B] = [G : A][A : A \cap B] = [G : A][G : B]$$

Since $[G : A]$ is finite, cancelling this number from both sides we get

$$[A : A \cap B] = [G : B].$$

But

$$[A : A \cap B] = [AB : B]$$

the number of cosets of $B$ contained in the set $AB$. Hence we get $[AB : B] = [G : B]$ this implies $AB = G$.

(10) If $[G : A]$ and $[G : B]$ are finite and relatively prime show that $G = AB$.

**Solution:** $[G : A \cap B] = [G : A][A : A \cap B] = [G : B][B : A \cap B]$. Since $[G : A]$ and $[G : B]$ are relatively prime

$$[G : A] \mid [B : A \cap B] = [AB : A]$$

This implies $[G : A] = [AB : A]$ because $[AB : A] \leq [G : A]$ and $AB \neq A$. Hence $AB = G$. see the previous question.

(11) Suppose $G$ acts on $S, x \in G$, and $s \in S$. Show that $Stab_G(x.s) = x\ Stab_G(s)x^{-1}$.

**Solution:** Let $g \in\ Stab_G(x.s)$. Then $g.(x.s) = (gx).s = x.s$. Multiplying from left by $x^{-1}$ we get $(x^{-1}gx) \cdot s = s$. Hence $x^{-1}gx \in Stab_G(s)$. This implies $g \in x\ Stab_G(s)x^{-1}$. Conversely assume that $g \in x\ Stab_G(s)x^{-1}$. Then $g = xhx^{-1}$ where $h \in\ Stab_G(s)$. Now

$$g \cdot (x.s) = (xhx^{-1}) \cdot (x.s) = (xh) \cdot s = (x.s)$$

as $h \in\ Stab_G(s)$. Hence $g \in\ Stab_G(x.s)$.

(12) If $A, B \leq G$ and $y \in G$ define the $(A, B)$-double coset

$$AyB = \{ayb : a \in A, b \in B\}.$$

Show that $G$ is the disjoint union of its $(A, B)$-double cosets. Show that

$$|AyB| = [A^y : A^y \cap B]|B|$$

if $A$ and $B$ are finite.

**Solution:** Let $x, y \in G$. Define $x \sim y$ if and only if there exists $a \in A$ and $b \in B$ such that $x = ayb$.

<u>" $\sim$ " is an equivalence relation:</u>

(i) $x = 1x1$ and $1 \in A, 1 \in B$ since $A$ and $B$ are subgroups of $G$. Hence $x \sim x$.

(ii) If $x \sim y$, then $x = ayb$ for some $a \in A$ and $b \in B$. This implies $y = a^{-1}xb^{-1}$ and $a^{-1} \in A, b^{-1} \in B$ since $A$ and $B$ are subgroups of $G$. Hence $y \sim x$.

(iii) $x \sim y$ and $y \sim z$ implies $x = ayb$ and $y = czd$ for some $a, c \in A$, and $b, d \in B$. Then $x = ayb = aczdb = (ac)z(db)$. Since $ac \in A$, and $db \in B$ we get $x \sim z$.

The equivalence class containing $y$ is $[y] = \{ayb | a \in A, b \in B\} = AyB$.

Since " $\sim$ " is an equivalence relation on $G$ we get $G$ is a disjoint union of equivalence classes, namely $AyB'$s.

Define a map

$$\alpha: \quad \begin{aligned} AyB &\to y^{-1}AyB \\ ayb \ &\to y^{-1}ayb \end{aligned}$$

It is easy to see that $\alpha$ is a bijective map. Hence if $A$ and $B$ are finite the number of elements in $AyB$ and $y^{-1}AyB$ are equal.

Since $y^{-1}Ay$ and $B$ are subgroup of $G$ we get

$$|A^yB| = \frac{|A^y||B|}{|A^y \cap B|} = [A^y : A^y \cap B]|B|$$

**Definition** Let $\Omega$ be a set and $G$ be a group acting on $\Omega$. We say that $G$ acts transitively on $\Omega$ if for any $\alpha, \beta \in \Omega$, there exists $g \in G$ such that $g.\alpha = \beta$.

(13) Suppose $G$ is a permutation group on a set $S$, with $|S| > 1$. Say that $G$ is doubly transitive on $S$ if given any $(a, b), (c, d) \in S \times S$ with $a = b$ if and only if $c = d$, then $xa = c$ and $xb = d$ for some $x \in G$.

(1) If $G$ is transitive on $S$ show that $G$ is doubly transitive if and only if $H = Stab_G(s)$ is transitive on $S \setminus \{s\}$ for each $s \in S$.

(2) If $G$ is doubly transitive on $S$ and $|S| = n$, show that $n(n-1) \mid |G|$.

**Solution:** (1) Assume that $G$ is doubly transitive on $S$. Let $s \in S$ and $H = Stab_G(s)$. Let $\alpha, \beta \in S \setminus \{s\}$. Then

$$(\alpha, s), (\beta, s) \in S \times S$$

So there exists $x \in G$ such that $x.\alpha = \beta$ and $x.s = s$. Hence $x \in H$ and $x.\alpha = \beta$ i.e $H$ is transitive on $S - \{s\}$.

Conversely assume that $H$ is transitive on $S \setminus \{s\}$ and $(a, b), (c, d) \in S \times S$. If $a = b$ and $c = d$ then it is clear that there exists $x \in G$ such that $x.a = c$ and $x.b = d$.

So assume that $a \neq b$ and $c \neq d$. Since $G$ is transitive on $S$ there exist $g_1, g_2 \in G$ such that $g_1.a = s$ and $g_2.s = c$. Moreover there exists $h \in H$ such that $h.(g_1.b) = g_2^{-1}.d$ since $H$ is transitive on $S \setminus \{s\}$ and $g_1.b,\ g_2^{-1}d \in S \setminus \{s\}$. Thus we have $h.(g_1.a) = s = g_2^{-1}.c$ or $g_2.[h.(g_1.a)] = c$ and $g_2.[h.(g_1.b)] = d$. So $(g_2 h g_1).(a,b) = (c,d)$. Hence $G$ is doubly transitive on $S$.

(2)Let $s \in S$ and $H = Stab_G(s)$. Then $[G : H] = n$ as $G$ acts transitively on $S$ and $|S| = n$.

Let $\alpha \in S \setminus \{s\}$ and $K = Stab_H(\alpha)$. Then $[H : K] = n - 1$ as $H$ acts transitively on $S \setminus \{s\}$ and $|S \setminus \{s\}| = n - 1$. Hence $[G : K] = [G : H] \cdot [H : K] = n(n-1)$ and so $n(n-1) \mid |G|$.

(14) Suppose $G$ is finite, $p$ is the smallest prime dividing $|G|$, $H \leq G$ and $[G : H] = p$. Show that $H \lhd G$.

**Solution:** Consider the right action of $G$ on the set of right cosets of $H$ in $G$. Then there exists a homomorphism $\varphi$ from $G$ into symmetric group on $p$ letters. $Ker\varphi = \cap_{x \in G} H^x$ and $G/Ker\varphi$ is isomorphic to a subgroup of $S_p$. Note that $|S_p| = p!$ so $[G : Ker\varphi] | p!$. If $Ker\varphi \lneqq H$, then $[G : Ker\varphi]$ is divisible by a prime which is smaller than $p$. But this is impossible by assumption. So $Ker\varphi = H$ This implies $H \lhd G$.

(15) Suppose $[G : H]$ is finite. Show that there is a normal subgroup $K$ of $G$ with $K \leq H$ such that $[G : K]$ is finite.

**Solution:** Let $[G : H] = n$ and $\Omega$ be the set of right cosets of $H$ in $G$. Then $G$ acts on $\Omega$ by right multiplication and there exists a homomorphism $\varphi$ from $G$ into $Sym(\Omega)$. Hence $G/Ker\varphi$ is isomorphic to a subgroup of $Sym(\Omega)$. Then $K = Ker\varphi$ satisfies the required properties, since $|Sym(\Omega)| = n!$

(16) Suppose $G$ is finite, $H \leq G$, and $G = \cup\{H^x : x \in G\}$. Show that $H = G$.

**Solution:** Let $|H| = m$. Then $|H^x| = m$ and there are at most $m-1$ distinct elements in $H$ and $H^x$. Assume that $|G| = n$. Then by Lagrange Theorem $m|n$. Say $n = km$ where $k \geq 2$.

Let $G = H^{x_1} \cup H^{x_2} \cup \cdots \cup H^{x_r}$ where $r$ is minimal satisfying this condition. i.e., $H^{x_i} \neq H^{x_j}$. Then

$$|G| = n \leq (m-1)r + 1 \quad km = n \leq mr - r + 1 \quad r \geq 2.$$

Since $H^{hx_i} = H^{x_i}$ and we assumed $H^{x_i} \neq H^{x_j}$, we get $r \leq k$. Since $r = [G : N_G(H)] \leq [G : H]$ as $H \leq N_G(H)$. Then, $mk = n \leq mr - r + 1$,
$mk - mr \leq -r + 1, \quad m(k-r) \leq -r+1$. Since $r \geq 2$ and $m(k-r) \geq 0$. This is impossible. This contradiction gives $H = G$.

(17) Let $G$ be the group $GL(2, \mathbb{C})$ of all $2 \times 2$ invertible complex matrices and $H$ be the subgroup of all lower triangular matrices $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$, $ac \neq 0$. Show that $G = \cup\{H^x : x \in G\}$. (Compare with the previous problem .)

**Solution:** Let $g = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ with $a_{11}a_{22} - a_{12}a_{21} \neq 0$ be any $2 \times 2$ matrix in $GL(2, \mathbb{C})$. Then $|xI - g| = \begin{vmatrix} x - a_{11} & -a_{12} \\ -a_{21} & x - a_{22} \end{vmatrix} = (x - a_{11})(x - a_{22}) - a_{21}a_{12} = x^2 - (a_{22} + a_{11})x + \underbrace{a_{11}a_{22} - a_{21}a_{12}}_{\neq 0}$ This is a polynomial of degree 2 with coefficients form $\mathbb{C}$. Since we work in $\mathbb{C}$, the minimal polynomial of this matrix is a product of linear factors. Hence this matrix is triangulable, i.e. there exists a matrix $x \in GL(n, \mathbb{C})$ such that $g^x$ is a triangular matrix. Hence $g^x \in H$ i.e. $g \in H^{x^{-1}}$. Hence $G = \cup_{x \in G} H^x$.

(18) Let $T$ be the set of $n-1$ successive transpositions $(12), (23), (34), \ldots, (n-1, n)$ in $S_n$. Show that $< T >= S_n$.

**Solution:** Recall that every permutation in $S_n$ can be written as a product of disjoint cycles. Hence it is enough to show that every cycle can be written as a product of transpositions from $T$. Recall also that every cycle can be written as a product of transpositions. Hence it is enough to show that any transposition can be written as a product of transpositions given above. Let $(kl)$ with $k<l$ be a transposition is $S_n$. Then

$$(k,l)=(k,k+1)(k+1,k+2)\cdots(l-2,l-1)(l-1,l)(l-1,l-2)\cdots(k+1,k).$$

Hence we are done.

(19) Suppose $H \leq S_n$ but $H \not\leq A_n$. Show that $[H : H \cap A_n] = 2$.
(Hint: Observe that $HA_n = S_n$.)

**Solution:** Since $H \not\leq A_n, H$ contains an odd permutation. Therefore $A_n \lneqq HA_n$ as $A_n \lhd S_n$. Moreover $|HA_n| \mid |S_n|$. But $\frac{|S_n|}{|A_n|} = 2$. Hence $|HA_n| = |S_n|$. This implies $HA_n = S_n$ and $HA_n/A_n = S_n/A_n$. Hence $[H : H \cap A_n] = [HA_n : A_n] = [S_n : A_n] = 2$.

(20) If $S = \{1,2,3,4,\ldots\}$. Let $A_\infty$ denote the (infinite) group of all $\sigma \in Perm(S)$ such that there is a finite subset $T \subset S$ for which $\sigma$ restricts to an even permutation of $T$ and $\sigma(s) = s$ for all $s \in S \setminus T$. Equivalently $A_\infty = \cup\{A_n : n = 1,2,3,\cdots\}$. Show that $A_\infty$ is simple.

**Solution:** We use the definition $A_\infty = \cup\{A_n \mid n = 1,2,3,\cdots\}$. Therefore each $A_n$ is embedded in $A_{n+1}$ naturally. This gives $A_n \leq A_{n+1} \leq \cdots$. Hence $A_\infty$ is a subgroup of $Perm(S)$. Assume that $N \neq \{1\}$ be a normal subgroup of $A_\infty$. Then there exists an $m \geq 5$ such that $N \cap A_m \neq \{1\}$. But this implies $N \cap A_j \neq \{1\}$ for all $j \geq m$. But $A_j$ is simple. Hence $N \cap A_j = A_j$ i.e. $A_j \leq N$ for all $j \geq 5$. This implies $A_j \leq N$ for all $j$ we get $N = A_\infty$.

(21) Let $\sigma = (1,2)$ and $\tau = (1,2,3,\ldots,n)$ in $S_n$.
a) Determine the centralizer of $\sigma$ in $S_n$.
b) Determine the centralizer of $\tau$ in $S_n$.

**Solution:** (a) Let $\sigma = (1,2)$ and $\beta$ be any permutation in $S_n$. Then $\sigma^\beta = \sigma$ means that $(12)^\beta = (1\beta, 2\beta) = (1,2)$. So $\beta$ could be a permutation on the set $\{1,2\}$. So this element is either 1 or $\sigma$ itself. If necessary by multiplying $\beta$ with $\sigma^{-1}$ we get $\sigma^{-1}\beta$ is a permutation on $X = \{3,4,\cdots,n\}$. But any permutation on $X$ commutes with $\sigma$. Hence $C_{S_n}(\sigma) = \langle\sigma\rangle S_{n-2}$ where $S_{n-2}$ is the permutation group on the set $X$.

(b) By considering the answer in part (a), if $\beta \in C_{S_n}(\tau)$ then $(123\cdots n)^\beta = (1\beta, 2\beta, \cdots, n\beta) = (123\cdots n)$. These two elements are equal implies that, if $1\beta = k$ then $2\beta = k+1, 3\beta = k+2, \cdots$. Hence if $1\beta$ is known then $\beta$ is uniquely determined. Therefore we can write at most $n$ elements satisfying this. But we have already $n$ elements satisfying this property, namely the subgroup generated by $\tau$. Hence $C_{S_n}(\tau) =< \tau >$ .

(22) Suppose $G$ is a finite group, $H \lhd G$, and $P$ is a Sylow $p$-subgroup of $H$. Set $N = N_G(P)$. Show that $G = NH$.

Hint: If $x \in G$, then $P^x$ is a Sylow $p$-subgroup of $H$.

**Solution:** Let $x \in G$ and $P \in Syl_p H$. Then $P^x \leq H^x = H$. Hence $P$ and $P^x$ are Sylow $p$-subgroups of $H$. By Sylow theorem any two Sylow $p$-subgroups of $H$ are conjugate in $H$. Hence there exists $h \in H$ such that $P^{xh} = P$. That means $xh \in N$. This implies $x \in NH$ Since $x$ is an arbitrary element of $G$ we get $G = NH$.

(23) If $G$ is a finite $p$-group and $1 \neq H \lhd G$. Show that $H \cap Z(G) \neq 1$.

Hint: $H$ is an union of $G$ conjugacy classes.

**Solution:** For a finite $p$-group $G$, we have upper central series of $G$.

$\{1\} = Z_0 \lhd Z_1 \lhd \cdots \lhd Z_n = G$ where $Z_i/Z_{i-1} = Z(G/Z_{i-1})$. Since $H \neq \{1\}$ there exists an $i$ such that $Z_i \cap H \neq \{1\}$ but $Z_{i-1} \cap H = 1$.

Since $H$ is normal, we have $[G,H] \leq H$ and $Z_i \cap H \leq Z_i$ implies $[Z_i \cap H, G] \leq Z_{i-1} \cap H = 1$. It follows that $Z_i \cap H \leq Z(G)$, i.e. $Z_i \cap H \cap Z(G) = Z_i \cap H \neq \{1\}$. Hence $H \cap Z(G) \neq 1$.

**Remark:** The above proof can be adopted to show that

If $G$ is a finite nilpotent group and $1 \neq H \lhd G$. Show that $H \cap Z(G) \neq 1$.

(24) Suppose $G$ is a finite $p$-group having a unique subgroup of index $p$. Show that $G$ is cyclic. (Use induction and look at $G/Z(G)$)

**Solution:** We use induction on the order of $G$. If $|G| = p$, then $G$ is cyclic. Assume that if $H$ is *a* $p$-group and $|H| \lneqq |G|$ and $H$ has a unique subgroup of index $p$, then $H$ is cyclic. Since $G$ is $p$-group, we know that $Z(G) \neq \{1\}$, $|G/Z(G)| \lneqq |G|$. Let $X$ be the unique subgroup of $G$ of index $p$. Since $N_G(X) \gneqq X$ we get $X \lhd G$. $XZ(G)/Z(G) \leq G/Z(G)$.

Claim: $XZ(G) \lneqq G$.

$Z(G) \lhd G$ and $G$ is a $p$-group. Therefore there exists an upper central series of $G$ containing $Z(G)$ say $\{1\} = Z_0(G) \lhd Z_1(G) \lhd \cdots \lhd Z_k(G) = G$. Since $G/Z_{k-1}$ is abelian $p$-group there exists a subgroup of $G/Z_{k-1}$ of index $p$ say $T/Z_{k-1}$. Then $T$ has index $p$ in $G$. Since $G$ has a unique subgroup of index $p$ we get $T = X$, i.e. $Z(G) \leq X$ and the case $XZ(G) = G$ is impossible.

$XZ(G) \lneqq G$, then as $X$ is maximal subgroup we get $Z(G) \leq X$ and $[G/Z(G) : X/Z(G)] = p$. The group $G/Z(G)$ has a unique subgroup of index $p$, then by induction assumption $G/Z(G)$ is cyclic. This implies that $G$ is abelian $p$-group and has a unique subgroup of index $p$. Using fundamental theorem of finite abelian groups one can easily see that $G$ is cyclic.

(25) Suppose that $G$ is a finite $p$-group. Show that $Z(G)$ is cyclic if and only if $G$ has exactly one normal subgroup of order $p$.

**Solution:** Assume that $Z(G)$ is cyclic but $G$ has two normal subgroups $N$ and $M$ of order $p$. Then by question 23, $N \cap Z(G) \neq \{1\}$ and $M \cap Z(G) \neq \{1\}$. Since $N$ has order $p$ we get $N \leq Z(G)$, and $M \leq Z(G)$. But in the cyclic group $Z(G)$ there exists only one subgroup of order $p$. This implies $N = M$.

Conversely assume that $G$ has exactly one normal subgroup of order $p$ but $Z(G)$ is not cyclic. Since $Z(G)$ is abelian it can be written as a direct product of cyclic subgroups. It has at least two component. As each component gives a normal subgroup of order $p$. We get $Z(G)$ must be cyclic.

(26) Show that there are no simple groups of order 104, 176, 182 or 312.

**Solution:**

(i) $104 = 13.2^3$. Let $n_{13}$ be the number of Sylow 13-subgroups of $G$. $n_{13} \equiv 1 \pmod{13}$ and $n_{13}|8$ implies $n_{13} = 1$. Hence Sylow 13-subgroup of $G$ is normal in $G$.

(ii) $176 = 11.2^4$. $n_{11} \equiv 1 \pmod{11}$ and $n_{11}|2^4$. Therefore $n_{11} = 1$. Hence Sylow 11-subgroup of $G$ is normal in $G$.

(iii) $182 = 13.7.2$ $\quad n_7 \equiv 1 \pmod 7$ $n_7|13.2$ so $n_7 = 1$. Hence Sylow 7-subgroup of $G$ is unique. This implies Sylow 7-subgroup of $G$ is normal in $G$.

(iv) $312 = 13.3.2^3$ $n_{13} \equiv 1 \pmod{13}$ $\quad n_{13}|3.2^3$. So $n_{13} = 1$. This implies Sylow 13-subgroup of $G$ is normal in $G$.

(27) There is a simple group $G$ of order 168. Show that $G$ has 48 elements of order 7.

**Solution:** Let $G$ be a simple group of order $168 = 7.3.2^3$. Let $n_p$ be the number of Sylow $p$-subgroups of $G$. $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 3.2^3$ $\quad n_7 = 1$ or 8.

Since $G$ is simple $n_7$ cannot be equal to 1. It follows that $n_7 = 8$. That means number of Sylow 7-subgroups of $G$ is 8. Intersection of any two distinct Sylow 7-subgroups is identity. Hence there are 6 elements of order 7 in each Sylow 7-subgroup. Therefore all together we have 48 elements of order 7 in $G$.

(28) If $p$ and $q$ are primes show that any group of order $p^2q$ is solvable.

**Solution:** i) $p = q$ then $G$ is a $p$-group hence solvable.

ii) $p > q$ then $n_p \equiv 1 \pmod p$ and $n_p|q$. But this implies $n_p = 1$ as $p > q$. Hence the Sylow $p$-subgroup $P$ of $G$ is normal in $G$. It follows that $G/P$ is a $q$-group, hence solvable. $P$ is a $p$-group so $P$ is solvable. Hence $G$ is solvable. (In fact $P$ is abelian and $G/P$ is cyclic.)

(iii) $p < q$ then $\begin{array}{ll} n_p \equiv 1 \ (mod\ p) & n_p | q \\ n_q \equiv 1 \ (mod\ q) & n_q | p^2. \end{array}$ Since $q > p$ the possibilities for $n_q$ are $1, q+1, kq+1$ and divide $p^2$. If $n_q = 1$, then Sylow $q$-subgroup $Q$ of $G$ is normal in $G$. Hence $|G/Q| = p^2$. Then it is abelian. $Q$ is cyclic. Hence $G$ is solvable. Assume that $n_q = kq+1, k \geq 1$. If $n_p = 1$, then by above part $G$ is solvable. So assume that $n_p = q$.

**Fact 1.**

If there exists a normal subgroup $N$ of $G$ then $G/N$ and $N$ are solvable implies $G$ is solvable.

Claim: $G$ is not simple.

Assume if possible that $G$ is simple. Let $P_1, P_2$ be two distinct Sylow $p$-subgroups of $G$. If $\{1\} \neq P_1 \cap P_2$, then $|P_1 \cap P_2| = p$. Then $P_1 \cap P_2 \leq Z(\langle P_1, P_2 \rangle)$ as any group of order $p^2$ is abelian. It follows that $T = \langle P_1, P_2 \rangle \neq G$. But $P_1 \lneqq T \leq G$ and $|G| = p^2 q$, $|T| \mid |G|$ implies that $P_1 \cap P_2 = \{1\}$. Then we get $q(p^2-1) = p^2q - q$ elements of order a power of $p$. So there are only $q$ elements coming from Sylow $q$-subgroup. This implies Sylow $q$-subgroup $Q$ is unique. Hence $G$ cannot be simple.

**Fact 2:**Any group of order $pq$ is solvable. Now combining Fact 1 and Fact 2, one can show that $G$ is solvable.

(29) If $G$ is a finite $p$-group, show that the composition factors of $G$ are isomorphic to $Z_p$.

**Solution:** Let $G$ be a finite $p$-group. Then $G$ has an upper central series $\{1\} = Z_0 \lhd Z_1 \lhd Z_2 \lhd \cdots \lhd Z_n = G$ where $Z_i/Z_{i-1} = Z(G/Z_{i-1})$. Therefore $Z_i/Z_{i-1}$ is the center of $G/Z_{i-1}$. In particular $Z_i/Z_{i-1}$ is an abelian $p$-group. Therefore by Cauchy's theorem it has a subgroup of order $p$ say $Z_{i1}/Z_{i-1} \leq Z_i/Z_{i-1}$. Since $Z_i/Z_{i-1}$ is abelian every subgroup is normal in particular $Z_{i1} \lhd Z_i$. If $Z_{i1} \neq Z_{i-1}$, then consider $Z_i/Z_{i1}$ and find a subgroup $Z_{i2}/Z_{i1} \leq Z_i/Z_{i1}$ of order $p$. Hence we can refine in the upper central series of $G$ the part $Z_{i-1} \lhd Z_i$ to $Z_{i-1} \lhd Z_{i1} \lhd Z_{i2} \lhd \cdots \lhd Z_i$ where each factor is of order $p$ hence isomorphic to $Z_p$. We can do this for each $i$. We get a series of $G$ in which each factor isomorphic to $Z_p$.

(30) If $A$ and $B$ are subnormal subgroups of $G$ show that $A \cap B$ is subnormal.

**Solution:** $A$ is subnormal in $G$ implies that there exists a series $A = A_0 \lhd A_1 \lhd A_2 \lhd \cdots \lhd A_n = G$. The group $B$ is subnormal in $G$ implies that there exists a series

$$B = B_0 \lhd B_1 \lhd B_2 \lhd \cdots \lhd B_m = G.$$

Then take the intersection with $B$ of the series of $A$ we get

$$A \cap B = A_0 \cap B \lhd A_1 \cap B \lhd \cdots \lhd A_n \cap B = G \cap B = B.$$

Therefore

$$A \cap B \lhd A_1 \cap B \lhd \cdots \lhd A_n \cap B = B \lhd B_1 \lhd B_2 \lhd \cdots \lhd B_n = G$$

is a series of $A \cap B$. Hence $A \cap B$ is subnormal in $G$.

(31) If $p$ is a prime, $|G| = p^3$ and $G$ is not abelian show that $G' = Z(G)$.

**Solution:** Recall that any finite $p$-group is solvable and $Z(G) \neq \{1\}$. Therefore by assumption $\{1\} \neq G' \lneqq G$. Since $Z(G) \neq G$, $G/Z(G)$ is a non-trivial group. If $G/Z(G)$ is cyclic then $G$ is abelian. Hence $|G/Z(G)| = p^2$. This implies that $G/Z(G)$ is an ( elementary ) abelian group of order $p^2$. Hence $G' \leq Z(G)$. As $G' \neq \{1\}$ and $|Z(G)| = p$ we get $G' = Z(G)$.

(32) If $G$ is a group and $x \in G$, define the inner automorphism $f_x$ by setting $f_x(y) = xyx^{-1}$, all $y \in G$. Write $I(G)$ for the set of all inner automorphisms of $G$.

1) Show that $I(G) \leq Aut(G)$

2) Show that $I(G) \cong G/Z(G)$

3) If $I(G)$ is abelian show that $G' \leq Z(G)$. Conclude that $G$ is nilpotent.

**Solution:** 1) $f_x : G \to G$, $f_x(uv) = xux^{-1}xvx^{-1} = f_x(u)f_x(v)$. Hence $f_x$ is a homomorphism.

$f_x(u) = f_x(v)$ implies $xux^{-1} = xvx^{-1}$. It follows that $u = v$. For any $u \in G$, $f_x(x^{-1}ux) = xx^{-1}uxx^{-1} = u$. Hence $f_x$ is an automorphism of $G$.

$f_xf_y(g) = f_x(ygy^{-1}) = xygy^{-1}x^{-1} = f_{xy}(g)$ for all $g \in G$. Hence composition of two inner automorphism is an inner automorphism $f_xf_y = f_{xy}$ and $f_{x^{-1}} = (f_x)^{-1}$. i.e. inverse of an inner automorphism is again an inner automorphism. Hence $I(G)$ is a subgroup of $Aut(G)$.

2) Define a map $f : \begin{array}{ccc} G & \to & Aut(G) \\ x & \mapsto & f_x \end{array}$. The map $f$ is a homomorphism. For any $x, y \in G$, $f(xy)(u) = f_{xy}(u) = xyu(xy)^{-1} = xyuy^{-1}x^{-1} = f_xf_y(u)$ for all $u \in G$. Hence $f(xy) = f_{xy} = f_xf_y = f(x)f(y)$.

$$Kerf = \{x \in G \mid f_x = Id\} = \{x \in G \mid f_x(u) = u \quad \text{for all } u \in G\} = Z(G).$$

Hence by isomorphism theorem,

$G/Z(G) \cong I(G)$ as image of $f$ is $I(G)$.

3) If $I(G)$ is abelian then by part (2) we have $G/Z(G)$ is abelian. This implies $G' \leq Z(G)$. Then $[G', G] \leq [Z(G), G] = 1$. Hence $G$ is nilpotent of class at most 2.

(33) If $A \lhd G$ and $B \lhd G$ show that $G/(A \cap B)$ is isomorphic with a subgroup of $G/A \times G/B$.

**Solution:** $A \lhd G$ and $B \lhd G$ implies that $A \cap B \lhd G$. Define a map

$$\varphi : \begin{array}{ccc} G/A \cap B & \to & G/A \times G/B \\ (A \cap B)x & \to & (Ax, Bx) \end{array}$$

It is easy to show that $\varphi$ is well defined. $\varphi$ is a homomorphism. $Ker\varphi = \{(A\cap B)x \mid (Ax, Bx) = (A, B)\} = \{A \cap B\}$. Hence $\varphi$ is a monomorphism. It follows from isomorphism theorems that $G/A \cap B$ is isomorphic to the image of $\varphi$ in $G/A \times G/B$.

(34) If $G$ is a finite $p$-group that is not cyclic show that there is a homomorphism from $G$ onto $Z_p \times Z_p$. (Hint: Let $A$ and $B$ be distinct maximal subgroups of $G$ and apply previous question.)

**Solution:** Since $G$ is not cyclic by question **24** $G$ has at least two distinct maximal subgroups $A$ and $B$. Since maximal subgroups of finite $p$-groups have index $p$ in $G$ (one can observe this by looking to the central series of $G$). We get $G/A\cap B \to G/A \times G/B \cong Z_p \times Z_p$. Since $A \neq B, |G/A \cap B\| \geq p^2$. Hence $G/(A \cap B) \cong G/A \times G/B$. Since there exists natural epimorphism from $G$ to $G/A \cap B$ we get $G \xrightarrow{\pi} G/A \cap B \to Z_p \times Z_p$ an epimorphism.

(35) If $A, B \leq G$ show that $[A, B] \trianglelefteq \langle A \cup B\rangle$.

**Solution:** $[A, B] = \langle a^{-1}b^{-1}ab \mid a \in A, b \in B\rangle$. It is enough to show that $[A, B]$ is normalized by $A$ and $B$. Let $a^{-1}b^{-1}ab$ be any generator of $[A, B]$ and $\alpha \in A$. then

$$\begin{aligned}
(a^{-1}b^{-1}ab)^{\alpha} &= \alpha^{-1}a^{-1}b^{-1}ab\alpha \\
&= (\alpha^{-1}a^{-1})b^{-1}a\alpha\alpha^{-1}b\alpha \\
&= (a\alpha)^{-1}b^{-1}a\alpha bb^{-1}\alpha^{-1}b\alpha = [a\alpha, b][b, \alpha]
\end{aligned}$$

Since $a, \alpha \in A$, $a\alpha \in A$ hence $[a\alpha, b] \in [A, B]$ and $[b, \alpha] = [\alpha, b]^{-1} \in [A, B]$. Hence $[A, B]$ is normalized by $A$. Similarly for $\beta \in B$ and $[a, b]^{\beta} = [\beta, a][a, b\beta]$, $[\beta, a] = [a, \beta]^{-1} \in [A, B], b, \beta \in B$ implies $b\beta \in B$. Hence we get $[A, B]$ is normalized by $B$. In particular $[A, B]$ is normalized by $\langle A \cup B\rangle$. It is clear that $[A, B] \leq \langle A \cup B\rangle$. Hence $[A, B] \lhd \langle A \cup B\rangle$

(36) If $G$ is a finite group in which every maximal subgroup is normal show that $G$ is nilpotent. (Hint: Suppose to the contrary that $P$ is

a non-normal Sylow $p$-subgroup and choose $M \leq G$ maximal with $N_G(P) \leq M$. If $x \in G \setminus M$ consider $P^x$.)

**Solution:** Recall that $G$ is nilpotent if and only if $G$ is a direct product of Sylow $p$-subgroups. We show that in the above conditions Sylow $p$-subgroups are normal. Assume if possible that $P$ is a Sylow $p$-subgroup of $G$ but $P$ is not normal in $G$. Then $P \leq N_G(P) \lneqq G$. Let $M$ be a maximal subgroup of $G$ containing $N_G(P)$. Hence by assumption $M$ is normal in $G$. For any $x \in G \setminus M$, we get $P \neq P^x \leq M$. Hence there exists $m \in M$ such that $P^{xm} = P$. It follows that $xm \in N_G(P) \leq M$. Since $m \in M$ we get $x \in M$ which is a contradiction. Hence $P \lhd G$ and the result follows.

(37) If $G = \langle a, b | a^4 = b^3 = 1, ab = ba^3 \rangle$, show that $G$ is cyclic of order 6.

**Solution:** $aba = ba^4 = b$. Then

$$\begin{aligned} 1 = b^3 &= (aba)(aba)(aba) \\ &= aba^2.ba^2.ba \end{aligned}$$

multiply from left and right by $a^{-1}$ we get

$$ba^2ba^2b = a^{-2} = a^2$$

Thus $a^2 = ba(aba)ab = babab = b^3 = 1$. This gives $b^3 = a^2 = 1$.

Hence we get $a^2 = 1$. This gives $ab = baa^2 = ba$. Hence $G$ is an abelian group. Since every element is of the form $a^i b^j$ we get $|G|$ is a divisor of 6. We may conclude that $|G| = 6$. i.e. $G$ is an abelian group of order 6. The order of $ab$ is 6. Hence $G$ is cyclic group of order 6, as $G = \langle \ ab \ | \ (ab)^6 = 1 \ \rangle$.

(38) Prove that there exists no simple group of order $180 = 2^2.3^2.5$

**Proof:** Let $n_2$ be the number of Sylow 2-subgroups. $n_3$ be the number of Sylow 3-subgroups, $n_5$ be the number of Sylow 5-subgroups.

(1) If one of $n_2, n_3, n_5$ is equal to 1, then the corresponding Sylow subgroup is normal in $G$. Hence we may assume that $n_i > 1$ for $i = 2, 3, 5$. If $n_i \leq 5$ for some $i = 2, 3, 5$, then $G$ can be embedded

in $S(n_i)$ but $|S_5| = 120$. Hence there must be a kernel but this implies $G$ is not simple. It follows that we may assume $n_i \geq 6$ for all $i = 2, 3, 5$ and $G$ is a simple group.

(2) if $n_5 = 6$, then there exists a homomorphism $\varphi : G \to S_6$. Since $G$ is simple $ker\varphi = \{1\}$. Hence $G$ is isomorphic to a subgroup of $S_6$. But $G' = G$ as $G' \trianglelefteq G$ and $G$ is simple. Hence $G = G' \leq S_6' = A_6$. But $|A_6| = 360$ and $|G| = 180$. But $A_6$ is simple hence it cannot have a subgroup of index 2. This implies that $n_5 > 6$ $n_5|36$, $n_5 \equiv 1 \pmod{5.}$ So $n_5 = 36$. This implies that $[G : N_G(P_5)] = 36$ i.e. $N_G(P_5) = P_5$ as $|N_G(P_5)| = 5$, where $P_5$ is a Sylow 5-subgroup of $G$.

(3) Let $H_1, H_2 \in Syl_3(G)$ $J = \langle H_1, H_2 \rangle, D = H_1 \cap H_2$. Then we shall see that $D \leq Z(J)$ and $[J : H_1] \geq 4$. Since $|H_1| = |H_2| = 3^2$, $H_1$ and $H_2$ are abelian groups. Hence $D \leq Z(J)$. Moreover the group $J$ has order $\gneqq 9$ as $H_1 \neq H_2$. Moreover $|H_1 \cap H_2| \leq 3$. If $[J : H_1] = 2$, then $H_1 \lhd J$ and $H_2$ normalizes $H_1$ i.e. $H_1H_2$ is a subgroup of $G$. But $|H_1H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} = \frac{3^2 3^2}{3} = 3^3$ this implies $3^3| \, |G|$ which is impossible. Since $H_1$ and $H_2$ are Sylow 3-subgroups $|J : H_1| \neq 3$. Hence $|J : H_1| \geq 4$.

(4) By (3), $|J| \geq 36$. If $D \neq 1$, then $J \neq G$ as $G$ is simple and $D \lhd J$. If $D \neq 1$ and $5||J|$, then Sylow 5-subgroup is contained in $J$ and $D$ normalizes Sylow 5-subgroup contradicts $N_G(P_5) = P_5$. So $[J : H_1] = 4$ this implies$[G : J] = 5$ and $G$ can be embedded inside $S_5$ but this is impossible. i.e. The intersection of any two distinct Sylow subgroups is trivial.

(5) So $D = 1$. Then we count the elements : $4.36 = 144$ elements of order 5.

$n_3 \equiv 1$, mod 3 and $n_3 | 2^2 5$ and $n_3 \gneqq 5$ implies $n_3 \geq 10$.

$8.10 = 80$ 3-elements.

4 2-elements.

1 identity

Total: 229 elements which is a contradiction.

(39) If $A, B, C$ are subgroups of a group $G, A \subseteq C$ and $AB = BA$ so $AB$ is a group, then $AB \cap C = A(B \cap C)$.

**Solution:** $A \subseteq AB$ and $A \subseteq C$ implies that $A(B \cap C) \subseteq AB \cap C$. For the converse let $x \in AB \cap C$ since $AB = BA$ we can write $x = ab$ where $a \in A, b \in B$. Now $x \in C$ implies $a^{-1}x \in B \cap C$. Hence $x \in A(B \cap C)$.

It follows that $AB \cap C \subseteq A(B \cap C)$ and we get the equality.

(40) Suppose $G$ is an infinite $p$-group (where $p$ is a prime) such that every proper non-trivial subgroup of $G$ has order $p$. (such groups are constructed by Ol'sanskii).

a) Prove that $p > 2$.

b) Prove that $G$ must be simple.

**Solution:** Assume that $p = 2$. Then for any $g \in G$ we get $g^2 = 1$. This implies that $G$ is abelian. Let $x \neq y$ be two elements of $G$, then the subgroup generated by $x$ and $y$ has order 4. But this is a contradiction. Hence $p$ can not be equal to 2.

(b) Assume if possible that, there exists a non-trivial normal subgroup $N$ of $G$. Let $x$ be any element of $G$. Then $\langle x \rangle N$ is a subgroup of $G$. Since $|\langle x \rangle| = p$, the group $\langle x \rangle \cap N$ is either 1 or $\langle x \rangle$. If it is 1, then $|\langle x \rangle N| = p^2$ which is impossible. Hence $\langle x \rangle \cap N = \langle x \rangle$. It follows that for any $x \in G$ the group $\langle x \rangle \leq N$ i.e., $N = G$ and this implies $G$ is simple.

(41) Suppose $G$ is a finite group with 7 Sylow 3-subgroups, each having order 27. Prove that $G$ is not simple.

**Solution:** Let $n_3 = 7$ be the number of Sylow 3-subgroups and $P_3$ be a Sylow 3-subgroup of $G$. Then $|G : N_G(P_3)| = 7$. Now consider the right action of $G$ on the right cosets of $N_G(P_3)$ in $G$. It follows that there exists a homomorphism $\varphi$ from $G$ into $S_7$. $Ker\ \varphi \leq N_G(P_3) \lneqq G$. Hence $G/ker\varphi$ is isomorphic to a subgroup of $S_7$. Since $3^3 \nmid 7!$. We get $\ker\varphi \neq \{1\}$. Hence $G$ is not simple.

(42) Suppose $G$ and $H$ are groups. Assume $N \trianglelefteq G$ such that $N \cong S_5$ and $G/N \cong S_3 \times Z_2$. Also assume that $M \trianglelefteq H$ with $M \cong Z_2$ and $H/M \cong S_6$. Prove that $G$ is not isomorphic to $H$.

**Solution:** $G$ has a composition series

$$G \rhd M_1 \rhd M_2 \rhd M_3 = N \rhd M_4 \cong A_5 \rhd 1.$$

$$G/M_1 \cong \mathbf{Z}_2, \quad M_1/M_2 \cong A_3, \quad M_2/M_3 \cong \mathbf{Z}_2, \quad M_3/M_4 \cong \mathbf{Z}_2.$$

$M_4 \cong A_5$. Hence composition factors of $G$ are $\{\mathbb{Z}_2, A_3, \mathbb{Z}_2, \mathbb{Z}_2, A_5\}$

$$H \rhd H_1 \rhd H_2 = M \rhd 1$$

$H/M \cong S_6$ so there exist a subgroup $H_1/M$ in $H/M$ such that $(H/M)/(H_1/M) \cong H/H_1 \cong \mathbf{Z}_2$ and $H_1/M \cong A_6$. Recall that $A_n$ is simple if $n \neq 4$. Hence composition factors of $H$ are isomorphic to $\{\ \mathbf{Z}_2, A_6, \mathbf{Z}_2\ \}$. By Jordan-Holder Theorem $G$ and $H$ can not be isomorphic.

# RINGS

(43) Let $R$ be a commutative ring and let $S$ be a subset of $R^*$ that is a multiplicative semigroup containing no zero divisors. Let $X$ be the Cartesian product $R \times S$ and define a relation $\sim$ on $X$ by agreeing that $(a, b) \sim (c, d)$ if and only if $ad = bc$.

(1) Show that the relation $\sim$ just defined is an equivalence relation on $X$.

(2) Denote the equivalence class of $(a, b)$ by $\frac{a}{b}$ and the set of all equivalence classes by $R_S$. Show that $R_S$ is a commutative ring with 1.

(3) If $a \in S$ show that $\{\frac{ra}{a} | r \in R\}$ is a subring of $R_S$ and that $r \to \frac{ra}{a}$ is a monomorphism, so that $R$ can be identified with a subring of $R_S$.

(4) Give a "universal definition" for the ring $R_S$ and show that $R_S$ is unique up to isomorphism.

The ring $R_S$ is called the **localization** of $R$ at $S$.

**Solution:**

1) (i) $\sim$ is reflexive: For any $(a, b) \in R \times S$, $ab = ba$. Hence $(a, b) \sim (a, b)$.

(ii) $\sim$ is symmetric: $(a, b) \sim (c, d)$ implies $ad = bc = cb = da$. Hence $(c, d) \sim (a, b)$

(iii) $\sim$ is transitive: $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ implies that $ad = bc$ and $cf = de$. Then $adf = bcf = bde$. Hence we get $(af - be)d = 0$. Since $d \in S$ and $S$ does not contain zero divisor we get $af - be = 0$. Hence $af = be$, equivalently $(a, b) \sim (e, f)$.

We conclude that $\sim$ is an equivalence relation.

(2) Let $\frac{a}{b} = \{(c, d) \ | (a, b) \sim (c, d) \ \}$. Let $R_S = \{\frac{a}{b} \ | \ a \in R, b \in S\}$.

Define addition and multiplication on $R_S$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad bd \in S$$

We first show that these definitions are well defined. If $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then $ab' = ba'$ and $cd' = dc'$. Hence $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$, or equivalently

$$\begin{aligned}(a'd' + b'c')bd &= a'd'bd + b'c'bd \\ &= ab'd'd + b'bd'c \\ &= (ad + bc)b'd'\end{aligned}$$

For multiplication $\frac{a}{c} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{a'c'}{b'd'}$. Equivalently we need to show $acb'd' = bda'c'$ Let's begin from the left hand side.

$$\begin{aligned}acb'd' = a'bcd' &= a'bc'd \\ &= a'c'.bd\end{aligned}$$

Hence multiplication is well defined. In the above, observe that we used $S$ is multiplicatively closed because we need $bd \in S$.

One can see easily that with the above addition and multiplication $R_S$ is a commutative ring. $\frac{a}{b} \cdot \frac{b}{b} = \frac{ab}{bb}$. But $\frac{ab}{bb} = \frac{a}{b}$ because $(ab, bb) \sim (a, b)$. Hence the equivalence class $\frac{b}{b}, b \in S$ is the identity in $R_S$.

(3) For $a \in S$, let $T = \{\frac{ra}{a} : r \in R\}$ and $\frac{r_1a}{a}, \frac{r_2a}{a}$ be two elements from $T$. Then

$$\frac{r_1a}{a} - \frac{r_2a}{a} = \frac{r_1a - r_2a}{a} = \frac{(r_1 - r_2)a}{a} \in T$$

and

$$\frac{r_1a}{a} \cdot \frac{r_2a}{a} = \frac{r_1r_2a^2}{a^2} = \frac{r_1r_2a}{a} \in T.$$

Hence $T$ is a subring of $R_S$.

Let $i : \begin{array}{ccc} R & \to & T \\ r & \to & \frac{ra}{a} \end{array}$

$$i(r_1 + r_2) = \frac{(r_1 + r_2)a}{a} = \frac{r_1a + r_2a}{a} = \frac{r_1a}{a} + \frac{r_2a}{a} = i(r_1) + i(r_2)$$

$$i(r_1r_2) = \frac{r_1r_2a}{a} = \frac{r_1r_2a^2}{a^2} = \frac{r_1a}{a}\frac{r_2a}{a} = i(r_1)i(r_2)$$

$i(r_1) = i(r_2)$ implies that $\frac{r_1a}{a} = \frac{r_2a}{a}$

$$0 = \frac{r_1a - r_2a}{a} = \frac{(r_1 - r_2)a}{a}.$$

This implies that $(r_1 - r_2)a = 0$, as $a \in S$ and $S$ does not have a zero divisor. Hence $r_1 - r_2 = 0$. i.e. $r_1 = r_2$. It follows that $i$ is a monomorphism of rings.

(4) Let $a \in S$. Recall that $\frac{a}{a}$ is the identity element of $R_S$. Let $a \to \frac{a^2}{a} \in R_S$ and $\frac{a}{a^2} \in R_S$. Then

$$\frac{a^2}{a} \cdot \frac{a}{a^2} = \frac{a^3}{a^3} = \frac{a}{a}.$$

Hence $\frac{a}{a^2}$ is the multiplicative inverse of $\frac{a^2}{a}$ in $R_S$.

Let $S$ be a multiplicative semigroup of a ring $R$ which does not have a zero divisor. Let $T$ be a ring and $\varphi : R \to T$ be a ring homomorphism such that for every $s \in S, \varphi(s)$ invertible in $T$. Then there exists a unique ring homomorphism $f$ from $R_S$ into $T$ satisfying $f.i = \varphi$.

$$\begin{tikzcd}
R \arrow[rr, "i"] \arrow[dr, "\varphi"'] & & R_S \arrow[dl, "f"] \\
& T &
\end{tikzcd}$$

To see that $R_S$ is unique satisfying this property. Let $\sum$ and $\beta$ be another pair satisfying this property. Then

$$\begin{tikzcd}
R \arrow[rr, "i"] \arrow[dr, "j"'] & & R_S \arrow[dl, shift right, "f"'] \\
& \Sigma \arrow[ur, shift right, "\beta"'] &
\end{tikzcd}$$

$f\beta = id_{R_S}$ and $\beta f = id_{\sum}$. Hence $f$ and $\beta$ are invertible ring homomorphism i.e. isomorphisms of rings.

The ring $R_S$ is called localization of $R$ at $S$.

(44) Suppose $R$ is an integral domain and $P \subseteq R$ a prime ideal.

(1) Show that both $P$ and $R \setminus P$ are multiplicative semigroups.

(2) If $S = R \setminus P$ show that $U(R_S) = R_S \setminus R_S P$ conclude that $R_S P$ is the unique maximal ideal in $R_S$.

**Solution:** (1) It is clear that $P$ is a multiplicative semigroup. Let $x, y \in R \setminus P$. Then $xy \in R \setminus P$. Indeed if $xy \in P$, then either $x \in P$ or $y \in P$ as $P$ is a prime ideal. But this is impossible.

(2) By previous exercise we have localization of $S = R \setminus P$. Now we show that $U(R_S) = R_S \setminus R_S P$. Let $x \in U(R_S)$. Assume if possible that $x \in R_S P$. Then $x = \frac{p}{s}$, where $p \in P$ and $s \in S$. Then there exist $\frac{a}{s'} \in R_S$ such that $\frac{a}{s'}\frac{p}{s} = 1$. Then $ap = s's$ and this implies $ss' \in P$. Then either $s \in P$ or $s' \in P$. This is a contradiction.

Observe that $R_S P$ is an ideal of $R_S$. Assume that $x \in R_S \setminus R_S P$. Then $x = \frac{a}{s}$ where $a \notin P$. Then $a \in R \setminus P = S$. It follows that $x \in U(R_S)$

**A field of fractions** of an integral domain $R$ is a localization of $R$ at $R^* = R \setminus \{0\}$. In particular field of fractions of an integral domain is a special case of localization. Another definition for a field of fractions of an integral domain $R$:

A field of fractions for an integral domain $R$ is a field $F_R$ with a monomorphism $\phi : R \to F_R$ such that if $K$ is any field and $\theta : R \to K$ a monomorphism then there is a unique homomorphism (necessarily a monomorphism) $f : F_R \to K$ for which the diagram commutes i.e. $\theta = f\phi$.

$$\begin{tikzcd} R \arrow[rr, "\phi"] \arrow[dr, "\theta"'] & & F_R \arrow[dl, "f"] \\ & K & \end{tikzcd}$$

(45) Find the invertible elements $U(R)$ in $R$, if $R = \mathbf{Z}_4[x]$. $\mathbf{Z}_4 = \{0, \bar{1}, \bar{2}, \bar{3}\}$. $\bar{1}$ and $\bar{3}$ are invertible in $\mathbf{Z}_4$.

**Solution:** Consider the homomorphism

$$Z_4[x] \to Z_2[x]$$

$$f = \sum a_i x^i \to \bar{f} = \sum \bar{a}_i x^i$$

obtained from the homomorphism $Z_4 \to Z_2 \cong Z_4/2Z_4$. Then $fg = 1$ implies that by homomorphism properties $\bar{f}\bar{g} = 1$. Since $Z_2$ is a field we get $Z_2[x]$ is an integral domain. Hence by degree properties $\bar{f} = \bar{a_0} = \bar{1}$ and $\bar{g} = \bar{b_0} = \bar{1}$. Thus $f = a_0 + 2\sum c_{i\geq 1} x^i$ with $a_0 \in \{\overline{-1}, \bar{1}\}$ and $a_i \in Z_4$.

Conversely for $f = \pm\bar{1} + \bar{2}\sum a_i x^i$ take $g = \pm\bar{1} - 2\sum a_i x^i$ and get $fg = gf = \bar{1} - (\bar{2}\sum a_i x^i)^2 = \bar{1}$. Thus $f^{-1} = g$. It follows that

$$U(\mathbf{Z}_4[x]) = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_0 \in \{1,3\}, a_i \in \{0,2\}, \quad i = 1,2,3,\cdots,n, n \in \mathbf{Z}\}$$

(46) Suppose $R$ is a commutative ring with 1. If $I$ is an ideal in $R[x]$ and $m$ is a nonnegative integer denote by $I(m)$ the set of all leading coefficients of polynomials of degree $m$ in $I$, together with 0.

(1) Show that $I(m)$ is an ideal in $R$

(2) Show that $I(m) \subseteq I(m+1)$ for all $m$.

(3) If $J$ is an ideal with $I \subseteq J$ show that $I(m) \subseteq J(m)$ for all $m$.

**Solution:**

(1) $I(m) = \{a_m \in R \mid \text{there exists a polynomial } a_m x^m + \cdots + a_0 \in I\} \cup \{0\}$.

Let $a_m, b_m \in I(m)$ and $r \in R$. Then there exists polynomials $f(x) = a_m x^m + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + \cdots + b_1 x + b_0 \in I$.

Since $I$ is an ideal $f(x) - g(x) \in I$ with $a_m - b_m$ is zero or leading coefficient of a polynomial of degree $m$ in $I$. Hence in any case $a_m - b_m \in I(m)$. Now for any $r \in$R we have $rf(x) \in I$. If $ra_m = 0$, then $0 \in I(m)$, if $ra_m \neq 0$, then $rf(x)$ will be a polynomial of degree $m$ in $I$. Hence $ra_m \in I(m)$. As $R$ is a commutative ring we get $I(m)$ is an ideal of $R$.

(2) If $a_m \in I(m)$, then there exists a polynomial $f(x) = a_m x^m + \cdots + a_1 x + a_0 \in I$. Then $xf(x) \in I$ and $xf(x)$ has degree $m+1$. Hence $a_m \in I(m+1)$. This implies

$$I(m) \subseteq I(m+1).$$

(3) Let $J$ be an ideal with $I \subseteq J$ and let $a_m \in I(m)$. Then $f(x) = a_m x^m + \cdots + a_1 x + a_0 \in I \subset J$. Hence $f(x) \in J$ and so $a_m \in J(m)$.

(47) If $R$ is a commutative ring with 1 and $\{x_a \mid a \in A\}$ is an infinite set of distinct commuting indeterminates show that the polynomial ring $R[\{x_a \mid a \in A\}]$ is not Noetherian.

**Solution:** Consider the following chain of ideals. Let $I_i$ be the ideal generated by distinct elements $x_{a_1}, x_{a_2}, \cdots, x_{a_i}$. Then we have $I_1 \subseteq I_2 \subseteq \cdots$ and $x_{a_i}$ is not an element of $I_j$ for $j < i$. Hence this chain is an infinite strictly ascending chain. It follows that $R[\{x_a | a \in A\}]$ is not Noetherian.

(48) Let $m$ be a square free integer. Show that $\mathbf{Q}[\sqrt{m}] = \{r + s\sqrt{m} : r, s \in \mathbf{Q}\}$, and that $\mathbf{Q}[\sqrt{m}]$ is a field. It is thus its own field of fractions, and we will write $\mathbf{Q}(\sqrt{m})$ rather than $\mathbf{Q}[\sqrt{m}]$.

**Solution: (i)** $\mathbf{Q}[\sqrt{m}] = \{a_0 + a_1\sqrt{m} + a_2(\sqrt{m})^2 + a_3(\sqrt{m})^3 + \ldots + a_k(\sqrt{m})^k \mid a_i \in \mathbf{Q}\}$. We can write every element of the form $a_0 + a_1\sqrt{m} + a_2(\sqrt{m})^2 + a_3(\sqrt{m})^3 + \ldots + a_k(\sqrt{m})^k$ in the form $b + t\sqrt{m}$ for some $b, t$ in $\mathbf{Q}$. Hence $\mathbf{Q}[\sqrt{m}] \subseteq \{\ b + t\sqrt{m} \mid b, t \in \mathbf{Q}\}$. Clearly $\{\ b + t\sqrt{m} \mid b, t \in \mathbf{Q}\} \subseteq \mathbf{Q}[\sqrt{m}]$. Hence we have the equality.

Clearly $\mathbf{Q}[\sqrt{m}] \subseteq \mathbb{C}$. We show that $\mathbf{Q}[\sqrt{m}]$ is a subring of $\mathbb{C}$. Let $w_1 = r_1 + s_1\sqrt{m}$ and $w_2 = r_2 + s_2\sqrt{m}$ be two elements of $\mathbf{Q}[\sqrt{m}]$.

Then $w_1-w_2=(r_1-r_2)+(s_1-s_2)\sqrt{m}\in \mathbf{Q}[\sqrt{m}]$ as $r_1-r_2\in\mathbf{Q}$ and $s_1-s_2\in Q$. For $w_1w_2=(r_1r_2+ms_1s_2+(r_1s_2+s_1r_2)\sqrt{m}\in\mathbf{Q}[\sqrt{m}]$ as $r_1r_2+ms_1s_2\in\mathbf{Q}$ and $r_1s_2+s_1r_2\in\mathbf{Q}$. Hence $\mathbf{Q}[\sqrt{m}]$ is a subring of $\mathbb{C}$. It is clear that it is an integral domain with 1.

$$(r_1+r_2\sqrt{m})\cdot\frac{r_1-r_2\sqrt{m}}{r_1^2-mr_2^2}=1.$$

Since $m$ is square free $0\neq r_1^2-mr_2^2\in\mathbf{Q}$. Hence $\frac{r_1}{r_1^2-mr_2^2}-\frac{r_2}{r_1^2-mr_2^2}\sqrt{m}\in \mathbf{Q}[\sqrt{m}]$ is the inverse of $r_1+r_2\sqrt{m}$ in $\mathbf{Q}[\sqrt{m}]$. It follows that every nonzero element of $\mathbf{Q}[\sqrt{m}]$ is invertible. Hence $\mathbf{Q}[\sqrt{m}]$ is a field. Therefore its field of fractions is equal to itself i.e. $\mathbf{Q}[\sqrt{m}]=\mathbf{Q}(\sqrt{m})$.

(49) (1) If $m\in\mathbf{Z}$ show that $I=m\mathbf{Z}=\{mk|k\in\mathbf{Z}\}$ is an ideal of $\mathbf{Z}$.

(2) if $R=M_2(\mathbf{Z})$ and $I=\{\begin{bmatrix} a & 0\\ c & 0\\ & \end{bmatrix}\mid a,c\in\mathbf{Z}\}$ show that $I$ is a left ideal but not a right ideal.

(3) If $R$ is a ring with 1 and $I$ is an ideal (left, right or two-sided) in $R$ such that $I\cap U(R)\neq\phi$ show that $I=R$.

**Solution:** (1) Clearly $I$ is non-empty. Let $mk$ and $mr$ be two elements from $I$. Then $mk-mr=m(k-r)\in I$. For any $s\in\mathbf{Z}$ , $s(mk)=m(sk)\in I$. Since $\mathbf{Z}$ is commutative this implies that $I$ is an ideal.

(2) For any $\begin{bmatrix} x & y\\ z & t\end{bmatrix}\in R$, $\begin{bmatrix} x & y\\ z & t\end{bmatrix}\begin{bmatrix} a & 0\\ c & 0\end{bmatrix}=\begin{bmatrix} ax+yc & 0\\ za+tc & 0\end{bmatrix}\in I$, and

$$\begin{bmatrix} a & 0\\ c & 0\\ & \end{bmatrix}-\begin{bmatrix} u & 0\\ v & 0\\ & \end{bmatrix}=\begin{bmatrix} a-u & 0\\ c-v & 0\\ & \end{bmatrix}\in I$$

Hence $I$ is a left ideal. But

$$\begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} ax & ay \\ cx & cy \end{bmatrix}$$

One can find $a$ and $y$ such that $ay \neq 0$, then $I$ is not a right ideal.

(3) Let $g \in I \cap U(R)$. If $I$ is a left ideal then there exists $g^{-1} \in R$, such that $g^{-1}g = 1 \in I$. Hence for any $r \in R, r1 \in I$. Similarly for right ideal and two sided ideal $I = R$.

(50) Let $R$ be a ring with 1.

(1) Show that the set of units $U(R)$ is a group.

(2) Find $U(R)$ when $R = \mathbf{Z}$ and when $R = \mathbf{Z}_n$.

(3) If $R = M_{2\times 2}(\mathbf{Z})$ show that $U(R)$ is the group of all matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with integer entries such that $ad - bc = \pm 1$.

**Solution:** (1) Let $x$ and $y$ be two elements of $U(R)$. Then there exists $x^{-1}$ and $y^{-1}$ such that $xx^{-1} = x^{-1}x = 1$ and $yy^{-1} = y^{-1}y = 1$. It follows that $(xy)(y^{-1}x^{-1}) = (y^{-1}x^{-1})(xy) = 1$. Hence $xy \in U(R)$. Since $x$ is invertible implies $x^{-1}$ is also invertible we get $U(R)$ is a group.

(2) Let $n \in \mathbf{Z}$ and $n$ be invertible. Then by (1), $\frac{1}{n} \in U(\mathbf{Z})$. This implies that $n = \pm 1$. It is easy to see that $\pm 1$ are invertible. Hence $U(\mathbf{Z}) = \{\pm 1\}$.

Let $R = \mathbf{Z}_n$. Every element $m \in R$ which is relatively prime to $n$ is invertible. Indeed if $(m, n) = 1$, then there exists $x$ any $y \in \mathbf{Z}$ such that $mx + ny = 1$. Hence $\overline{x}$ is the inverse of $m$ in $R$ where bar denotes the element $x$ modulo $n$. $x \equiv \overline{x}$ (mod n).

Assume that $(m, n) = d \neq 1$ and $m$ is invertible. Then $m = dk$, and $n = dl$. If $\overline{ms} \equiv 1$ $(mod\ n)$ for some $s \in \mathbf{Z}$, then $dks \equiv 1$ (mod n). But $dl = n$ implies $ld(ks + l) \equiv l \equiv 0$ $(mod\ n)$ which is a contradiction as $l < n$. Hence the only units $m$ in $\mathbf{Z}_n$ are those with $(m, n) = 1$. $|U(\mathbf{Z}_n)| = \varphi(n)$ where $\varphi$ is Euler $\varphi$ function.

(3) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbf{Z})$ be an invertible matrix in $R$. Then $AA^{-1} = A^{-1}A = I$ It follows that $(detA)(detA^{-1}) = 1$. Hence $detA$ is an invertible element in $Z$. Therefore $detA = ad - bc = \pm 1$.

Converse is clear.

(51) If $R$ is a commutative ring and $a \in R$ Show that the principal ideal $(a)$ has the form $(a) = \{ra + na : r \in R, n \in \mathbf{Z}\}$. Describe the elements of $(a)$ explicitly if $R$ is not necessarily commutative.

**Solution:** Let $S = \{ra + na | r \in R, n \in \mathbf{Z}\}$. We first observe that $S$ is an ideal of $R$ containing $a$. Let $r_1a + n_1a$ and $r_2a + n_2a$ be two elements from the set $S$. Then $(r_1 - r_2)a + (n_1 - n_2)a \in S$ and for any $r \in R, r(r_1a + n_1a) = rr_1a + rn_1a = rr_1a + n_1ra \in S$. Since $R$ is commutative ring we get $S$ is an ideal containing $a$. Hence $(a) \subseteq S$.

Conversely for any $r \in R$, $ra \in (a)$ and for any integer $n$, if positive $na = a + a + \cdots + a \in (a)$ if negative, $na = -a - a - \cdots - a \in (a)$. Hence $ra + na \in (a)$ i.e. $S \subseteq (a)$. It follows that $(a) = S$. If $R$ is not commutative, then

$$(a) = \{r_1a + ar_2 + na + \sum_{i=1}^{m} s_iau_i | r_1, r_2, s_i, u_i \in R, n, m \in \mathbf{Z}, m \geq 0\}$$

Let

$$A = \{r_1a + ar_2 + na + \sum_{i=1}^{m} s_iau_i | r_1, r_2, s_i, u_i \in R, n, m \in \mathbf{Z} \quad m \geq 0\}$$

We show that $A$ is an ideal containing a. It is clear that $a = 1a \in A$. Let

$$w_1 = r_1a + ar_2 + na + \sum_{i=1}^{m} s_iau_i$$

$$w_2 = r_1'a + ar_2' + n'a + \sum_{j=1}^{k} s_{j'}au_j'$$

It is easy to see that $w_1 - w_2 \in A$. Now for any $x \in R$ we have

$$\begin{aligned} xw_1 &= xr_1a + xar_2 + xna + \sum_{i=1}^{m} xs_iau_i \\ &= (xr_1)a + xar_2 + nxa + \sum_{i=1}^{m}(xs_i)au_i \in A. \end{aligned}$$

Similarly, $w_1x \in A$.

Hence $(a) \subseteq A$. One can see that $A \subseteq (a)$. Hence $(a) = A$.

(52) Show that there is no ring $R$ with 1 whose additive group is isomorphic with $\mathbf{Q}/\mathbf{Z}$.

**Solution:** Assume that $f : R^+ \to \mathbf{Q}/\mathbf{Z}$ is an isomorphism of abelian groups. Since $f$ is an isomorphism $0 \neq f(1_R) = \frac{m}{n} + \mathbf{Z}$ where $m < n$. Then $n1_R \in Kerf = \{0\}$. Hence for any $a \in R$, $na = 0$. Let $k$ be an integer greater then $n$ and $\frac{1}{k} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$. Since $f$ is onto, there exists $b \in R$ such that $f(b) = \frac{1}{k} + \mathbf{Z}$. But $0 = f(n.b) = \frac{n}{k} + \mathbf{Z} \neq \mathbf{Z}$, as $n < k$. Hence we obtain a contradiction. Such an isomorphism can not exist.

(53) If $R$ is any ring denote by $R_1$ the additive group $R \oplus \mathbf{Z}$, with multiplication defined by setting

$$(r, n)(s, m) = (rs + mr + ns, nm)$$

Show that $R_1$ is a ring with 1. If $r \in R$ is identified with $(r, 0) \in R$. Show that $R$ is a subring of $R_1$. Conclude that every ring is a subring of a ring with 1.

**Solution:** $R_1$ is an abelian group with respect to addition defined by

$$(r_1, z_1) + (r_2, z_2) = (r_1 + r_2, z_1 + z_2)$$

Since $R$ and $\mathbf{Z}$ are abelian groups, $R_1$ is an abelian group.

Clearly multiplication is closed, since $rs + mr + ns \in R$ and $nm \in \mathbf{Z}$.

$$\begin{aligned}
(r_1,n)[(r_2,m)(r_3,s)] &= (r_1,n)(r_2r_3+sr_2+mr_3,ms)\\
&= (r_1(r_2r_3+sr_2+mr_3)+msr_1+n(r_2r_3+sr_2+mr_3),nms)\\
&= (r_1r_2r_3+sr_1r_2+mr_1r_3+msr_1+nr_2r_3+nsr_2+nmr_3,nms)\\
((r_1n)(r_2,m)](r_3s)) &= (r_1r_2+mr_1+nr_2,nm)(r_3,s)\\
&= ((r_1r_2+nr_2+mr_1)r_3+s(r_1r_2+nr_2+mr_1)+nmr_3,nms)\\
&= (r_1r_2r_3+nr_2r_3+mr_1r_3+sr_1r_2+snr_2+smr_1+nmr_3,nms)
\end{aligned}$$

So

$$[(r_1,n)(r_2,m)](r_3,s)=(r_1,n)[(r_2,m)(r_3,s)].$$

Since $R$ and $\mathbf{Z}$ associate we get multiplication is associative in $R_1$.

$$\begin{aligned}
(r,n)[(r_1,m)+(r_2,s)] &= (r,n)(r_1+r_2,m+s)\\
&= r(r_1+r_2)+(m+s)r+n(r_1+r_2),n(m+s)\\
&= rr_1+rr_2+mr+sr+nr_1+nr_2,nm+ns\\
(r,n)(r_1,m)+(r,n)(r_2,s) &= (rr_1+mr+nr_1,nm)+(rr_2+sr+nr_2,ns)\\
&= rr_1+mr+nr_1+rr_2+sr+nr_2,ns+nm\\
((r,s)+(r_1,s_1))(r_2,s_2) &= (r+r_1,s+s_1)(r_2,s_2)\\
&= ((r+r_1)r_2+s_2(r+r_1)+(s+s_1)r_2,(s+s_1)s_2)\\
&= (rr_2+r_1r_2+s_2r+s_2r_1+sr_2+s_1r_2,ss_2+s_1s_2)\\
(r,s)(r_2,s_2)+(r_1,s_1)(r_2,s_2) &= (rr_2+s_2r+sr_2,ss_2)+(r_1r_2+s_2r_1+s_1r_2,s_1s_2)\\
&= (rr_2+s_2r+sr_2+r_1r_2+s_2r_1+s_1r_2,ss_2+s_1s_2)
\end{aligned}$$

So $R_1$ is a ring.

$$(r,s)(a,b)=(r,s)$$
$$(ra+br+sa,sb)=(r,s)$$

$$\left.\begin{array}{l} ra+br+sa=r \\ sb=s \Rightarrow b=1 \end{array}\right\} \Rightarrow ra+br+sa=r \Rightarrow ra+sa=0$$

This is true for all $r \in R$ and for all $s \in \mathbf{Z}$. For $a = 0, b = 1$ $(r,s)(0,1) = (0,1)(r,s) = (r,s)$.

So, $(0,1)$ is the identity element of $R_1$
$(r,0) - (r_1,0) = (r - r_1, 0) \in R$
$(r,0)(r_1,0) = (rr_1 + 0r + 0r_1, 0) = (rr_1, 0) \in R$
$R$ is a subring of $R_1$ and so every ring can be embeddable in a ring with 1.

(54) (The Binomial Theorem) Suppose $R$ is a commutative ring $a, b \in R$ and $0 < n \in \mathbf{Z}$. Show that

$$(a+b)^n = \sum\{\left(\begin{array}{c} n \\ k \end{array}\right) a^{n-k}b^k, 0 \leq k \leq n\}$$

where

$$\left(\begin{array}{c} n \\ k \end{array}\right) = \frac{n!}{(n-k)!k!}$$

**Proof:** Induction on $n$. If $n = 1$, then

$$(a+b) = \sum_{k=o}^{1} \left(\begin{array}{c} 1 \\ k \end{array}\right) a^{1-k}b^k = \left(\begin{array}{c} 1 \\ 0 \end{array}\right) a + \left(\begin{array}{c} 1 \\ 1 \end{array}\right) b = a+b$$

Assume it is true for $n$. Then

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n(a+b) \quad \text{by induction assumption} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^{k+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k}b^{k+1} + b^{n+1} \\
&= \\
& \quad a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1}b^k + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} [\binom{n}{k} + \binom{n}{k-1}] a^{n-k+1}b^k + b^{n+1}
\end{aligned}$$

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{(n-k)!k!} + \frac{n!}{(n-k+1)!(k-1)!}$$

$$= \quad \frac{n!(n-k+1)+n!k}{(n-k+1)!k!} = \frac{n!(n-k+1+k}{(n-k+1)!k!} = \frac{n!(n+1)}{(n+1-k)!k!}$$

$$= \quad \frac{(n+1)!}{(n+1-k)!k!} = \binom{n+1}{k}$$

hence

$$\begin{aligned}
(a+b)^{n+1} &= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k}b^k + b^{n+1} \\
&= \sum_{n=0}^{k+1} \binom{n+1}{k} a^{n+1-k}b^k
\end{aligned}$$

This completes the proof.

(55) Show that every ideal in $\mathbf{Z}_n$ is principal.

**Solution:** Let $I$ be a non-zero ideal in $\mathbf{Z}_n$. There is a natural order in the elements of $\mathbf{Z}_n$. Assume that $k$ be the minimal non-zero element in $I$. If $m$ is any other element in $\mathbf{Z}_n$. Then write $m = ak + r$ where $0 \leq r < k$. Consider this in $\mathbf{Z}$ and write it modulo $n$. This implies that $r = m - ak \in I$ and $r < k$. Hence $r = 0$. This implies $I = (k)$.

The above proof is the modified version of the proof of statement $\mathbf{Z}$ is a principal ideal domain.

(56) If $F$ is a field show that the ring $M_n(F)$ of all $n \times n$ matrices over $F$ is a simple ring.

**Proof:** Let $E_{ij}$ be an $n \times n$ matrix such that in the $(i, j) - th$ entry it has 1 and zero elsewhere.

$$E_{ij} = \begin{array}{cc} & \begin{array}{ccccc} \phantom{0} & \phantom{0} & \phantom{\cdots} & j & \phantom{\cdots} \end{array} \\ i & \begin{bmatrix} & & & 0 & \cdots \\ & & & . & \\ 0 & 0 & \cdots & 1 & \cdots \\ & & & & \\ & & & & \end{bmatrix} \end{array}.$$

Observe the following properties of $E_{ij}$.

$$E_{ij}E_{ij} = 0 \quad \text{if } i \neq j$$

$$E_{ij}E_{jk} = E_{ik}$$

$$E_{ij}E_{kl} = 0 \quad \text{if} \quad j \neq k.$$

It is clear that $M_n(F)$ can be generated by $\{E_{ij} | i = 1, \cdots, n, j = 1, \cdots, n\}$ as a vector space over $F$ of dimension $n^2$. We first show that if I is a non-zero ideal in $M_n(F)$ and I contains one of $E_{ij}$, then $I = M_n(F)$. To see this, by the above observation it is enough to show that every $E_{lf} \in I$ for all $l = 1, \cdots, n, f = 1, \cdots, n$. Since $E_{ij} \in I$, then $E_{li}E_{ij} = E_{lj} \in I$, $E_{lj}E_{jf} = E_{lf} \in I$. Hence I contains all $E_{lf}$. It follows that $I = M_n(F)$. Hence it is enough to show that every non-zero ideal contains one of $E_{ij}$.

Let $X$ be a non-zero element in $I$, such that $a_{ij}$, the $(i,j)$-th entry is not zero. Then

$$\begin{aligned} E_{ii}XE_{jj} &= \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 \\ 0 & & & 0 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & & a_{1n} \\ a_{i1} & a_{i2} & a_{ij} & a_{in} \\ a_{n1} & a_{n2} & & a_{nn} \\ & & & \end{bmatrix} \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \\ &= E_{ij}(a_{11}E_{11} + a_{12}E_{12} + \cdots + a_{nn}E_{nn})E_{jj} \\ &= (a_{i1}E_{i1} + \cdots + a_{in}E_{in})E_{jj} \\ &= a_{ij}E_{ij} \in I. \end{aligned}$$

This implies $E_{ij} \in I$. Hence $M_n(F)$ is a simple ring.

(57) Suppose $R$ is a commutative ring, $I_1$ and $I_2$ are ideal in $R, P$ is a prime ideal in $R$, and $I_1 \cap I_2 \subseteq P$. Show that $I_1 \subseteq P$ or $I_2 \subseteq P$.

**Solution:** First observe that $I_1 \cap I_2$ is an ideal in $R$. Let $x$ and $y$ be two elements in $I_1 \cap I_2$. Then $x - y \in I_1 \cap I_2$ and for any $r \in R, rx \in I_1$ as $x \in I_1$ and $rx \in I_2$ as $x \in I_2$, hence $rx \in I_1 \cap I_2$. Similarly by commutativity $xr \in I_1 \cap I_2$. Hence $I_1 \cap I_2$ is an ideal of $R$.

Assume that $I_1 \cap I_2 \subseteq P$ and $I_1 \not\subseteq P$ so there exists non-zero element $a_1 \in I_1 \setminus P$. Let $a_2$ be an arbitrary element of $I_2$. Then $a_1a_2 \in I_1 \cap I_2 \subseteq P$. Since $P$ is a prime ideal either $a_1 \in P$ or $a_2 \in P$. But $a_1 \notin P$ hence $a_2 \in P$. But $a_2$ is an arbitrary element of $I_2$ and it is in $P$. Hence $I_2 \subseteq P$.

(58) For a commutative ring $R$ with identity the following are equivalent:

a) $R$ has a unique maximal ideal,
b) all non-units of $R$ are contained in some ideal $M \neq R$,
c) the non-units of $R$ form an ideal,
d) for all $r, s \in R, r + s = 1_R$ implies $r$ or $s$ unit.

Such a ring $R$ is called a **local ring**.

**Solution:** (a) $\Rightarrow$ (b) Let $M$ be the unique maximal ideal of $R$, and let $x$ be a non-unit element of $R$. Since $x$ is non-unit the ideal generated by $x$ namely $Rx$ is a proper ideal of $R$. But in $R$ every proper ideal is contained in a maximal ideal. Hence $Rx \subseteq M$. So $x \in M$.

(b) $\Rightarrow$ (c) Let $x$ and $y$ be two non-unit elements of $R$. Then by assumption $x$ and $y$ in $M$ and $x + y$ is also in $M$ since $M$ is an ideal. Similarly for any $r \in R, rx \in M$. That means $x + y$ and $rx$ are non-units because $M \neq R$. Hence the sum of two non-unit elements is non-unit and multiplication by an element $r \in R$ is also non-unit. It follows that the set of non-units of $R$ forms an ideal.

(c) $\Rightarrow$ (d) If both $r$ and $s$ are non-units, then their sum must be non-unit by assumption. Since $1_R$ is a unit either $r$ or $s$ must be a unit.

(d) $\Rightarrow$ (a) Let $M_1$ and $M_2$ be two different maximal ideals of $R$. Then $M_1 + M_2 = R$. It follows that there exists $m_1 \in M_1$ and $m_2 \in M_2$ such that $m_1 + m_2 = 1$. Now by assumption either $m_1$ or $m_2$ invertible. This implies either $M_1 = R$ or $M_2 = R$. Hence there exists a unique maximal ideal.

(59) Suppose $R$ is a commutative ring with 1 and $x \in \cap\{M : M$ is maximal ideal in $R\}$. Show that $1 + x \in U(R)$.

**Solution:** Recall the fact that in a commutative ring with 1, every proper ideal is contained in a maximal ideal. Assume that $1+x$ is not invertible. Then the ideal generated by $1+x$ is a proper ideal, hence contained in a maximal ideal $M$. But then $1 + x \in M$ and by assumption $x \in M$ implies that $1 + x - x \in M$. Which is impossible as $M$ is a maximal ideal, $M \neq R$.

(60) An element $a$ of a ring $R$ is called nilpotent if $a^n = 0$ for some positive integer $n$. Show that the set of nilpotent elements in a commutative ring $R$ is an ideal of $R$.

**Solution:** Let $a$ and $b$ be nilpotent elements of $R$. Then there exist $m$ and $n$ such that $a^n = 0, b^m = 0$.

Since $R$ is commutative, by binomial expansion we have

$$
\begin{aligned}
(a+b)^{mn} &= a^{nm} + \begin{pmatrix} nm \\ 1 \end{pmatrix} a^{nm-1}b + \cdots \begin{pmatrix} nm \\ mn-n \end{pmatrix} a^n b^{mn-n} \\
&\quad + \begin{pmatrix} nm \\ mn-n+1 \end{pmatrix} a^{n-1}b^{mn-n+1} + \cdots + b^{nm}
\end{aligned}
$$

$mn - n + i \geq m$ for $i \geq 1$, hence $b^{mn-n+1} = b^{mn-n+2} = \cdots = b^{nm} = 0$. But the remaining terms have powers of a greater than $n$. This implies $(a+b)^{mn} = 0$ i.e. $a+b$ is also nilpotent. Now for any $r \in R, (ar)^n = (ra)^n = r^n a^n = 0$ as $R$ commutative. Hence $ra$ is nilpotent.

**Remark.** Observe that $n+m$ th power is sufficient to show that $a+b$ is nilpotent.

(61) Find all nilpotent elements in $\mathbf{Z}_{p^k}$, then more generally in $\mathbf{Z}_n$. (See previous question).

**Solution:** First observe that every element of the form $pt$ for some $t \in \mathbf{Z}_n$ is nilpotent and there are $p^{n-1}$ elements of this form. On the other hand if $x$ is nilpotent, then there exists an $m$ such that $x^m \equiv 0 \bmod p^k$ or $p^k | x^m$. Hence $p|x$ as $\mathbf{Z}_p$ is a PID and $p$ is a prime element. Hence $\{p, 2p, 3p, \cdots, p^{k-1}p\}$ is the set of all nilpotent elements in $\mathbf{Z}_{p^k}$.

By Chinese remainder Theorem if $n = p_1^{m_1} \cdots p_k^{m_k}$, then $\mathbf{Z}_n = \mathbf{Z}_{p_1^{m_1} \cdots p_k^{m_k}} \cong \mathbf{Z}_{p_1^{m_1}} \oplus \cdots \oplus \mathbf{Z}_{p_k^{m_k}}$

If $x$ is a nilpotent element in $\mathbf{Z}_n$, then $x^t \equiv 0$ (mod n) i.e. $p_1^{m_1} \cdots p_k^{m_k} | x^t$. Since $p_1, p_2, \cdots, p_k$ are prime elements each prime should divide $x$. On the other hand any $x$ which is divisible by all $p_i$ is nilpotent.

(62) Suppose $R$ is a ring with 1, $u \in U(R)$, $a$ is a nilpotent element of $R$ and $ua = au$. Show that $u + a \in U(R)$. In particular $1 + a \in U(R)$ for every nilpotent $a$.

**Hint:** Write $(u+a)^{-1}$ suggestively as $\frac{1}{u+a} = \frac{u^{-1}}{1+u^{-1}a}$ and expand in a power series. Then verify directly that the resulting element of $R$ is an inverse for $u + a$.

**Solution:** Assume that $a^n = 0$. Then we have

$$(u+a)^{-1} = \frac{1}{u+a} = \frac{1}{u(1+u^{-1}a)} = \frac{u^{-1}}{1+u^{-1}a}$$
$$= u^{-1}[1 - u^{-1}a + (u^{-1}a)^2 + \cdots + (-1)^{n-1}(u^{-1}a)^{n-1}]$$

Therefore $(u+a)u^{-1}(1-u^{-1}a+u^{-2}a^2+\cdots+(-1)^{n-1}(u^{-1})^{n-1}a^{n-1}) = 1$. In particular when $u = 1$, then $1 + a \in U(R)$.

(63) Give an example of a ring $R$ with prime ideal $P \neq 0$ that is not maximal.

**Solution:** Let $R = \mathbf{Z}[x]$. The ideal $P(x) = \{xf(x)|f(x) \in \mathbf{Z}[x]\}$ is a prime ideal. Indeed define a map

$$\varphi : \mathbf{Z}[x] \to \mathbf{Z}.$$

$$a_0 + a_1x + \cdots + a_nx^n \to a_0$$

$\varphi$ is an evaluation ring epimorphism at $x = 0$.

Let $f(x) = a_0+a_1x+\cdots+a_nx^n$ and $g(x) = b_0+b_1x+\cdots+b_mx^m$. Then $\varphi(f(x) + g(x)) = a_0 + b_0 = \varphi(f(x)) + \varphi(g(x))$ and

$$\varphi(f(x)g(x)) = a_0b_0 = \varphi(f(x))\varphi(g(x)).$$

It is clear that $\varphi$ is onto. Hence $\mathbf{Z}[x]/(x) \cong \mathbf{Z}$. Since $\mathbf{Z}$ is an integral domain we get $P$ is a prime ideal. $P$ is not maximal because $\mathbf{Z}[x]/P \cong \mathbf{Z}$ is not a field.

(64) Show that the ideal $I = (2, x)$ is not principal in $\mathbf{Z}[x]$.

**Solution:** Assume if possible that $I$ is principal and generated by a polynomial $f(x) \in \mathbf{Z}[x]$. Then $2 \in I$ implies, $2 = f(x)g(x)$, for some $g(x) \in \mathbf{Z}[x]$. Since $\mathbf{Z}[x]$ is an integral domain we get $deg\ (f(x)g(x)) = deg\ f(x) + deg\ g(x) = 0$. Hence $f(x)$ is a constant. It is clear that $I$ is a proper ideal. If $1 \in I$, then $1 = a2 + bx$ for some $a, b \in \mathbf{Z}[x]$. Evaluating at $x = 0$ we obtain $2a_0 = 1$. So $a_0 = \frac{1}{2} \notin \mathbf{Z}$. Hence $1 \notin I$. Then the only possibilities for $f(x)$ are $\pm 2$. But then, $x \in I$ implies $x = 2g(x)$, for some $g(x) \in \mathbf{Z}[x]$. But this is impossible in $\mathbf{Z}[x]$. Hence $I$ is not a principal ideal.

(65) Suppose $R$ and $S$ are commutative rings with $R \subseteq S$ and $1_R = 1_S$ and that $R$ is an integral domain. If $a \in S$ is transcendental over $R$ and $g(x)$ is nonconstant polynomial in $R[x]$ show that $g(a)$ is transcendental over $R$.

**Proof:** Assume that $g(a)$ is algebraic over $R$. Then there exists a polynomial $f(x) \in R[x]$ such that

$$f(g(a)) = 0$$

Consider the polynomial $(f \circ g)(x)$ in $R[x]$. Since $R$ is an integral domain and $g(x)$ is not a constant polynomial $(f \circ g)(x)$ is not a constant polynomial. Since $1_R = 1_S$ substitution Theorem can be applied and so we get $(f \circ g)(a) = 0$. This implies a is algebraic over $R$ which is a contradiction.

Hence $g(a)$ is transcendental over $R$.

(66) (Lagrange Interpolation) Suppose $F$ is a field $a_1, a_2, \cdots, a_n$ are $n$ distinct elements of $F$ and $b_1, b_2, \cdots, b_n$ are arbitrary elements of $F$, set

$$p_i(x) = \Pi\{x - a_j : j \neq i\}$$

and set

$$f(x) = \sum_{i=1}^{n} b_i \frac{p_i(x)}{p_i(a_i)}, \quad i \leq i \leq n$$

Show that $f(x)$ is the unique polynomial of degree $\leq n-1$ over $F$ for which $f(a_i) = b_i$ $1 \leq i \leq n$.

**Proof:** $f(x) = \sum_{i=1}^{n} b_i \frac{\Pi_{i\neq j}(x-a_j)}{\Pi_{i\neq j}(a_i-a_j)}$

$$f(a_k) = b_k \frac{\Pi(a_k - a_j)}{\Pi(a_k - a_j)} = b_k$$

all the other terms are of the form

$$b_i \frac{\Pi(a_k - a_j)}{\Pi(a_i - a_j)} = b_i \frac{(a_k - a_2)(a_k - a_3)\cdots(a_k - a_k)\dots}{(a_i - a_1)(a_i - a_2)\cdots(a_i - a_{k-1})(a_i - a_{k+1})\cdots(a_i - a_n)} = 0$$

hence

$$f(a_k) = b_k.$$

Uniqueness:

Assume that $g(x)$ is another polynomial such that $g(a_i) = b_i$, for all $i = 1, \cdots, n$ and $deg\ g(x) \leq n-1$. Hence $h(a_i) = g(a_i) - f(a_i) = 0$ then $h(a_i)$ has $a_i$ as a root for all $i = 1, \cdots, n$. So $deg\ h(a_i) \geq n$ as all $a_i$'s are distinct but $n \leq d(g(x_i) - f(x)) \leq \max deg\{f(x), g(x)\} = n-1$ so $f - g = 0$ hence, $f = g$.

(67) Find $f(x) \in \mathbf{Q}[x]$ of degree 3 or less such that $f(0) = f(1) = 1, f(2) = 3$ and $f(3) = 4$.

**Solution:** By Lagrange interpolation in the previous question we get

$$\begin{aligned}
p_1(x) &= (x-1)(x-2)(x-3)\\
p_2(x) &= x(x-2)(x-3)\\
p_3(x) &= x(x-1)(x-3)\\
p_4(x) &= x(x-1)(x-2)
\end{aligned}$$

$$\begin{aligned}
f(x) &= \frac{1p_1(x)}{p_1(0)}+\frac{1p_2(x)}{p_2(1)}+\frac{3p_3(x)}{p_3(2)}+\frac{4p_4(x)}{p_4(3)}\\
&= \frac{(x-1)(x-2)(x-3)}{-6}+\frac{(x)(x-2)(x-3)}{2}+\frac{3x(x-1)(x-3)}{-2}\\
&+ \frac{4x(x-1)(x-2)}{6}\\
&= -\frac{1}{2}x^3+\frac{5}{2}x^2-2x+1.
\end{aligned}$$

Another Solution:
Let $f(x) = ax^3 + bx^2 + cx + d$

$$f(0) = d = 1$$

$$\begin{aligned}
f(1) &= a+b+c+d = 1\\
f(2) &= 8a+4b+2c+d = 3\\
f(3) &= 27a+9b+3c+d = 4
\end{aligned}$$

so

$$a+b+c = 0$$
$$8a+4b+2c = 2$$
$$27a+9b+3c = 3$$

Then we solve the system $\begin{bmatrix} 1 & 1 & 1 & 0\\ 8 & 4 & 2 & 2\\ 27 & 9 & 3 & 3\end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 0\\ 4 & 2 & 1 & 1\\ 9 & 3 & 1 & 1\end{bmatrix} \to$
$\begin{bmatrix} 1 & 1 & 1 & 0\\ 0 & -2 & -3 & 1\\ 0 & -6 & -8 & 1\end{bmatrix}$

$$\to \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & -2 & -3 & 1 \\ 0 & 0 & 1 & -2 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 & 2 \\ 0 & -2 & 0 & -5 \\ 0 & 0 & 1 & -2 \end{bmatrix} \to$$

$$\begin{bmatrix} 1 & 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & \frac{5}{2} \\ 0 & 0 & 1 & -2 \end{bmatrix}$$

$$a = -\frac{1}{2}, \quad b = \frac{5}{2}, \quad c = -2, \quad d = 1$$

$$\begin{aligned} f(x) &= -\frac{1}{2}x^3 + \frac{5}{2}x^2 - 2x + 1 \\ f(0) &= 1 \\ f(1) &= -\frac{1}{2} + \frac{5}{2} - 2 + 1 = 1 \\ f(2) &= (-\frac{1}{2})8 + \frac{5}{2}(4) - 2(2) + 1 \\ &= -4 + 10 - 4 + 1 = 3 \\ f(3) &= -\frac{1}{2}(27) + \frac{5}{2}9 - 2.3 + 1 \\ &= \frac{-27+45}{2} - 6 + 1 = 9 - 6 + 1 = 4 \end{aligned}$$

So we are done.

(68) $R$ is Noetherian if and only if every ideal is finitely generated.

**Proof:** Assume $R$ is Noetherian. If $I$ is any ideal in $R$ let $\rho$ be the set of all finitely generated ideals of $R$ that are contained in $I$ ($e.g$ $0 \in \rho$). Let $I_0$ be a maximal element of $\rho$ say with $I_0$ generated by $r_1, \cdots, r_k$. If $I_0 \neq I$ choose $r \in I \setminus I_0$ and let $J$ be the ideal generated by $r_1, \cdots, r_k$ and $r$. Then $J \in \rho$ but $I_0 \subseteq J$ and $I_0 \neq J$ contradicting maximality. Thus $I = I_0$ is finitely generated.

Conversely if $I_0 \subseteq I_1 \subseteq I_2 \subset \cdots$ is any ascending chain of ideals, then $I = U_j I_j$ is an ideal say $I$ is generated by $r_1, \cdots, r_k$ and say that $r_i \in I_{j(i)}, 1 \leq i \leq k$. Let $m = max\{j(1), j(2) \cdots, j(k)\}$. Then $I_m = I$. Hence chain terminates at $I_m$.

(69) Suppose $R$ is an Euclidean domain $a, b \in R^* = R \setminus \{0\}$, $a|b$ and $d(a) = d(b)$.

Show that $a$ and $b$ are associates.

**Proof:** Since $a|b$, $b = ca$ for some $c \in R^*$. (Since $b \in R^*, c \in R^*$).

$R$ is an Euclidean domain, $a = qb + r$ where $r = 0$ or $d(r) < d(b)$. If $r = 0$ then $b|a$ and we are done. If $r \neq 0$, then $d(r) < d(b)$

$$\begin{aligned} a &= qb + r \\ a &= q(ca) + r \\ a(1 - qc) &= r \end{aligned}$$

$$d(b) = d(a) \leq d(a(1 - qc)) = d(r) < d(b).$$

This is a contradiction. Hence $r = 0$ and $b|a$. It follows that $a \sim b$.

(70) If $p \in \mathbf{Z}$ is prime and $1 < m \in Z$ show that $f(x) = x^m - p$ is irreducible in $\mathbf{Q}[x]$ and conclude that $p^{\frac{1}{m}}$ is irrational.

**Proof:** $p$ is prime in $\mathbf{Z}$ by Eiesenstein Criterion $f(x)$ is irreducible, since $p|a_0$, $\quad p^2 \not| a_0$, and $p \not| a_m$.

If $p^{\frac{1}{m}} \in \mathbf{Q}$, then $x - p^{\frac{1}{m}} \in \mathbf{Q}[x]$. This is a divisor of $x^m - p$ in $\mathbf{Q}[x]$ for $m \geq 2$, this contradicts to the irreducibility of $x^m - p \in \mathbf{Q}[x]$

**$2^n d$ Method:**

Now suppose that $p^{\frac{1}{m}}$ is rational. Let $a, b \in \mathbf{Z}$, $\quad (a, b) = 1$ and $p^{\frac{1}{m}} = \frac{a}{b} \in \mathbf{Q}$. Then $p = \frac{a^m}{b^m}$, $\quad pb^m = a^m$ since $p$ is a prime and divide left hand side so $p|a^m$, then $p|a$. Hence $p^m|a^m, p^m|pb^m$ since $m > 1, p|b$. This is a contradiction since

$$p|a, \quad p|b, \quad \text{so} \quad gcd(a, b) \geq p.$$

Hence $p^{\frac{1}{m}}$ is an irrational number.

(71) (The Euclidean Algorithm) Suppose $R$ is a Euclidean domain $a, b \in R$ and $ab \neq 0$ write

$$
\begin{aligned}
a &= bq_1 + r_1 \quad d(r_1) < d(b)\\
b &= r_1q_2 + r_2 \quad d(r_2) < d(r_1)\\
r_1 &= r_2q_3 + r_3 \quad d(r_3) < d(r_2)\\
&\vdots\\
r_{k-2} &= r_{k-1}q_k + r_k \quad d(r_k) < d(r_{k-1})\\
r_{k-1} &= r_kq_{k+1}
\end{aligned}
$$

with all $r_i, q_j \in R$. Show that $r_k = (a,b)$ and "solve" for $r_k$ in terms of $a$ and $b$ thereby expressing $(a,b)$ in the form $ua+vb$, with $u,v \in R$.

**Proof:**

$$\begin{aligned}
a &= bq_1 + r_1 \quad d(r_1) < d(b)\\
b &= r_1q_2 + r_2 \quad d(r_2) < d(r_2)\\
r_1 &= r_2q_3 + r_3 \quad d(r_3) < d(r_2)\\
r_2 &= r_3q_4 + r_4 \quad d(r_4) < d(r_3)\\
&\vdots\\
r_{k-5} &= r_{k-4}q_{k-3} + r_{k-3} \quad d(r_{k-3}) < d(r_{k-4})\\
r_{k-4} &= r_{k-3}q_{k-2} + r_{k-2} \quad d(r_{k-2}) < d(r_{k-3})\\
r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1} \quad d(r_{k-1}) < d(r_{k-2})\\
r_{k-2} &= r_{k-1}q_k + r_k \quad d(r_k) < d(r_{k-1})\\
r_{k-1} &= r_kq_{k+1}\\
r_{k-2} &= r_{k-1}q_k + r_k = (r_kq_{k+1})q_k + r_k = r_k(q_{k+1}q_k + 1)\\
r_{k-3} &= r_k(q_{k+1}q_k + 1)q_{k-1} + r_kq_{k+1} = r_k(q_{k+1}q_kq_{k-1} + q_{k-1} + q_{k+1})\\
&\vdots\\
b &= r_k[q_{k+1}q_kq_{k-1} + q_{k-2} + \cdots + \cdots + 1]q_2 + r_k[\cdots]\\
a &= r_k[q_{k+1}q_kq_{k-1}\cdots + 1]q_1 + r_k[\cdots]
\end{aligned}$$

hence $r_k|a$ and $r_k|b$. If $c|a$ and $c|b$ then $c|(a - bq_1) = r_1$

Similarly,

$$\begin{aligned}
c &\mid (b - r_1q_2) = r_2\\
c &\mid (r_1 - r_2q_3) = r_3\\
&\vdots\\
c &\mid (r_{k-2} - r_{k-1}q_k) = r_k
\end{aligned}$$

so $r_k = (a, b)$. For $(a, b) = ua + vb :$

$$
\begin{aligned}
(a,b) = r_k = r_{k-2} - r_{k-1}q_k &= r_{k-2} - (r_{k-3} - r_{k-2}q_{k-1}) \\
&\vdots \\
&= r_2 n + r_3 m \\
&= r_2 n - (r_1 - r_2 q_3)m \\
&= r_2(n + q_3 m) - r_1 \\
&= (b - r_1 q_2)(n + q_3 m) - r_1 \\
&= b(n + q_3 m) - r_1(q_2 + 1) \\
&= b(n + q_3 m) - (a - bq_1)q_2 + 1) \\
&= b(n + q_3 m) - a(q_2 + 1) + bq_1(q_2 + 1) \\
&= b(n + q_3 m + q_1(q_2 + 1) - a(q_2 + 1) \\
\text{Hence} u &= -(q_2 + 1) \\
v &= n + q_3 m + q_1(q_2 + 1) \\
(a,b) &= ua + vb
\end{aligned}
$$

(72) Use Euclidean Algorithm to find $d = (a,b)$ and to write $d = ua + vb$ in the following cases

(1) $a = 29041, b = 23843, R = \mathbf{Z}$.

**Solution:**

$$\begin{aligned}
a &= 29041 = (23843)1 + 5198 \\
&\quad 23843 = (5198)4 + 3051 \\
&\quad 5198 = (3051).1 + 2147 \\
&\quad 3051 = 2147.1 + 904 \\
&\quad 2147 = 904.2 + 339 \\
&\quad 904 = 339.2 + 226 \\
&\quad 339 = 226.1 + 113 \\
&\quad 226 = 113.2
\end{aligned}$$

Hence 113 is a greatest common divisor.

For $(a, b) = ua + vb$ :

$$\begin{aligned}
113 &= 339 - 226.1 = 339 - (904 - 339.2) \\
&= (2147 - 904.2) - (904 - [(2147 - 904.2).2]) \\
&= 2147 - [(3051 - 2147).2] - (3051 - 2147 - 2[2147 - (3051 - 2147)2] \\
&= 2147 - 2.3051 + 2.2147 - (3051 - 2147 - 2147).2 - (4.3051 - 4.2147) \\
&= 2147 - 2.3051 + 2.2147 - 3051 + 2147 + 2147.2 - 4.3051 + 4.2147 \\
&= 10.2147 - 7.3051 \\
&= 10(5198 - 3051) - 7.3051 \\
&= 10.5198 - 10.3051 - 7.3051 = 10.5198 - 7.3051 \\
&= 10.5198 - 7(23843 - 5198.4) = 10.5198 - 7.23843 + 68.5198 \\
&= 78.5198 - 7.23843 \\
&= 78(29841 - 23843) - 7(23843) = 78.29041 - 95.23843 \\
113 &= 78.29041 - 95.23843 \\
u &= 78 \\
v &= -95
\end{aligned}$$

(2) $a = x^3 - 2x^2 - 2x - 3$, $b = x^4 + 3x^3 + 3x^2 + 2x$, and $R = \mathbf{Q}[x]$

**Solution:**

$$a = x^3 - 2x^2 - 2x - 3 = (x^4 + 3x^3 + 3x^2 + 2x)0 + (x^3 - 2x^2 - 2x - 3)$$

$$x^4 + 3x^3 + 3x^2 + 2x = (x^3 - 2x^2 - 2x - 3)(x + 5) + (15x^2 + 15x + 15)$$

$$x^3 - 2x^2 - 2x - 3 = (15x^2 + 15x + 15)(\frac{1}{15}x - \frac{3}{15})$$

Hence $15x^2 + 15x + 15$ is a greatest common divisor

$$(a, b) = ua + vb$$

$$15x^2+15x+15 = (x^4-3x^3+3x^2+2x)-(x^3-2x^2-2x-3)(x+5)$$
$$u=-(x+5), \quad v=1$$

(3) $a=7-3i$ and $b=5+3i$, $R=R_{-1}$
**Solution:** $\frac{7-3i}{5+3i}=\frac{(7-3i)(5-3i)}{34}=\frac{26-36i}{34}$
$a=7-3i=(5+3i)(1-i)+(-1-i)$
$5+3i=(-1-i)(-4+i)$ $\frac{5+3i}{-1-i}=\frac{(5+3i)(-1+i)}{2}=\frac{-5-3+2i}{2}=-4+i$
So $-1-i$ is a greatest common divisor.
$(a,b)=ua+vb$ :

$$-1-i=1(7-3i)-(5+3i)(1-i)$$
$$u=1 \quad v=-(1-i)$$

(73) Establish the Eiesenstein Criterion for a polynomial $f(x)$ over a UFD. Statement of Criterion. Let $f(x)\in R[x]$, be a primitive polynomial where $R$ is a UFD and let $p$ be a prime in $R$ such that, if $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ $p|a_i$ for all $i<n, p\not|a_n$ and $p^2\not|a_0$, then $f(x)$ is irreducible in $R[x]$.

**Proof:** Assume that $f(x)=h(x)g(x)$ where $h(x)$, $g(x)\in R[x]$ and $\deg(h(x))\geq 1$, deg $(g(x))\geq 1$

$$h(x)=\sum_{v=0}^{s}c_vx^v \quad \text{and} \quad g(x)=\sum_{v=0}^{r}b_vx^v$$

where $s+r=n$.

The coefficient of $x^i$ is

$$a_i=b_ic_0+b_{i-1}c_1+\cdots+b_0c_i$$

the constant term is $b_0c_0=a_0$ since $p|a_0$ and $p^2\not|a_0$, $p$ divides either $b_0$ or $c_0$ but not both (else $p^2$ divides $a_0$). Assume without loss of generality that, $p|b_0$ i.e. $b_0\equiv 0$ (mod p).

Since the coefficient of $x^n$ is $c_sb_r=a_n$ and $p\not|a_n$, there exists $b_i$ such that $p\not|b_i$ (else $p|a_n$).

Let $b_i$ is the first coefficient such that $p$ doesn't divide. Then

$$\begin{aligned} a_i &= b_i c_0 + b_{i-1}c_1 + \cdots + b_0 c_i \\ a_i &\equiv 0 \pmod p \quad \text{or} \quad i = n \\ b_{i-1} &\equiv 0 \pmod p \\ b_{i-2} &\equiv 0 \pmod p \\ &\vdots \\ b_0 &\equiv 0 \pmod p \end{aligned}$$

but

$$c_0 \not\equiv 0 \pmod p$$

Hence $b_i c_0 \equiv 0$ (mod p), $p|b_i c_0$. Since $p \not| c_0$ we obtain $p|b_i$.

But this is contradiction since we assume that $b_i$ is the first coefficient of $f(x)$ such that $p$ doesn't divide. So $f(x)$ can not be factored as a product of two polynomials of smaller degree.

(74) Solve the congruences

$$f(x) \equiv 1 \pmod{(x-1)}, \quad f(x) \equiv x \pmod{(x^2+1)},$$
$$f(x) \equiv x^3 \pmod{(x+1)}$$

simultaneously for $f(x)$ in $F[x]$ where $F$ is a field in which $1+1 \neq 0$.

**Solution:** $(x-1, x^2+1) = 1, \quad (x-1, x+1) = 1, \quad (x+1, x^2+1) = 1$

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

Then

$$\frac{1}{4}(x^3+x^2+x+1) - \frac{1}{4}(x^2+2x+3)(x-1) = 1$$
$$\text{where} \quad (x^3+x^2+x+1) = (x^2+1)(x+1)$$
$$\frac{1}{2}(x^3-x^2+x-1) - \frac{1}{2}(x+1)(x^2-2x+3) = 1.$$

$$\text{where } x^3 - x^2 + x - 1 = (x^2+1)(x-1)$$

and finally

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

These products will work even if characteristic is 3.

$$\begin{aligned} s_1 &= \frac{1}{4}(x^3+x^2+x+1) \\ s_2 &= -\frac{1}{2}(x^2-1) \\ s_3 &= \frac{1}{2}(x^3-x^2+x-1) \end{aligned}$$

$$f(x) = \frac{1}{4}(x^3+x^2+x+1) + \frac{x^3}{2}(x^3-x^2+x-1) - \frac{x}{2}(x^2-1)$$

(75) It is well known that if $R$ is a UFD, then any two elements has a greatest common divisor.

Find an example of an integral domain and two elements $a, b$ such that $a$ and $b$ does not have a greatest common divisor.

**Solution:** Recall that $R = \mathbf{Z}[\sqrt{-5}]$ is not a unique factorization domain as $9 = 3.3 = (2+\sqrt{-5})(2-\sqrt{-5})$. In $R$ consider the elements 3 and $1+2\sqrt{-5}$. These two elements has no greatest common divisor. If $d$ is a greatest common divisor, then $d|3$ and $d|(1+2\sqrt{-5})$. Then the norm $N(d)|9$ and $N(d)|21 = N(1+2\sqrt{-5}$. Let $d = m + n\sqrt{-5}$ where $m$ and $n$ are elements of $\mathbf{Z}$. Then $N(d)|3 = gcd(9, 21)$. But the equation $3 = m + n\sqrt{-5}$ has no solution in $R$. Hence these two elements has no greatest common divisor.

**$2^{nd}$ Method:** Let $R = 2\mathbf{Z}$, it is an integral domain. $2 \in R$ but 2 does not have any divisor because $1 \notin R$. Hence 2 and 4 does not have a greatest common divisor.

# FIELDS

(76) Let $A$ be the field of all complex numbers which are algebraic over $\mathbf{Q}$. Then show that $|A : \mathbf{Q}|$ is infinite.

**Solution:** Assume if possible that $|A : \mathbf{Q}| = n$. Let $p$ be a prime number and $p > n+2$. Then $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$. Then $\frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$. By Eisenstein criteria this is an irreducible polynomial because $\frac{(x+1)^p-1}{(x+1)-1} = x^{p-1} + px^{p-2} + \cdots + p$ is irreducible. But every primitive $p^{th}$ root of unity is in $A$. Hence for any prime $p$, there exists an element $a_p$ algebraic over $\mathbf{Q}$ and $|\mathbf{Q}(a_p) : \mathbf{Q}| \geq p-1$. Hence we get

$$n = |A : \mathbf{Q}| \geq |\mathbf{Q}(a_p) : \mathbf{Q}| \geq p - 1 > n + 1 \quad \text{contradiction.}$$

It follows that $|A : \mathbf{Q}|$ is infinite.

(77) Find a splitting field $K \subseteq \mathbb{C}$ over $\mathbf{Q}$ for

$$f(x) \in \mathbf{Q}[x] \quad \text{if} \quad f(x) = x^3 - 1.$$

**Solution:** $x^3 - 1 = (x-1)(x^2+x+1) \in \mathbf{Q}[x]$, $g(x) = x^2+x+1$ is irreducible over $\mathbf{Q}$. The roots of $g(x)$ are

$$\frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{-3}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}i}{2}$$

Hence $\mathbf{Q}(\frac{1}{2} \pm \frac{\sqrt{3}i}{2}) = \mathbf{Q}(\sqrt{3}i)$ is the splitting field of $g(x)$ and

$$|\mathbf{Q}(\sqrt{3}i) : \mathbf{Q}| = 2$$

(78) If $m \in \mathbf{Z}$ is square free and $m \neq 0, 1$, show that $K = \mathbf{Q}(\sqrt{m})$ is Galois over $F = \mathbf{Q}$.

**Solution:** $m \neq 0, 1$ and $m$ is square free implies that $\mathbf{Q}(\sqrt{m}) \neq \mathbf{Q}$. Since $\sqrt{m}$ is a root of the polynomial $f(x) = x^2 - m \in \mathbf{Q}[x]$ and $f(x)$ is irreducible we get $|\mathbf{Q}(\sqrt{m}) : \mathbf{Q}| = 2$. Moreover the map

$$\begin{aligned} \alpha : \mathbf{Q}(\sqrt{m}) &\rightarrow \mathbf{Q}(\sqrt{m}) \\ a + b\sqrt{m} &\rightarrow a - b\sqrt{m} \end{aligned}$$

is a $\mathbf{Q}$-automorphism of $\mathbf{Q}(\sqrt{m})$

$$G(\mathbf{Q}(\sqrt{m}),\mathbf{Q}) = \{1,\alpha\} \quad \text{and} \quad \mathcal{F}(G) = \mathbf{Q}.$$

$$\mathcal{F}(\{1\}) = \mathbf{Q}(\sqrt{m}), \quad \mathcal{F}\{\alpha\} = \{a + b\sqrt{m} \mid \ a + b\sqrt{m} = a - b\sqrt{m} \ \} = \mathbf{Q}$$

Hence $G$ is a cyclic group of order 2. It follows that $\mathbf{Q}\sqrt{m}$ is a Galois extension of $\mathbf{Q}$.

(79) Describe the elements of $\mathbf{Q}(\sqrt[3]{5})$.

**Solution:** $\mathbf{Q}(\sqrt[3]{5})$ is an extension of the field of rational numbers. $\mathbf{Q}(\sqrt[3]{5})$ is a vector space over $\mathbf{Q}$ with basis 1, $\sqrt[3]{5}$, $\sqrt[3]{5^2}$. Hence

$$\mathbf{Q}(\sqrt[3]{5}) = \{a + b\sqrt[3]{5} + c\sqrt[3]{5^2} \ \mid \ a,b,c \in \mathbf{Q}\}.$$

(80) Find the splitting field of $x^4+1$ over $\mathbf{Q}$.

**Solution:**

$$x^4 + 1 = 0, \quad x^4 = -1 = e^{\pi i + 2n\pi i}$$

$$4\theta i = \pi i + 2\pi n i, \quad \theta = \frac{\pi + 2\pi n}{4}. \text{ Then we have } \quad \theta_1 = \frac{\pi}{4}, \theta_2 = \frac{3\pi}{4}, \theta_3 = \frac{5\pi}{4}, \theta_4 = \frac{7\pi}{4}.$$

Then the roots of the polynomial $x^4+1$ are

$$\begin{aligned}
x_1 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} &= \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \\
x_2 = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} &= \frac{-\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \\
x_3 = \cos\frac{5\pi}{4} + \sin\frac{5\pi}{4} &= -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\
x_4 = \cos\frac{7\pi}{4} + \sin\frac{7\pi}{4} &= \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i
\end{aligned}$$

$$\mathbf{Q}(\sqrt{2} + \sqrt{2}i) = \mathbf{Q}(\sqrt{2}, i)$$

Indeed let $K = \mathbf{Q}(\sqrt{2} + \sqrt{2}i)$. Then $K \subseteq \mathbf{Q}(\sqrt{2}, i)$ Since $(\sqrt{2} + \sqrt{2}i)^2 = 4i$ we get $i \in K$. Then $i((\sqrt{2} + \sqrt{2}i) = (\sqrt{2}i - \sqrt{2}) \in K$. Adding with $(\sqrt{2} + \sqrt{2}i)$ gives $2\sqrt{2}i \in K$ . Since $i \in K$ we obtain $\sqrt{2} \in K$. Hence we get the other side of the inequality.

(81) Find the splitting field of $x^4+x^2+1=(x^2+x+1)(x^2-x+1)$ over $\mathbf{Q}$.

**Solution:**

$$x_{1,2}=\frac{-1\pm\sqrt{3}i}{2}, \quad x_{3,4}=\frac{1\pm\sqrt{3}i}{2}$$

$\mathbf{Q}(\sqrt{3}i)$ is the splitting field of $x^4+x^2+1$.

(82) Let $a,b\in\mathbf{R}$ with $b\neq 0$. Show that $\mathbf{R}\ (a+bi)=\mathbf{C}$.

**Solution:** $\mathbf{R}(a+bi)=\mathbf{R}(bi)=\mathbf{R}(i)=\mathbf{C}$

(83) Find a polynomial $p(x)$ in $\mathbf{Q}[x]$ so that $\mathbf{Q}(\sqrt{1+\sqrt{5}})$ is isomorphic to $\mathbf{Q}[x]/<p(x)>$

**Solution:** Let $x=\sqrt{1+\sqrt{5}}$. Then $x^2=1+\sqrt{5}$ and so $x^2-1=\sqrt{5}$. Then we obtain $(x^2-1)^2=5$. Hence

$$x^4-2x^2+1-5=0, \text{ and hence } x^4-2x^2-4=0,$$

$$x_{1,2}^2=\frac{2\pm\sqrt{4+16}}{2}=\frac{2\pm\sqrt{20}}{2}=1\pm\sqrt{5}$$

$$p(x)=x^4-2x^2-4. \text{ Then}$$

$$p(x)=(x^2-1-\sqrt{5})(x^2-1+\sqrt{5})$$

If $(x^2+ax+b)(x^2+cx+d)=x^4-2x^2-4$ with $a,b,c,d\in\mathbf{Q}$

then $x^4+(c+a)x^3+(d+ac+b)x^2+(ad+bc)x+bd$.

We obtain the equations

$$a+c=0, \quad ad+bc=0, \quad bd=-4$$

$$ac+b+d=-2.$$

$a=-c$, implies $-a^2+b+d=-2$, $ad-ba=0$ and so $a(d-b)=0$ It follows that either $a=0$ or $d-b=0$.

The first case $a=0$ implies $c=0$, $b+d=-2$. Then $b=-2-d$, $bd=-4$, $(-2-d)d=-4$, and so $-d^2-2d=$

4, $d^2 + 2d - 4 = 0$. Solving the equation for the unknown $d$ we have

$$d_{12} = \frac{-2 \pm \sqrt{4+16}}{2} = \frac{-2 \pm \sqrt{20}}{2} \notin \mathbf{Q}.$$

Hence this case is impossible. Then $d - b = 0$ which implies $d = b$. The equality $bd = -4$ gives $b^2 = -4$ which is impossible. Also the polynomial $x^4 - 2x^2 - 4 \in \mathbf{Q}[x]$ does not accept $\pm 1, \pm 2, \pm 4$ as a root. Hence by integral root test $p(x) = x^4 - 2x^2 - 4$ is irreducible in $\mathbf{Q}[x]$. Since $p(x)$ is irreducible the quotient $\mathbf{Q}[x]/\langle p(x)\rangle$ is a field.

$$\mathbf{Q}[x]/\langle p(x)\rangle \to \mathbf{Q}(\sqrt{1+\sqrt{5}})$$
$$f(x) + \langle p(x)\rangle \to f(\sqrt{1+\sqrt{5}})$$

is an isomorphism of fields.

(84) Show that $\mathbf{Q}(\sqrt{2})$ is not isomorphic to $\mathbf{Q}(\sqrt{3})$.

**Solution:** Assume that $\alpha$ is an isomorphism from $\mathbf{Q}(\sqrt{2})$ to $\mathbf{Q}(\sqrt{3})$. So $\alpha(0) = 0$, $\alpha(1) = 1$. Hence $\alpha(n) = n$ and

$$\alpha = (\frac{m}{m}) = \alpha(m)\alpha(\frac{1}{m}) = 1 \Rightarrow \alpha(\frac{1}{m}) = \frac{1}{m}.$$

Hence $\alpha$ is identity on $\mathbf{Q}$.

Let $a + b\sqrt{2} \in \mathbf{Q}(\sqrt{2})$ where $a, b \in \mathbf{Q}$.

$$\alpha(a + b\sqrt{2}) = \alpha(a) + \alpha(b)\alpha(\sqrt{2}) = a + b\alpha(\sqrt{2}).$$

Hence we need to find out $\alpha(\sqrt{2})$. But

$$\begin{aligned}
\alpha(\sqrt{2}\sqrt{2}) &= \alpha(\sqrt{2})\alpha(\sqrt{2}) = 2 \\
&(\alpha(\sqrt{2}))^2 = 2 \\
&\alpha(\sqrt{2}) = \pm\sqrt{2} \notin \mathbf{Q}(\sqrt{3}).
\end{aligned}$$

Indeed if $\sqrt{2} = a + b\sqrt{3}$ where $a, b \in \mathbf{Q}$, then by taking the square of both sides we get $2 = a^2 + 2ab\sqrt{3} + 3b^2$. But then $\sqrt{3}$ will be a rational number. Hence such an isomorphism does not exist.

(85) Show $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

**Solution:** Since $\sqrt{2} + \sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$ we have

$$\mathbf{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3}).$$

Now we show the other inclusion.

$$(\sqrt{2} + \sqrt{3})^2 = 2 + 3 + 2\sqrt{2}\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

Hence $2\sqrt{2}\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$. This implies that

$$\sqrt{2}\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3}).$$

Then $\sqrt{2}\sqrt{3}(\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

Then $2(\sqrt{2} + \sqrt{3}) \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$. This implies

$$3\sqrt{2} + 2\sqrt{3} - 2\sqrt{2} - 2\sqrt{3} = \sqrt{2} \in \mathbf{Q}(\sqrt{2} + \sqrt{3}).$$

Hence $\sqrt{2} + \sqrt{3} - \sqrt{2} = \sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$. So

$$\mathbf{Q}(\sqrt{2} + \sqrt{3}) \supset \mathbf{Q}(\sqrt{2}, \sqrt{3})$$

So we get equality $\mathbf{Q}(\sqrt{2} + \sqrt{3}) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$.

(86) Suppose $K$ is an algebraic extension of $F$ and $R$ is a ring, with $F \subseteq R \subseteq K$. Show that $R$ is a field.

**Solution:** Clearly $R$ is a commutative ring. It is enough to show that every nonzero element $a \in R$ has an inverse. Since $K$ is an algebraic extension of $F$ we get $F(a)$ is an algebraic extension of $F$. Since

$$F(a) = \{c_0 + c_1 a + \cdots + c_{k-1}a^{k-1} \mid c_i \in F\} \quad \text{where} \quad k = |F(a) : F|$$

Since every element of the form $c_0 + c_1 a + \cdots + c_{k-1}a^{k-1}$ is an element of the ring and $a^{-1} \in F(a)$ can be written in this form we get $a^{-1} \in R$ as required.

(87) Find all solutions to $x^2+1=0$ in the ring $H$ of quaternions.

**Solution:** Recall that $H = \{a_0 + a_1 i + a_2 j + a_3 k | a_i \in \mathbb{R},\ i^2 = j^2 = k^2 = -1,\ ij = k, jk = i, kj = -i, \cdots\}$.

$(a_0 + a_1 i + a_2 j + a_3 k)(a_0 + a_1 i + a_2 j + a_3 k) = -1$ implies that
$a_0^2 - a_1^2 - a_2^2 - a_3^2 = -1$
$a_0 a_1 + a_1 a_0 = 2a_1 a_0 = 0$
$a_0 a_2 + a_2 a_0 = 2a_2 a_0 = 0$
$a_0 a_3 + a_3 a_0 = 2a_3 a_0 = 0$
$a_0 \neq 0$ implies that $a_1 = a_2 = a_3 = 0$ We get no solution in this case.

$a_0 = 0$ implies $a_1^2 + a_2^2 + a_3^2 = 1$ is the only equation. Hence we get infinitely many solutions of the equation.

The reason why a polynomial of degree two has infinitely many distinct roots is, $H[x]$ is not a unique factorization domain. $H$ is not a unique factorization domain either. Moreover $H$ is not commutative.

(88) If $f : \mathbb{C} \to R$ is a ring homomorphism. Show that $f(a) = 0$ for all $a \in \mathbb{C}$.

**Solution:** Let $f$ be a ring homomorphism. If there exists a non-zero element $a \in \mathbb{C}$ such that $f(a) = 0$. Then $Kerf \neq \{0\}$ and an ideal of $\mathbb{C}$. This implies $Kerf = \mathbb{C}$ since any non-zero ideal of field is itself. It follows that $f(c) = 0$ for all $c \in \mathbb{C}$. Now we will show that the other case namely $Kerf = \{0\}$ is impossible. $f(1) = f(1)f(1)$, then $f(1)(f(1) - 1) = 0$. Since $f(1) \neq 0$ we get $f(1) = 1$. Hence $f(i) = a \in \mathbb{R}$ implies $-1 = f(-1) = f(i^2) = f(i)^2 = a^2$. i.e., there exists a real number whose square is -1, which is impossible. Hence $f = 0$.

(89) Find a splitting field $K \subseteq \mathbb{C}$ for $x^3 - 2 \in \mathbf{Q}[x]$ over $\mathbf{Q}$ and determine $|K : \mathbf{Q}|$.

**Solution:** $x^3-2=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{2^2})$ Then the roots of $g(x)=x^2+\sqrt[3]{2}x+\sqrt[3]{2^2}$ are

$$\frac{-\sqrt[3]{2}\pm\sqrt{\sqrt[3]{2^2}-4\sqrt{\sqrt[3]{2^2}}}}{2}=\frac{-\sqrt[3]{2}\pm\sqrt[3]{2}\sqrt{3}i}{2}=\frac{\sqrt[3]{2}(-1\pm\sqrt{3}i)}{2}$$

Hence the splitting field of $x^3-2$ is $\mathbf{Q}(\sqrt[3]{2},\sqrt{3}i)$. It follows that

$$|\mathbf{Q}(\sqrt[3]{2},\sqrt{3}i)\ :\ \mathbf{Q}|=\underbrace{|\mathbf{Q}(\sqrt[3]{2},\sqrt{3}i):\mathbf{Q}(\sqrt[3]{2})|}_{2}\underbrace{|\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}}_{3}|=6.$$

(90) If $K\subseteq\mathbb{C}$ is a splitting field over $\mathbf{Q}$ for $x^3-2$ find all subfields of $K$.

**Solution:** We have already found in Question 89 that the splitting field of $x^3-2$ is

$\mathbf{Q}(\sqrt[3]{2},w)$ where $w$ is a primitive cube root of unity. $(w^3=1), w=\frac{-1+\sqrt{3}i}{2}$ The roots of $x^3-2$ are $\sqrt[3]{2},w\sqrt[3]{2},w^2\sqrt[3]{2}$. Since

$|K:\mathbf{Q}|=|\mathbf{Q}(\sqrt[3]{2},w):\mathbf{Q}(\sqrt[3]{2})|\ |\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}|=6$ we get degree of the extension is 6. Since

$K=\{a_1+a_2\sqrt[3]{2}+a_3\sqrt[3]{2}^2+a_4w+a_5\sqrt[3]{2}w+a_6\sqrt[3]{2}^2w|a_i\in\mathbf{Q}\}$,

as a vector space over $\mathbf{Q}$ the field $K$ has a basis $\{1,\sqrt[3]{2},\sqrt[3]{2}^2,w,w\sqrt[3]{2},w\sqrt[3]{2}^2\}$

$G(K,\mathbf{Q})$ is the group of all permutations of roots

$$\text{Let}\quad \phi:\sqrt[3]{2}\to\sqrt[3]{2}w,\quad \phi(w)=w.\qquad \text{Then}\quad \begin{aligned}\phi(\sqrt[3]{2}w)&=\sqrt[3]{2}w^2\\ \phi(\sqrt[3]{2}w^2)&=\sqrt[3]{2}.\end{aligned}$$

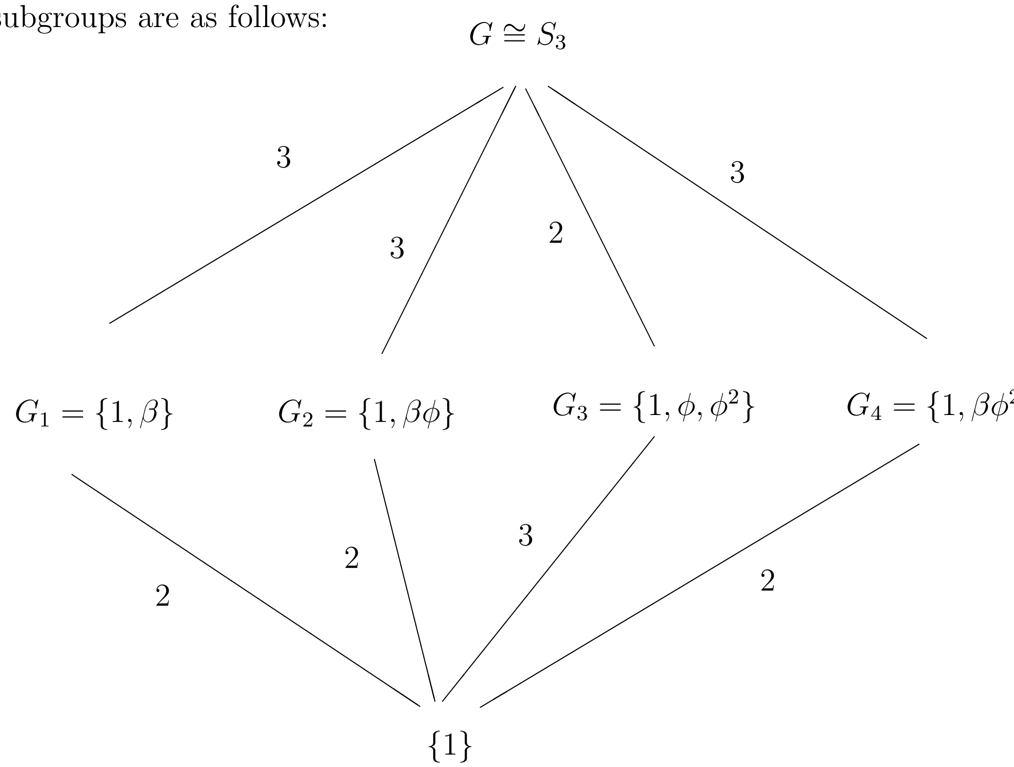
Hence $\phi$ is a $\mathbf{Q}$-automorphism of $K$ of order 3.

$$\begin{aligned}\textit{Let}\quad \beta:K&\longrightarrow K.\\ w&\longrightarrow w^2\\ \sqrt[3]{2}&\longrightarrow \sqrt[3]{2}.\end{aligned}$$

$\beta^2 = 1$,

$$\begin{aligned} G(K, \mathbf{Q}) &= \{1, \phi, \phi^2, \beta, \beta\phi, \beta\phi^2\} \\ \phi\beta(\sqrt[3]{2}) &= \phi(\sqrt[3]{2}) = \sqrt[3]{2}w \\ \beta\phi(\sqrt[3]{2}) &= \beta(\sqrt[3]{2}w) = \sqrt[3]{2}w^2. \end{aligned}$$

Hence $G$ is a non-commutative group of order 6. It follows that $G \cong S_3$ subgroups are as follows:




$$\mathcal{F}_{G_1} = \{\alpha = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{2}^2 + a_4 w + a_5\sqrt[3]{2}w + a_6\sqrt[3]{2}^2 w | \beta(\alpha) = \alpha\}$$

It follows that,

$$\mathcal{F}_{G_1} = \{a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{2}^2 | a_1, a_2, a_3 \in \mathbf{Q}\} = \mathbf{Q}(\sqrt[3]{2}).$$

$$\mathcal{F}_{G_2} = \{\alpha | \beta\phi(\alpha) = \alpha\}$$

$$a_1 + a_2\sqrt[3]{2}w + a_3\sqrt[3]{2}^2 w^2 + a_4 w^2 + a_5\sqrt[3]{2}w + a_6\sqrt[3]{2}$$

$= a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{2}^2 + a_4 w + a_5\sqrt[3]{2}w + a_6\sqrt[3]{2}^2 w$, $w^2 + w + 1 = 0$ implies $w^2 = -w - 1$. Then
$a_1 + a_2\sqrt[3]{2}(-w-1) + a_3\sqrt[3]{2}^2)w + a_4(-w-1) + a_5\sqrt[3]{2}w + a_6\sqrt[3]{2}^2$

$$(a_1 - a_4) + \sqrt[3]{2}(a_2 + a_6) + \sqrt[3]{2}^2(-a_3) + w(-a_4)$$

$$+\sqrt[3]{2}w(-a_2 + a_5) + \sqrt[3]{2}^2 w(-a_3)$$

$$\begin{array}{rclrcl} a_1 - a_4 & = & a_1, & -a_2 + a_5 & = & a_5 \\ -a_2 + & = & a_2, & +a_3 & = & a_6 \\ a_6 & = & a_3, & a_2 & = & 0 \\ -a_4 & = & a_4, & a_3 & = & a_6 \end{array}$$

$$\mathcal{F}_{G_2} \quad = \quad \{a_1 + a_3\sqrt[3]{2}^2 + a_5\sqrt[3]{2}w + a_3\sqrt[3]{2}^2 w | a, a_3, a_5 \in \mathbf{Q}\}$$

For $\mathcal{F}_{G_3}$ we have

$$\mathcal{F}_{G_3} \quad = \quad \{\alpha \mid \phi(\alpha) = \alpha\}$$

$\alpha = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{2}^2 + a_4 w + a_5\sqrt[3]{2}w + a_6\sqrt[3]{2}^2 w$, and $\phi(\alpha) = \alpha$ implies

$\phi(\alpha) = a_1 + a_2\sqrt[3]{2}w + a_3\sqrt[3]{2}^2 w^2 + a_4 w + a_5\sqrt[3]{2}w^2 + a_6\sqrt[3]{2}^2$.

$\phi(\alpha) = a_1 + a_2\sqrt[3]{2}w + a_3\sqrt[3]{2}^2(-w-1) + a_4 w + a_5\sqrt[3]{2}(-w-1) + a_6\sqrt[3]{2}^2$.

It follows that

$$\begin{aligned}
a_1 &= a_1. \\
a_2 &= -a_5 \\
a_3 &= -a_3 + a_6 \\
a_4 &= a_4 \\
a_5 &= a_2 - a_5 \\
a_6 &= -a_3 \quad \text{Then} \\
a_5 &= 0 \\
a_2 &= 0 \\
a_3 &= 0 \\
a_6 &= 0
\end{aligned}$$

$$\mathcal{F}_{G_3} = \{a_1 + a_4 w \ \mid \ a_1, a_4 \in \mathbf{Q}\} = \mathbf{Q}(w)$$

$$\mathcal{F}_{G_4} = \{\alpha \ \mid \ \beta\phi^2(\alpha) = \alpha\}$$

$$\begin{aligned}
\beta\phi^2(\alpha) &= \beta(a_1 + a_2\sqrt[3]{2}w^2 + a_3\sqrt[3]{2^2}w + a_4 w + a_5\sqrt[3]{2} + a_6\sqrt[3]{2^2}w^2) \\
&= a_1 + a_2\sqrt[3]{2}w + a_3\sqrt[3]{2^2}w^2 + a_4 w^2 + a_5\sqrt[3]{2} + a_6\sqrt[3]{2^2}w \\
&= a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{2^2} + a_4 w + a_5\sqrt[3]{2}w + a_6\sqrt[3]{2^2}w = \alpha \quad \text{implies} \\
a_1 &= a_1 - a_4 \\
a_2 &= a_5 \\
a_3 &= -a_3 \\
a_4 &= -a_4 \\
a_5 &= a_2 \\
a_6 &= -a_3 + a_6
\end{aligned}$$

Then $a_3 = 0$, $a_4 = 0$,

$$\mathcal{F}_{G_4} = \{a_1 + a_2\sqrt[3]{2} + a_2\sqrt[3]{2}w + a_6\sqrt[3]{2^2}w \ \mid \ a_1, a_2, a_6 \in \mathbf{Q}\}$$

$$\begin{aligned}\mathcal{F}_{G_4} &= \{a_1 + a_2(\sqrt[3]{2} + \sqrt[3]{2}w) + a_6\sqrt[3]{2}w \ \mid \ a_1, a_2, a_6 \in \mathbf{Q}\} \\ &= \mathbf{Q}(\sqrt[3]{2} + \sqrt[3]{2}w) \quad \text{as} \quad \sqrt[3]{2^2}w = (\sqrt[3]{2} + \sqrt[3]{2}w)^2\end{aligned}$$

(91) Find a splitting field $K \subseteq \mathbb{C}$ for $x^5 - 1 \in \mathbf{Q}[x]$ and determine $|K : \mathbf{Q}|$.

**Solution:** $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$

Let for a prime $p$, $g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Then $\frac{x^p - 1}{x-1} = g(x)$. Now substitute, $y+1$ for $x$ we get

$$\frac{(y+1)^p - 1}{y} = g(y+1) = \frac{y^p + py^{p-1} + \cdots + py}{y} = y^{p-1} + py^{p-2} + \cdots + p.$$

But this is an irreducible polynomial by Einsenstein's criterion. In particular $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbf{Q}$.

If $\alpha$ is a root of $x^4+x^3+x^2+x+1$, then $\alpha$ satisfies $x^5-1$. Then, $1,\ \alpha, \alpha^2, \alpha^3\alpha^4$ are distinct roots of $x^5-1$. Hence $\mathbf{Q}(\alpha)$ is a splitting field for $x^5 - 1$ and $|\mathbf{Q}(\alpha) : \mathbf{Q}| = 4$, where $\alpha = cos72 + isin72$ as $\alpha = re^{i\theta}$ and $\alpha^5 = 1$ implies $e^{5i\theta} = 1$ and so $\theta = \frac{2\pi}{5} = 72^o$

(92) If $S = \{\sqrt{p} : p \in Z,\, p \text{ prime }\}$. Show that $|\mathbf{Q}(S) : \mathbf{Q}|$ is infinite.

**Solution:** Let $p_1, p_2, \cdots$ be the positive prime numbers in their natural order. It is clear that the polynomial $x^2 - p$ in $\mathbf{Q}[x]$ has $\sqrt{p}$ as a root and by Einsenstein's criterion it is irreducible over $\mathbf{Q}$. We will show by induction that $\sqrt{p_i} \notin \mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{i-1}})$. Proof by induction on $i$. It is clear that $\sqrt{p_1} \notin \mathbf{Q}$. $i = 2$ shed a light to the induction step, because of this we will show for $i = 2$ as well. If $\sqrt{p}_2 \in \mathbf{Q}(\sqrt{p_1})$, then $\sqrt{p}_2 = a + b\sqrt{p_1}$ where $a$ and $b$ are rational numbers. Then taking the square of both sides we get

$$p_2 = a^2 + b^2 p_1 + 2ab\sqrt{p_1}.$$

But this implies $\sqrt{p_1} \in \mathbf{Q}$ which is impossible. Similar to this technique assume if possible that for all $i < k$, $\sqrt{p_i} \notin \mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{i-1}})$ and $\sqrt{p}_k \in \mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{k-1}})$. This implies $\sqrt{p}_k = a + b\sqrt{p_{k-1}}$

where $a, b \in \mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{k-2}})$. As $\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{k-1}}) = \mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{k-2}})(\sqrt{p_{k-1}})$

Then taking square of both side we get $p_k = a^2 + b^2 p_{k-1} + 2ab\sqrt{p_{k-1}}$. This implies $\sqrt{p_{k-1}}$ is in $\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{k-2}})$ which is impossible by assumption. Hence for any $i$, $\sqrt{p_i} \notin \mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{i-1}})$ and it follows that $|\mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_i}) : \mathbf{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{i-1}})| = 2$. Hence $|\mathbf{Q}(S) : \mathbf{Q}|$ is infinite.

(93) Suppose K is an extension of $F$, $a \in K$ is algebraic over $F$, and deg $m_a(x)$ is odd. Show that $F(a^2) = F(a)$.

**Solution:** deg $m_a(x)$ is odd implies

$$|F(a) : F| = \deg \quad m_a(x) = \quad \text{odd number. But then}$$

$$|F(a) : F(a^2)||F(a^2) : F| = |F(a) : F|$$

Clearly

$$|F(a) : F(a^2)| \leq 2, \quad \text{as} \quad x^2 - a^2 \in F(a^2)[x] \quad \text{is satisfied by a. It cannot be 2 because}$$

$$|F(a) : F(a^2)| \quad | \quad |F(a) : F| \quad \text{which is odd.}$$

Hence

$$|F(a) : F(a^2)| = 1. \quad \text{That implies} \quad F(a) = F(a^2)$$

(94) Show that the field $A \subseteq \mathbb{C}$ of algebraic numbers is algebraically closed.

**Solution:** Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, be any polynomial with $a_i \in A$. Then $|\mathbf{Q}(a_0, a_1, \cdots, a_n) : \mathbf{Q}|$ is finite. Since $\mathbb{C}$ is algebraically closed $f(x)$ has a root $\alpha$ in $\mathbb{C}$ and $|\mathbf{Q}(a_0, a_1, \cdots, a_n, \alpha) : \mathbf{Q}|$ is finite. So $|\mathbf{Q}(\alpha) : \mathbf{Q}|$ is finite. Hence $\alpha \in A$, as every algebraic number $\mathbf{Q}$ is in $A$.

(95) Determine the Galois groups over $\mathbf{Q}$ of the following polynomials:

**a)** $x^3 - 1$

**Solution:** $x^3 - 1 = (x-1)(x^2+x+1)$. Then the roots are $-\frac{1}{2} \pm \frac{\sqrt{3}i}{2}$. Splitting field of $f(x)$ is $K = \mathbf{Q}(-\frac{1}{2} \pm \frac{\sqrt{3}i}{2})$. The map

$$\sigma : K \to K$$

$$a + b\sqrt{3}i \to a - b\sqrt{3}i$$

where $a, b \in \mathbf{Q}$ is a $\mathbf{Q}$-automorphism of $K$ of order 2. Hence $G(K, \mathbf{Q}) = \{1, \sigma\}$.

**b)** $f(x) = x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$.

**Solution:** Since $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbf{Q}$ for any prime $p$, we get $g(x) = x^4+x^3+x^2+x+1$ is irreducible over $\mathbf{Q}$. Observe that if $w$ is a root of $g(x)$, then it satisfies $w^5 = 1$. Hence $w, w^2, w^3, w^4$ are distinct roots of $g(x)$, otherwise minimal polynomial of $w$ will be of degree $< 4$, $K = \mathbf{Q}(w)$ is a splitting field of $g(x)$. The map $\sigma$

$$\begin{array}{rcl} \sigma : K & \to & K \\ w & \to & w^2 \end{array}$$

is a $\mathbf{Q}$-automorphism of $K$ of order 4. Since $|G(K, \mathbf{Q})| = 4$ we get $G = \{1, \sigma^1, \sigma^2, \sigma^3\}$ is the Galois group of $K$ over $\mathbf{Q}$, which is cyclic of order 4.

**c)** $f(x) = x^6 - 1 = (x^3-1)(x^3+1) = (x-1)(x^2+x+1)(x^2-x+1)$

**Solution:** $x^2+x+1$ irreducible over $\mathbf{Q}$.

$x^2-x+1$ irreducible over $\mathbf{Q}$

roots of $x^2+x+1$ is $w = \frac{-1+\sqrt{3}i}{2}, w^2 = \frac{-1-\sqrt{3}i}{2}$

roots of $x^2-x+1$ is $w_1 = \frac{1+\sqrt{3}i}{2}, w_1^2 = \frac{1-\sqrt{3}i}{2}$

$K = \mathbf{Q}(-\frac{1}{2} + \frac{\sqrt{3}i}{2}, -\frac{1}{2} - \frac{\sqrt{3}i}{2}, -\frac{1}{2} - \frac{\sqrt{3}i}{2}, -\frac{1}{2} + \frac{\sqrt{3}i}{2})$ is a splitting field for $f(x)$.

$K = \mathbf{Q}(\frac{\sqrt{3}i}{2})$ since $\pm\frac{1}{2} \in \mathbf{Q}$. $\sqrt{3}i = a$, $a^2 = -3$, $a^2 + 3 = 0$ this implies $m_{a,\mathbf{Q}}(x) = x^2 + 3$ hence $|K : \mathbf{Q}| = 2$.

Let $1 \neq \sigma \in G(K/\mathbf{Q})$ such that

$$\left\{ \begin{array}{l} \sigma(w) = w^2 \\ \sigma(w_1) = w_1^2 \end{array} \right\}. \quad \text{Then} \quad \begin{array}{l} \sigma^2(w) = w \\ \sigma^2(w_1) = w_1 \end{array}$$

hence $G(K/\mathbf{Q}) = \{1, \sigma\}$

(96) Let $G = G(\mathbb{R} : \mathbf{Q})$

(i) If $\varphi \in G$ and $a \leq b$ in $\mathbb{R}$ show that $\varphi(a) \leq \varphi(b)$.

(ii). Show that $G = 1$.

**Solution:** (i) If $a = b$, then $\varphi(a) = \varphi(b)$. If $a \leq b$, then $b - a \geq 0$ so $(b - a) = t^2$ for some $t \in \mathbb{R}$.

$\varphi(b - a) = \varphi(b) - \varphi(a) = \varphi(t^2) = \varphi(t)\varphi(t) = (\varphi(t))^2 \geq 0$ hence $\varphi(b) - \varphi(a) \geq 0$ it follows that $\varphi(a) \leq \varphi(b)$.

(ii) Assume $1 \neq \varphi \in G$ and let $a \in \mathbb{R}$ such that $\varphi(a) = b \neq a$. Assume without loss of generality that $a < b$. Then there exists $q \in \mathbf{Q}$ such that $a < q < b$.

By the above observation.

$\varphi(q) > \varphi(a)$ and $\varphi(b) > \varphi(q)$ this implies that $q > b$ and $b > q$. This is a contradiction hence $\varphi = 1$.

(97) Give an example of fields $F \subseteq E \subseteq K$ such that $K$ is normal over $E$ and $E$ is normal over $F$ but $K$ is not normal over $F$.

**Solution:** $\mathbf{Q}(\sqrt{2})$ is a normal extension of $\mathbf{Q}$.

The minimal polynomial of $\sqrt{2}$ over $\mathbf{Q}$ is $x^2 - 2$ (By Einsenstein Criterion it is irreducible). Then $|\mathbf{Q}(\sqrt{2}) : \mathbf{Q}| = 2$.

$\mathbf{Q}(\sqrt{2})$ is a splitting field for $x^2 - 2$ hence $\mathbf{Q}(\sqrt{2})$ is a normal extension of $\mathbf{Q}$. In fact any extension of $\mathbf{Q}$ of degree 2 is a normal extension.

Similarly $\mathbf{Q}(\sqrt[4]{2})$ is a normal extension of $\mathbf{Q}(\sqrt{2})$ since the minimal polynomial of $\sqrt[4]{2}$ over $\mathbf{Q}(\sqrt{2})$ is $x^2 - \sqrt{2}$. $\mathbf{Q}(\sqrt[4]{2})$ is a splitting field for $x^2 - \sqrt{2}$ then again by Theorem 3.5 it is normal $(x^2 - \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2}) \in \mathbf{Q}(\sqrt[4]{2})[x]$.

But $\mathbf{Q}(\sqrt[4]{2})$ is not a normal extension of $\mathbf{Q}$ since minimal polynomial of $\sqrt[4]{2}$ over $\mathbf{Q}$ is $x^4 - 2$. By Eisenstein criterion it is irreducible and the roots of $x^4 - 2$ are $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$, $-i\sqrt[4]{2}$.

$i\sqrt[4]{2}$ is a root of the irreducible polynomial $(x^4 - 2)$ but $i\sqrt[4]{2}$ is not an element of $\mathbf{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ and $i\sqrt[4]{2} \in \mathbb{C} \setminus R$ therefore $\mathbf{Q}(\sqrt[4]{2})$ is not a normal extension of $\mathbf{Q}$.

(98) A field $F$ is called perfect if either char $F = 0$ or else $CharF = p$ and $F = F^p = \{a^p : a \in F\}$.

(i) If $F$ is finite show that the map $\varphi : a \to a^p$ is a monomorphism and conclude that $F$ is perfect.

**Solution:** $\begin{array}{rcl} \varphi : F & \to & F^p \\ a & \to & a^p \end{array}$

**Claim:** $\varphi$ is a homomorphism $\varphi(a + b) = (a + b)^p = a^p + b^p = \varphi(a) + \varphi(b)$ $\varphi(ab) = a^p b^p = \varphi(a)\varphi(b)$

$$\ker \varphi = \{a \in F : a^p = 0\} = \{0\}$$

$\varphi$ is also onto since for all $x^p \in F^p$ there exists $x \in F$ such that

$$\varphi(x) = x^p \in F^p.$$

$F^p \subset F$ and on a finite set $B$ a one-to-one map from $B$ into $B$ is onto. This implies $F = F^p$.

(ii) Show that the field $Z_p(t)$ of rational functions in the indeterminate $t$ is not perfect.

$$Z_p(t) = \{\frac{f(t)}{g(t)} \mid f(t) \in Z_p[t] \quad \text{and} \quad 0 \neq g(t) \in Z_p(t)\ \}$$

$$(Z_p(t))^p = \{\frac{f(t)^p}{g(t)^p} \mid f \quad \text{and} \quad g \in Z_p[t] \quad \text{and} \quad g(t) \neq 0\ \}$$

since Char $Z_p(t) = p \neq 0$, so it is enough to show that $Z_p(t) \neq (Z_p(t))^p$. Observe that $t \in Z_p(t)$ but $t \notin (Z_p(t))^p$ since all polynomials in $(Z_p(t))^p$ is of degree $\geq p$. Therefore

$(Z_p(t))^p \neq Z_p(t)$ i.e. $Z_p(t)$ is not a perfect field.

(99) If $F$ is a finite field of characteristic $p$ show that every element of $F$ has a unique $p^{th}$ root.

**Solution:** We have shown in Question 98 that if $F$ is a finite field of characteristic $p$, the Frobenius map $\begin{array}{rcl}\sigma : F & \to & F \\ x & \to & x^p\end{array}$ is an automorphism of the field $F$. Since $\sigma$ is an automorphism the inverse of $\sigma$ sends $x^p$ to $x$, i.e. to the $p^{th}$ roots of $x^p$. Therefore every element has a unique $p^{th}$ root as $\sigma^{-1} : F^p = F \to F$

(100) Let $F$ be a finite field.

(1) Show that the product of all elements in $F^*$ is -1.

(2) Conclude Wilson's Theorem: If $p \in \mathbf{Z}$ is a prime, then $(p-1)! \equiv -1$ (mod p).

**Solution:** (1) Every finite field $F$ is a splitting field for a polynomial $f(x) = x^q - x$ for some prime power $q = p^n$. Since $F^* = F - \{0\}$ and $F$ is a splitting field for $f(x)$, we get every element of $F^*$ is a root of $x^{q-1} - 1$. Since $x^{q-1} - 1$ splits over $F$ and all the roots in $F^*$ are distinct, we get the product of elements of $F^*$ is -1. i.e.

$$x^{q-1} - 1 = (x - a_1)(x - a_2) \cdots (x - a_{q-1})$$

giving $-1 = (-1)^{q-1} a_1 \ldots a_{q-1}$. If $q$ is odd we are done. If $q$ is even then $\mathrm{char}(F) = 2$ we have $-1 = 1$ and again the result follows.

(2) If $p$ is a prime, then $Z_p$ is a field and

$$Z_p^* = \{1, 2, 3, \cdots, p-1\}.$$

Hence $1.2. \cdots p - 1 = (p-1)! \equiv -1$ (mod p).

(101) If $F$ is a finite field, show that every element of $F$ is a sum of two squares in $F$.

Hint: Use, if $S \subseteq G, G$ is a finite group and $|S| > \frac{|G|}{2}$ , then $S^2 = G$ See Question 8.

**Solution:** Let $S = \{a^2 \mid a \in F\} \subseteq F$. Consider the map $\begin{array}{rcl} \varphi : F^* & \to & F^* \\ x & \to x^2 & \end{array}$ $\varphi$ is a group homomorphism and $F^*/\ker\varphi \cong Im\varphi = (F^*)^2$. $\ker\varphi = \{x \in F^* \mid x^2 = 1\}$.

Since $F^*$ is a cyclic group, there exists only one subgroup of any given order dividing $|F^*|$. Hence either $|\ker\varphi| = 2$ or $|\ker\varphi| = 1$. In any case by including $0 \in F$ to $(F^*)^2$ we get $S = \{(F^*)^2\} \cup \{0\}$. Then $|S| = \frac{|F^*|}{2} + 1 = \frac{|F|-1}{2} + 1 = \frac{|F|}{2} + \frac{1}{2} > \frac{|F|}{2}$. Hence $|S| > \frac{|F|}{2}$. Hence we get $S + S = F$ in the additive notation. Namely every element in $F$ can be written as a sum of two squares in $F$.

(102) If $f(x) \in F[x]$ and $K$ is a splitting field for $f(x)$ over $F$, denote by $S$ the set of distinct roots of $f(x)$ in $K$ and let $G = G(K : F)$. If $f(x)$ is irreducible over $F$ show that $G$ is transitive on $S$. If $f(x)$ has no repeated roots and $G$ is transitive on $S$ show that $f(x)$ is irreducible over $F$.

**Solution:** Assume that $f(x)$ is irreducible over $F$, and $a$ and $b$ be two elements of $S$. Then $a$ and $b$ are conjugates hence there exists an $F$-isomorphism

$$\begin{array}{rcr} \phi : F(a) & \to & F(b) \\ a & \to & b \end{array}$$

But this isomorphism can be extended to an $F$-automorphism $\overline{\phi}$ of the field $K$. Hence $\overline{\phi}(a) = b$, and $\overline{\phi} \in G(K : F)$. So $G$ is transitive on $S$.

Now assume that $f(x)$ has no repeated roots and $G$ is transitive on $S$. Assume if possible that $f(x)$ is reducible, say $f(x) = g(x)h(x)$ $\deg g(x) \geq 1$ and $\deg h(x) \geq 1$. Since $K$ is a splitting field for $f(x)$, let $a$ be a root of $g(x)$ and $b$ be a root of $h(x)$ in $K$. Then as $G$ is transitive there exists an automorphism $\phi \in G$ such that $\phi(a) = b$. But then $m_{a,F}(x) \in F[x]$ and $b$ satisfies $m_{a,F}(x)$. Then every root of $g(x)$ is a root of $h(x)$. But $f(x)$ does not have repeated roots. Hence we get $f(x)$ is irreducible.

(103) Determine the Galois group (over $\mathbf{Q}$ ) of the following polynomials.

(i) $f(x) = x^4 - 2$.

(ii) $f(x) = x^4 - 7x^2 + 10 = (x^2 - 5)(x^2 - 2)$.

(iii) $f(x) = x^6 - 3x^3 + 2$.

**Solution: (i)** $x^4 - 2$ is irreducible over $\mathbf{Q}$ and the roots of $f(x)$ over $\mathbf{Q}$ in $\mathbb{R}$, are $a = \sqrt[4]{2}$ and the others are

$$\begin{aligned} w^4 = 1. \text{ Then } w^4 - 1 &= (w^2-1)(w^2+1) \quad \text{and} \\ &= (w-1)(w+1)(w^2+1) \end{aligned}$$

So $a, -a, ia, -ia$ are roots of $f(x)$

$$|(K : \mathbf{Q})| = |K : \mathbf{Q}(a)|\ |\mathbf{Q}(a) : \mathbf{Q}| = 8.$$

hence $|(G(K : \mathbf{Q}))| = 8$. Let $\tau$, $1 \pm \sigma \in G(K : \mathbf{Q})$. Then

$$\begin{aligned} \sigma(a) &= ai \\ \sigma^2(a) &= -a \\ \sigma^3(a) &= -ia \\ \sigma^4(a) &= a \\ \tau(ai) &= -ai \qquad \tau(a) = a \\ \tau^2(ai) &= ai \end{aligned}$$

$$G = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

since $\sigma(ai) = -a, \quad \tau(ai) = -ai$ we have $\tau \neq \sigma$.

$$\tau^{-1}\sigma\tau(a) = \tau^{-1}\sigma(a) = \tau^{-1}(ai) = -ai$$

$$\tau^{-1}\sigma(\tau(ai)) = \tau^{-1}\sigma(-ai) = \tau^{-1}(-ai)i = a$$

$$\sigma^3(ai) = \sigma(\sigma(\sigma(ai)) = \sigma\sigma(-a) = \sigma(-ai) = ai(-i) = a$$

$$\tau^{-1}\sigma\tau = \sigma^3.$$

So $G(K, \mathbf{Q})$ is isomorphic to $D_8$.

**(ii).** $f(x) = x^4 - 7x^2 + 10 = (x^2 - 5)(x^2 - 2)$. The polynomials $x^2 - 5$ and $x^2 - 2$ are irreducible by Eisenstein criterion over $\mathbf{Q}$ hence

$$x^2 - 5 = 0 \Rightarrow x = \pm\sqrt{5} \quad x^2 - 2 = 0 \Rightarrow x = \pm\sqrt{2}$$

$K = \mathbf{Q}(\sqrt{5}, \sqrt{2})$ is a splitting field for $f(x)$ and it is separable hence Galois extension and as $\sqrt{2} \notin \mathbf{Q}(\sqrt{5})$

$$|K : \mathbf{Q}| = |K : \mathbf{Q}(\sqrt{5})| \; |\mathbf{Q}(\sqrt{5}) : \mathbf{Q}| = 4$$

the roots are $\sqrt{5}, -\sqrt{5}, \sqrt{2}, -\sqrt{2}$. Let $\sigma \in G(K : \mathbf{Q})$ $\sigma(\sqrt{5}) = -\sqrt{5}$, $\sigma(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{5}) = \sqrt{5}$, $\tau(\sqrt{2}) = \sqrt{2}$.

$$\sigma\tau(\sqrt{5}) = \sigma(\sqrt{5}) = -\sqrt{5}$$

$$\tau\sigma(\sqrt{5}) = \tau(-\sqrt{5}) = -\sqrt{5}$$

and

$$\tau\sigma\tau = (\sqrt{5}) = \tau\sigma(\sqrt{5}) = \tau(-\sqrt{5}) = -\sqrt{5}$$

$$\tau\sigma\tau(\sqrt{2}) = \tau\sigma(-\sqrt{2}) = \tau(-\sqrt{2}) = \sqrt{2}$$

so $\tau\sigma\tau = \tau$. Therefore $G = \{1, \sigma, \tau, \sigma\tau\}$ is a commutative noncyclic group of order 4. Hence it is isomorphic to Klein Four group.

**(iii)** We have $f(x) = x^6 - 3x^3 + 2 = (x^3 - 2)(x^3 - 1) = 0 = (x^3 - 2)(x - 1)(x^2 + x + 1)$ where $x^3 - 2$ and $x^2 + x + 1$ are irreducible.

The roots of $x^3 - 2$ are $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2$ where $w$ is a primitive $3^{rd}$ root of unity, and roots of $x^2 + x + 1$ are $w, w^2$. $K = \mathbf{Q}(\sqrt[3]{2}, w)$ is splitting field for $f(x)$

$$\underbrace{|K : \mathbf{Q}(\sqrt[3]{2})|}\,\underbrace{|\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}|} = 6$$

$$\sigma(\sqrt[3]{2} = \sqrt[3]{2}w \qquad \sigma(w) = w$$

$$\tau(\sqrt[3]{2} = \sqrt[3]{2} \qquad \tau(w) = w^2$$

since the roots of $f(x)$ are $1, \sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2, w, w^2$

$$\{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

$$\tau^{-1}\sigma\tau(\sqrt[3]{2}) = \tau^{-1}\sigma(\sqrt[3]{2}) = \tau^{-1}(\sqrt[3]{2}w) = \sqrt[3]{2}w^2$$

$$\tau^{-1}\sigma\tau(w) = \tau^{-1}(\sigma w^2) = \tau(w^2) = w$$

$$\tau^{-1}\sigma\tau = \sigma^2$$

hence $G$ is of order 6 non abelian and $\tau\sigma\tau = \sigma^2$

$$G =< \sigma, \tau | \tau\sigma\tau = \sigma^2, \quad \sigma^3 = 1, \quad \tau^2 = 1 >$$

hence $G \cong S_3$.

(104) For any $f(x) \in F[x]$ set $f^0(x) = f(x), f^{(1)}(x) = f'(x)$ and in general let $f^{(n)}(x)$ be the derivative of $f^{(n-1)}(x), 1 \leq n \in Z$ if $f(x)$; $g(x) \in F[x]$ set $h(x) = f(x)g(x)$ and show that

$$h^{(n)}(x) = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} f^{(n-k)}(x)g^{(k)}(x)$$

(This is Leibniz's rule)

**Solution.** Induction on $n$

If $n = 0$, then $h(x) = f(x)g(x)$

If $n = 1$, then $h'(x) = f'(x)g(x) + f(x)g'(x)$

Assume it is true for $n - 1$. Then

$$\begin{aligned} h^{(n-1)}(x) &= \sum_{k=0}^{n-1} \begin{pmatrix} n-1 \\ k \end{pmatrix} f^{(n-1-k)}(x)g^{(k)}(x). \\ \frac{d}{dx}(h^{(n-1)}(x)) &= \sum_{k=0}^{n-1} \begin{pmatrix} n-1 \\ k \end{pmatrix} \frac{d}{dx} f^{(n-1-k)}(x)g^{(k)}(x) \end{aligned}$$

$$\begin{aligned} h^{(n)}(x) &= \sum_{k=0}^{n-1} \begin{pmatrix} n-1 \\ k \end{pmatrix} [f^{(n-k)}(x)g^{(k)}(x) + f^{(n-1-k)}(x)g^{(k+1)}(x) \\ &= \sum_{k=0}^{n-1} \begin{pmatrix} n-1 \\ k \end{pmatrix} f^{(n-k)}(x)g^{(k)}(x) + \sum_{k=0}^{n-1} \begin{pmatrix} n-1 \\ k \end{pmatrix} f^{(n-1-k)}(x)g^{(k+1)}(x) \end{aligned}$$

Let $k + 1 = m$ for the second equation. Then

$$= \sum_{k=0}^{n-1} \binom{n-1}{k} f^{(n-k)}(x)g^{(k)}(x) + \sum_{m=1}^{n} \binom{n-1}{m-1} f^{(n-m)}g^{(m)}(x) \tag{1}$$

$$= \sum_{k=0}^{n-1} \binom{n-1}{k} f^{(n-k)}(x)g^{(k)}(x) + \sum_{k=1}^{n} \binom{n-1}{k-1} f^{(n-k)}(x)g^{(k)}(x) \tag{2}$$

$$= \sum_{k=1}^{n-1} \binom{n-1}{k} f^{(n-k)}(x)g^{(k)}(x) + \sum_{k=1}^{n-1} \binom{n-1}{k-1} f^{n-k}(x)g^{k}(x) + f^{(n)}(x)g(x) + f(x)g^{(n)}(x) \tag{3}$$

$$= \sum_{k=1}^{n-1} \left[\binom{n-1}{k} + \binom{n-1}{k-1}\right] f^{(n-k)}(x)g^{(k)}(x) + f^{(n)}(x)g(x) + f(x)g^{(n)}(x). \tag{4}$$

Now we will show that $\left[\binom{n-1}{k} + \binom{n-1}{k-1}\right] = \binom{n}{k}$ (5)

$$\frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-1-k-1)!} = \frac{(n-1)!}{k!(n-k-1)!} + \frac{(n-1)!}{(n-k)!(k-1)!} \tag{6}$$

(7)

$$= \frac{(n-1)!(n-k) + (n-1)!(k)}{k!(n-k)!} = \frac{(n-1)!(n-k+k)}{k!(n-k)!} = \frac{(n-1)!n}{k!(n-k)!} = \frac{n!}{(n-k)!k!}. \tag{8}$$

Then (9)

$$\sum_{k=1}^{n-1} \binom{n}{k} f^{(n-k)}(x)g^{(k)}(x) + f^{(n)}(x)g(x) + f(x)g^{(n)}(x) \tag{10}$$

$$= \sum_{k=0}^{n} \binom{n}{k} f^{(n-k)}(x)g^{(k)}(x) \tag{11}$$

(105) If char $(F) = 0$, and $f(x)$ has degree $n$ in $F[x]$ show that $f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k$.

**Proof.** Let

$$g(x) = \sum_{k=0}^{n} \frac{f^{k}(a)}{k!}(x-a)^k = f(a)+f'(a)(x-a)+\frac{f''(a)}{2!}(x-a)^2+\cdots+\frac{f^{n}(a)}{n!}(x-a)^n$$

Then

$$\begin{aligned} g(a) &= f(a) \\ g'(a) &= f'(a) \\ &\vdots \\ g^{(n)} &= f^{(n)}(a). \end{aligned}$$

Let $h(x) = f(x) - g(x)$. Then $h(a) = g(a) - f(a) = 0$ implies that $x - a|h(x)$.

$h'(x) = f'(x) - g'(x) \qquad h'(a) = g'(a) - f'(a) = 0$ implies $(x-a)^2|h(x)$

$h^{(n)}(x) = f^{(n)} - g^{(n)}(x)$. Hence $h^{(n)}(a) = f^{(n)}(a) - g^{(n)}(a) = 0$ implies $(x-a)^{n+1}|h(x)$.

But degree of $h(x) \leq n$ since $\deg f = \deg g = n$ hence. $h(x) = 0$ this implies $f(x) = g(x)$ i.e.

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k$$

(106) Suppose $F$ is a field and $K = F(x)$ the field of rational functions in the indeterminate $x$ over $F$.

If $u \in K \setminus F$ show that $u$ is transcendental over $F$.

**Solution:** Let $K = F(x) = \{\frac{f(x)}{g(x)} \mid f(x),\ g(x) \in F[x], g(x) \neq 0\}$. Let $u \in K \setminus F$. Assume if possible that $u$ is algebraic over $F$, so there exists a polynomial $h(t) \in F[t]$ such that $h(u) = 0$. Since $u \in K \setminus F$ the element $u$ is of the form $\frac{f(x)}{g(x)}$ where $g(x) \neq 0$ and $\frac{f(x)}{g(x)}$ is not a constant (not in $F$) $(f(x),\ g(x)) = 1$.

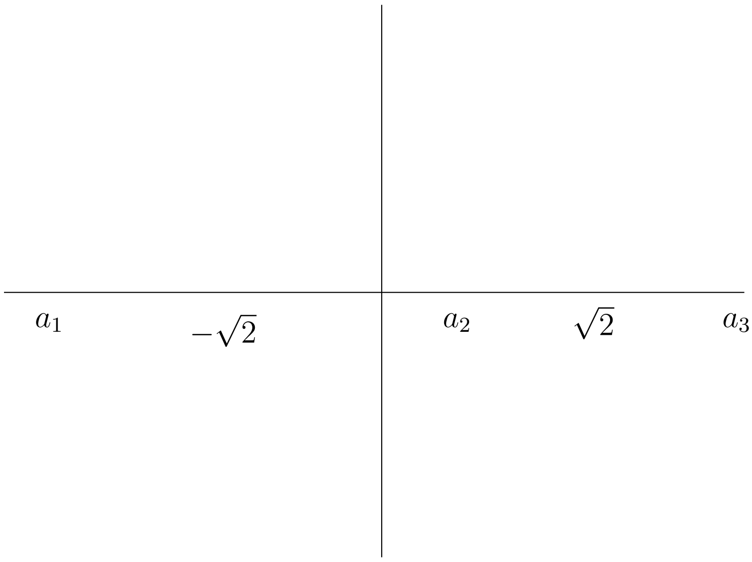
If $h$ is of degree $n$, then consider the polynomial $t(x)$ where $t(x) = (g(x))^n$. Then $h(u) = 0$ implies $h(u) = (g(x))^n h(\frac{f(x)}{g(x)}) = 0$ which is a polynomial in $F[x]$. This implies that $x$ is algebraic over $F$ but $x$ is indeterminate. This contradiction implies that, $u$ is a transcendental element.

(107) Show that $f(x) = x^5 - 2x^3 - 8x + 2$ is not solvable by radicals over $\mathbf{Q}$.

**Solution:** By Eisenstein criteria, $f(x)$ is an irreducible polynomial.

$f'(x) = 5x^4 - 6x^2 - 8 = (5x^2+4)(x^2-2)$.

Since $5x^2+4$ is always positive, the graph of $f(x)$ is roughly the following




Hence $f(x)$ has 3 real roots $a_1, a_2, a_3$ and two complex roots which are conjugate of each other.

Let $K \subseteq \mathbb{C}$ be a splitting field for $f(x)$ over $\mathbf{Q}$ and let $G = G(K : \mathbf{Q})$ be the Galois group of $f(x)$ viewed as a subgroup of $S_5$. Since $5 \mid |K : \mathbf{Q}|$ and hence $5 \mid |G|$ there must be a 5-cycle in $G$. There exists an automorphism which sends $a_4$ to $a_5$ and fix the others. This gives a 2-cycle in $G$. Hence in $G$ there exists a 5-cycle and a 2-cycle. It follows that $G \cong S_5 = \langle (1,2,3,4,5), (4,5) \rangle$. But $S_5$ is not a solvable group, as $A_5$ is a simple group of order 60. Hence $f(x)$ is not solvable by radicals.

(108) Suppose $F_q$ and $F_r$ are finite fields, with $q = p^m$ and $r = p^n$, $p$ prime. Show that $F_q$ has a subfield (isomorphic with) $F_r$ if and only if $n|m$.

**Solution.** Assume that $F_q$ has a subfield isomorphic to $F_r$ where $r = p^n$. Let $F = F_p$ prime field isomorphic to $Z_p$. Then $F_q$ is an extension of the field $F_r$. Hence

$$m = |F_q : F| = |F_q : F_r|\ |F_r : F| = |F_q : F_r|.n$$

Hence $n|m$.

Conversely assume that $n$ divides $m$. We already know that all finite fields of characteristic $p$ and of order $p^m$ are isomorphic and they are splitting fields of $x^{p^m} - x$. Therefore it is enough to show that all roots of $x^{p^n} - x$ are roots of $x^{p^m} - x$.

Let $a$ be a root of $x^{p^n} - x$. Then $a^{p^n} = a$. If $kn = m$ we get $a^{p^m} = a^{p^{nk}} = (a^{p^n})^{p^{(k-1)n}} = a^{p^{(k-1)n}} = \cdots = a^{p^n} = a$. Hence we are done.

(109) List al subfields of $F_q$ if $q = 2^{20}$, $q = p^{30}$, $p$-prime.

**Solution.** For $q = 2^{20}$. By previous question $F_q = F_{2^{20}}$ has subfields of order $2^n$ for $n|20$. So they are $n = 1, 2, 4, 5, 10, 20$. Hence $F_2, F_{2^2}, F_{2^4}, F_{2^5}, F_{2^{10}}, F_{2^{20}}$.

By the same reason $q = p^{30}$ we have the divisors of 30 as, 1,2,3,5,6,10,15,30. Hence the subfields are $F_p, F_{p^2}, F_{p^3}, F_{p^5}, F_{p^6}, F_{p^{10}}, F_{p^{15}}, F_{p^{30}}$.

# MODULES

(110) If $R$ is a ring with 1 and $M$ is an $R$-module that is not unitary show that $Rm = 0$ for some non-zero $m \in M$.

**Solution:** $M$ is not unitary implies that there exist $x \in M$ such that $1x \neq x$. Let $m = 1x - x \neq 0$. Then for any $r \in R, rm = r(1x - x) = rx - rx = 0$. Hence $m$ is the required element and $Rm = 0$.

(111) Give an example of an $R$-module $M$ having $R$-isomorphic submodules $N_1$ and $N_2$ such that $M/N_1$ and $M/N_2$ are not isomorphic.

**Solution:** $\mathbf{Z} = M$ is a $\mathbf{Z}$-module. Let $N_1 = \mathbf{Z}$. Let $N_2 = 2\mathbf{Z}$. Define a map

$$\begin{aligned} f \quad &: \quad \mathbf{Z} \to 2\mathbf{Z}. \\ x \quad &\to \quad 2x. \end{aligned}$$

$f(x + y) = 2(x + y) = 2x + 2y$ and for any $m \in \mathbf{Z}$, $f(mx) = 2mx = m2x = mf(x)$. Moreover $Ker\ (f) = \{x \in \mathbf{Z} \mid 2x = 0\} = \{0\}$ and $f$ is onto. Hence $\mathbf{Z} \cong 2\mathbf{Z}$ as a $\mathbf{Z}$-module. Hence $\mathbf{Z} \cong 2\mathbf{Z}$. But $\mathbf{Z}_2 \cong \mathbf{Z}/2\mathbf{Z}$ has 2-elements and $\mathbf{Z}/\mathbf{Z} \cong \{\bar{0}\}$ has only one element. Hence they can not be isomorphic.

(112) Suppose $V$ is a finite dimensional vector space over the field $F$, viewed as an $F$-module. Describe a composition series for $V$ and determine its factors.

**Solution:** Every vector space of dimension $n$ over the field $F$ is isomorphic to $F^n = F \times \cdots \times F$ ($n$ times). Since factor modules are also vector spaces, over the field $F$, in the composition series they must have dimension 1. Hence the composition series is of length $n$ and each factor isomorphic to $F$ as an $F$-vector space of dimension 1. If $\{e_1, e_2, \ldots e_n\}$ is a basis for $V$ then $\{0\} \subseteq \{e_1\} \subseteq \{e_1, e_2\} \subseteq \ldots$ becomes a composition series of $V$.

(113) A sequence $K \xrightarrow{f} M \xrightarrow{g} N$ of $R$-homomorphisms of $R$-modules is exact at $M$ if $Im(f) = \ker g$. A short exact sequence $0 \to K \to M \to N \to 0$ is exact at $K, M$ and $N$.

If $0 \to K \xrightarrow{f} M \xrightarrow{g} N \to 0$ is a short exact sequence show that $M$ is Noetherian if and only if $K$ and $N$ are both Noetherian.

**Solution:** Assume that $M$ is Noetherian. Then as $K$ is isomorphic to $Imf$ which is a submodule of $M$ by using the fact that submodule of a Noetherian module is Noetherian we get that $K$ is Noetherian. Since $g$ is onto $M/\ker g \cong N$. Moreover as $M$ is Noetherian $M/\ker g$ is Noetherian as homomorphic image of a Noetherian module is again Noetherian. Hence $N$ is Noetherian.

Conversely one can see easily from the previous paragraph and from the assumption $Imf = \ker g$ that $M/\ker g$ and $Imf \cong K$ are Noetherian. This implies $M$ is Noetherian as extension of a Noetherian module by a Noetherian module is Noetherian.

(114) Suppose $M_1, M_2$ and $N$ are submodules of an $R$-module $M$ with $M_1 \subseteq M_2$. Show that there is an exact sequence.

$$0 \to (M_2 \cap N)/(M_1 \cap N) \xrightarrow{f} M_2/M_1 \xrightarrow{g} (M_2 + N)/(M_1 + N) \to 0$$

**Solution:** $M_1 \subseteq M_2$ implies that $M_1 + N \subseteq M_2 + N$. Hence define a map

$$\begin{aligned} g\colon\ & M_2/M_1 \to (M_2 + N)/(M_1 + N) \\ & m + M_1 \to m + (M_1 + N) \end{aligned}$$

It is easy to check that $g$ is a module epimorphism.

$$\begin{aligned}
\ker g &= \{m + M_1 \mid m + (M_1 + N) = (M_1 + N) \text{ where } m + M_1 \in M_2/M_1\ \} \\
&= \{m + M_1 \mid m \in M_1 + N\ \} \\
&= \{m + M_1 \mid m \in M_2 \cap (M_1 + N)\ \} = \{m + M_1 \mid m \in (M_2 \cap N) + M_1\} \\
&= (M_2 \cap N) + M_1/M_1
\end{aligned}$$

Hence $\ker g = Im(f)$ where $f$ is the module homomorphism from $(M_2 \cap N)/(M_1 \cap N)$ into $M_2/M_1$ such that

$$f(m + (M_1 \cap N)) = m + M_1 \text{ where } \ m \in (M_2 \cap N)$$

$f$ is clearly one to one and moreover $g$ is onto. Hence $Im\ f = \ker\ g$ and the given sequence is exact.

(115) Let $R = F[x]$ and $F$ be a field. Let $V$ be a vector space over $F$, and let $T : V \to V$ be a linear transformation. If $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ define $f(T) = a_0I + a_1T + \cdots + a_nT^n$ also a linear transformation on $V$. Let $L(V, V)$ be the set of linear transformations on $V$. Then $f(x) \to f(T)$ becomes a homomorphisms from $F[x]$ into $L(V, V)$. If we define $f(x) \cdot v = f(T)(v)$, then $V$ becomes an $F[x]$-module which is usually denoted by $V_T$.

a) If $F = \mathbf{Q}$ and $V$ is the $\mathbf{Q}$-space of all column vectors with 2 entries from $\mathbf{Q}$, the map $T : V \to V$ is the result of the multiplication by the matrix $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ & \end{bmatrix}$ and $f(x) = x^m - x$ determine the module action $f(x)v$ on an arbitrary vector $v = \begin{bmatrix} a \\ b \end{bmatrix}$ in $V_T$.

b) If $u = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $v = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ find order of $u$ and $v$.

**Solution:** a) $f(x) = x^m - x$. Then $A^m - A = \begin{bmatrix} 0 & m-1 \\ 0 & 0 \end{bmatrix}$.

Then for any $v = \begin{bmatrix} a \\ b \end{bmatrix}$ in $V_T$.

$$f(x).v = \begin{bmatrix} 0 & m-1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} (m-1)b \\ 0 \end{bmatrix}$$

b) Let $u = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Then

$$A(u) = \{\ f(x) \in \mathbf{Q}[x] \quad | \quad f(x).u = 0 \ \}$$

Let $f(x) = x - 1$. Then $(T - I)(u) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.

Since $f$ is polynomial of degree 1, we get $A(u) = (x - 1)$.

$$A(v) = \{g(x) \quad | \quad g(T).v = 0 \quad \}$$

$(T^2 - 2T + I)v = 0$. Hence $g(x) = x^2 - 2x + 1 \in A(v)$ and for any divisor $h(x) \neq g(x)$ of $g(x)$ we get $h(x).v \neq 0$. Hence $A(v) = (x^2 - 2x + 1)$.

(116) Let $F$ be a free abelian group ( vector space over a field $K$) with countably infinite basis $\{a_1, a_2, \cdots\}$, and let $R = End(F)$. Show that $R$, as a free $R$-module, has one basis $B_1 = \{1_R\}$, but also another basis $B_2 = \{\phi_1, \phi_2\}$ where

$$\phi_1(a_{2n}) = a_n \qquad \phi_1(a_{2n-1}) = 0$$

$$\phi_2(a_{2n}) = 0 \qquad \phi_2(a_{2n-1}) = a_n \qquad n = 1, 2, 3, \cdots$$

**Remark:** Recall that if $R$ is a principal ideal domain rank of a free module $M$ is an invariant and rank of a submodule of a free module $M$ is less than or equal to rank of $M$.

**Solution:** It is clear that, $1_R$ is linearly independent over $R$ and it spans $R$. First observe that $\phi_1$ and $\phi_2$ are $R-$linearly independent. Indeed if

$$r_1\phi_1 + r_2\phi_2 = 0 \qquad r_1, r_2 \in R,$$

then for any $n \in \mathbf{N}$ we have,

$$r_1(a_n) = r_1\phi_1(a_{2n}) + r_2\phi_2(a_{2n}) = (r_1\phi_1 + r_2\phi_2)(a_{2n}) = 0.$$

Since $r_1$ is an endomorphism and sends every basis element to zero we obtain $r_1 = 0$. Similarly for all $n \geq 1$

$$\begin{aligned} r_2(a_n) &= r_1\phi_1(a_{2n-1}) + r_2\phi_2(a_{2n-1}) \\ &= (r_1\phi_1 + r_2\phi_2)(a_{2n-1}) = 0 \end{aligned}$$

Hence by the above explanation we have $r_2 = 0 \in End(F)$.

Now we show that $B_2$ spans $R$ as an $R$-module i.e., for any $f \in End(F)$ there exists $r_1, r_2 \in R$ such that

$$f = r_1\phi_1 + r_2\phi_2$$

$B = \{a_i \mid i \geq 1\}$ is a basis for a free abelian group $F$. Therefore we may define a map on $B$ and extend it linearly to $F$. Then it becomes an element of $R = End(F)$.

Let $r_1(a_i) = a_{2i}$ and $r_2(a_i) = a_{2i-1}$ for all $i \geq 1$. Then $r_1, r_2 \in R$ and $r_1\phi_1 + r_2\phi_2 = 1$. Hence for any $f \in R$, we have $f = fr_1\phi_1 + fr_2\phi_2$. It follows that $B_2$ spans $R$.

(117) Give an example of an $R$-module $M$ over a commutative ring $R$ where the set $T(M)$ of torsion elements of $M$ is not a submodule.

**Solution:** Consider $\mathbf{Z}_6$ as a $\mathbf{Z}_6$-module

2 is a torsion element since $2.3 = 0$

3 is a torsion element since $3.2 = 0$

But $2 + 3$ is not a torsion element because for any $0 \neq r \in \mathbf{Z}_6$ $r.5 = r(-1) \neq 0$.

(118) Let $R$ be a PID and $M$ be an $R$-module. If $x$ and $y$ are torsion elements with orders $r$ and $s$ respectively and that $r$ and $s$ are relatively prime in $R$. Show that $x + y$ has order $rs$.

**Solution:** Since $r$ and $s$ are relatively prime there exists $r', s' \in R$ such that $rr' + ss' = 1$ Then $k = k1 = krr' + kss'$. If $k$

is the order of $x+y$, then $k(x+y)=0$. Then $kx=-ky$ and $0=rkx=-rky$. This implies that $s|rk$ by assumption $(r,s)=1$ and hence $s|k$. Similarly $r|k$, say $k=r_1r=s_1s$, then $k=(krr'+kss')=s_1srr'+r_1rss'=(s_1r'+r_1s')rs$. i.e. $rs|k$ giving $(k)=(rs)$ i.e $|x+y|=rs$.

(119) Suppose $R$ is a commutative ring and $M$ is an $R$-module. A submodule $N$ is called **pure** if $rN=rM\cap N$ for all $r\in R$

(i) show that any direct summand of $M$ is pure,

(ii) if $M$ is torsion free and $N$ is a pure submodule, show that $M/N$ is torsion free,

(iii) if $M/N$ is torsion free, show that $N$ is pure.

**Solution:** (i) Let $K$ be a direct summand of $M$. Then $M=K\oplus L$, where $K$ and $L$ are submodules of $M$. Then $rM=rK\oplus rL$ . For any $rm\in rM$, there exists $k\in K$ and $l\in L$ such that $m=k+l$. Then $rm=rk+rl\in rK+rL$. Hence $rM\subseteq rK+rL$. Since $rK$ and $rL$ are submodules of $K$ and $L$ respectively we have $rM=rK\oplus rL$. Then $K\cap rM=K\cap(rK\oplus rL)=rK\oplus(rL\cap K)=rK$. Clearly $rK\subseteq K\cap(rK+rL)$ on the other hand if $x\in K\cap(rK\cap rL)$, then $x=rk_1+sl_1\in K$. Then $x-rk_1\in K\cap rL=0$. Then $x=rk_1$. Hence $K$ is pure.

(ii) Assume that there exists an element $x+N\in M/N$ and $0\neq r\in R$ such that $r(x+N)=rx+N=N$. Then $rx\in N$ and since $x\in M$, we have $rx\in rM\cap N=rN$ as $N$ is pure submodule of $M$. It follows that $rx=ry$ for some $y\in N$. Then $r(x-y)=0$. But $M$ is torsion free and $r\neq 0$. This gives $x-y=0$ i.e., $x=y$. Hence $x+N=N$, $x\in N$ and it follows that $M/N$ is torsion free.

(iii) Assume that $M/N$ is torsion free. Let $r\in R$. Then clearly $rM\cap N\supseteq rN$. Assume that $rM\cap N\not\subseteq rN$. Let $rm\in(rM\cap N\setminus rN)$. Consider $m+N\in M/N$. Then $r(m+N)=rm+N=N$ as $rm\in N$. Hence $m+N$ is a torsion element which is impossible or $r=0$.

(120) Suppose $L, M$ and $N$ are $R$-modules and $f : M \to N$ is an $R$-homomorphism. Define

$$\begin{aligned} f^* &: Hom_R(N,L) \to Hom_R(M,L) \\ \text{via} \quad f^*(\phi) &: m \to \phi(f(m)) \end{aligned}$$

for all $\phi \in Hom_R(N,L), m \in M$.

(i) Show that $f^*$ is a $\mathbf{Z}$-homomorphism.

(ii) If $R$ is commutative show that $f^*$ is an $R$-homomorphism

**Solution:**

$$\begin{aligned} f^*(\phi_1+\phi_2)(m) &= (\phi_1+\phi_2)(f(m)) \quad \text{where} \quad \phi_1,\phi_2 \in Hom_R(N,L), \quad m \in M \\ &= \phi_1(f(m))+\phi_2(f(m)) \\ &= f^*\phi_1(m)+f^*(\phi_2)(m) \\ &= (f^*\phi_1+f^*\phi_2)(m). \end{aligned}$$

and for any $k \in \mathbf{Z}$,

$$f^*(k\phi_1)(m) = (k\phi_1)(f(m)) = k\phi_1(f(m)) = kf^*(\phi_1)(m)$$

Hence $f^*(k\phi_1) = k(f^*\phi_1)$ for all $k \in \mathbf{Z}$.

(ii) If $R$ is commutative, then

$$f^*(r\phi_1)(m) = (r\phi_1)(f(m)) = r\phi_1(f(m)) = r(f^*\phi_1)(m) = (rf^*\phi_1)(m)$$

( We need commutativity of $R$ so that $r\phi_1$ is an $R-$module homomorphism.

$$\begin{aligned} \text{Indeed} \quad (r\phi_1)(sx) = r(\phi_1(sx) &= rs\phi_1(x) \\ &= sr\phi_1(x) \quad \text{by commutativity of } R.) \end{aligned}$$

Hence $r\ \phi_1$ is an element of $Hom_R(N,L)$ )

(121) (i) If $R$ is an integral domain show that free $R$-modules are torsion free.

(ii) If $K$ is an integral domain with 1 that is not a field exhibit a torsion free $R$-module that is not free.

**Solution: (i)** Let $R$ be an integral domain and $m$ be an element of a free module $M$. Let $B$ be a basis for $M$. Then there exist non-zero $r_1, r_2, \cdots, r_k \in R$ and $b_1, b_2, \cdots, b_k \in B$ such that

$$m = r_1 b_1 + \cdots + r_k b_k$$

If $sm = sr_1 b_1 + \cdots + sr_k b_k = 0$, then we get $sr_i = 0$, for all $i = 1, \cdots, k$ Since $b_i$ are independent. But this implies $s = 0$, since $R$ is an integral domain.

**(ii)** Let $\mathbf{Q}$ be the set of rational numbers. $\mathbf{Q}$ is a torsion free $\mathbf{Z}$-module. But $\mathbf{Q}$ is not a free module, because $\mathbf{Q}$ does not have a basis as a $\mathbf{Z}$-module. If $b_1, b_2$ are two elements of $\mathbf{Q}$ say $b_1 = \frac{m_1}{n_1}$ and $b_2 = \frac{m_2}{n_2}$. Then $n_1 m_2 b_1 - n_2 m_1 b_2 = 0$ where $n_1 m_2 \neq 0$ and $n_2 m_1 \neq 0$. Hence any subset of $\mathbf{Q}$ containing two elements are $\mathbf{Z}$-dependent. Hence a linearly independent subset of $\mathbf{Q}$ has at most one element. But it is clear that $\mathbf{Q}$ can not be generated by one element. Hence $\mathbf{Q}$ is not a free $\mathbf{Z}$-module.

(122) Let $R$ be a PID show that $M[s]$ and $sM = \{sx | x \in M\}$ are submodules of $M$.

**Solution:** $M[s] = \{x \in M | sx = 0\}$. Let $x_1, x_2 \in M[s]$, then $s(x_1 + x_2) = sx_1 + sx_2 = 0$ let $r \in R$ and $x \in M[s]$ then $s(rx) = r(sx) = 0$ hence $M[s]$ is an $R$-module.

Let $y_1, y_2 \in sM$. Then $y_1 = sx_1$ and $y_2 = sx_2$ for some $x_1, x_2 \in M$. Then

$$y_1 + y_2 = sx_1 + sx_2 = s(x_1 + x_2) \in sM.$$

Let $y \in sM$ and $r \in R$. Then $ry = rsx = s(rx) \in M$ since $M$ is an $R$-module where $y = sx$. Hence $sM$ is an $R$-module.

(123) (i) If $M$ is an $R$-module show that there is a ring homomorphism $\phi : r \to \phi_r$ from $R$ to $End(M)$ with $\phi_r(x) = rx$ all $r \in R$ and $x \in M$.

(ii) Conversely, if $M$ is an abelian group and $\phi : R \to End(M)$ is a homomorphism show that $M$ becomes an $R$-module if we define $rx = \phi_r(x)$.

**Solution:** Let $\phi : R \to End(M)$ and $r_1, r_2 \in R$.

$$\begin{aligned} \phi_{r_1+r_2}(x) = (r_1 + r_2)x &= r_1x + r_2x \\ &= \phi_{r_1}(x) + \phi_{r_2}(x) \\ &= (\phi_{r_1} + \phi_{r_2})(x) \end{aligned}$$

$\phi(r_1r_2) = \phi_{r_1r_2}$ indeed

$$\begin{aligned} \phi_{r_1r_2}(x) = r_1r_2(x) &= r_1(r_2(x)) \\ &= r_1(\phi_{r_2}(x)) \\ &= \phi_{r_1}(\phi_{r_2}(x)) \\ \text{Hence } \phi_{r_1r_2} &= \phi_{r_1}\phi_{r_2} \end{aligned}$$

Thus $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1r_2) = \phi(r_1)\phi(r_2)$ so $\phi$ is a ring homomorphism.

(ii) Suppose $\phi : R \to End(M)$ is a homomorphism.

$M$ is an $R$-module for

$$\begin{aligned} (r_1 + r_2)x &= \phi_{(r_1+r_2)}(x) = \phi_{r_1}(x) + \phi_{r_2}(x) = r_1x + r_2x. \\ (r_1r_2)x &= \phi_{r_1r_2}(x) = (\phi_{r_1}\phi_{r_2})(x) = r_1(r_2x) \\ r(x + y) &= \phi_r(x + y) = \phi_r(x) + \phi_r(y) = rx + ry \end{aligned}$$

So $M$ is an $R$-module.

(124) Show that $M = \oplus M_\alpha$ an internal direct sum of submodules if and only if each $x \in M$ has a unique expression of the form

$x = x_1 + x_2 + \cdots + x_k$ for some $k$ with $x_i \in M_{\alpha_i}$.

**Solution:** Since $M = \oplus_{\alpha \in A} M_\alpha$ every element $m \in M$ can be written of the form $m = x_1 + x_2 + \cdots + x_k \quad x_i \in M_{\alpha_i}$ for some $\alpha_i \in A$.

If

$m = x_1 + x_2 + \cdots + x_k = y_1 + y_2 + \cdots + y_l$ where without loss of generality $l \geq k$

then

$$(x_1 - y_1) + (x_2 - y_2) + \cdots + (x_k - y_k) - y_{k+1} - \cdots - y_{l-1} = y_l$$

so

$$y_l \in (M_{\alpha_1} + M_{\alpha_2} + \cdots + M_{\alpha_{l-1}}) \cap M_{\alpha_l} = 0$$

this implies that $l = k$ and similarly

$$x_i - y_i \in M_{\alpha_i} \cap (M_{\alpha_1} + \cdots + M_{\alpha_{i-1}} + M_{\alpha_{i+1}} + \cdots + M_{\alpha_k}) = 0.$$

$x_i = y_i$ so for all $i = 1, \cdots, k$. Hence $x_i = y_i$.

Conversely, since every element $x$ in $M$ can be written uniquely of the form $x = x_1 + x_2 + \cdots + x_k$, then

$$M = \sum \{M_\alpha \quad | \ \alpha \in A \quad \}$$

we need to show that sum is direct sum. For this we need to show $M_{\alpha^*} \cap \sum_{\alpha \neq \alpha^*} M_\alpha = 0$. Let

$$m_{\alpha^*} \in M_{\alpha^*} \cap \sum_{\alpha \neq \alpha^*} M_\alpha$$

$$m_{\alpha^*} = -(m_{\alpha_1} + m_{\alpha_2} + \cdots + m_{\alpha_k}) \quad \alpha_i \neq \alpha^* \quad \text{for all } i = 1, \cdots, k \ \ (\alpha_i \neq \alpha_j).$$

Since every element can be expressed uniquely, then

$$m_{\alpha^*} + m_{\alpha_1} + \cdots + m_{\alpha_k} = 0$$

This implies that $m_{\alpha^*} = 0$ hence

$$M_{\alpha^*} \cap \sum_{\alpha \neq \alpha^*} M_\alpha = 0$$

so the sum is direct sum.

(125) Suppose $R$ is a commutative ring and $M$ is an $R$-module then the $R$-module $M^* = Hom_R(M, R)$ is called the dual module of $M$. The elements of $M^*$ are commonly called $R$-linear functionals on $M$. If $M$ is free of finite rank with basis $\{x_1, x_2, \cdots, x_n\}$ show that $M^*$ is also free with basis $\{f_1, f_2, \cdots, f_n\}$ where

$$f_i(x_j) = \left\{ \begin{array}{lll} 1 & if & i = j \\ 0 & if & i \neq j \end{array} \right\}.$$

conclude that $M$ and $M^*$ are $R$-isomorphic in that case.

**Solution:** $f_1, f_2, \cdots, f_n$ generates $M^*$. Indeed if $f \in R^*$ and $f(x_i) = a_i$, $i = 1 \cdots n$, then
$a_1 f_1 + \cdots + a_n f_n = f$. To show this let,
$\varphi = a_1 f_1 + \cdots + a_n f_n - f$. Then

$$\begin{aligned} \varphi(x_i) &= a_1 f_1(x_i) + \cdots + a_i f_i(x_i) + \cdots + a_n f_n(x_i) - f(x_i) \\ &= a_i - a_i = 0 \end{aligned}$$

So for all $i = 1 \cdots n$, $\varphi(x_i) = 0$. Since $x_1 \cdots x_n$ is a basis for $M$ every element $x \in M$ can be written $b_1 x_1 + b_2 x_2 + \cdots + b_n x_n$. So for all $x \in M$, $\varphi(x) = 0$ implies $\varphi$ is the zero map. Thus $a_1 f_1 + \cdots + a_n f_n = f$ hence $f_1, f_2, \cdots, f_n$ generates $M^*$

**Claim:** $f_1, f_2, \cdots, f_n$ are linearly independent assume that $b_1 f_1 + b_2 f_2 + \cdots + b_n f_n = 0$, then

$$(b_1 f_1 + \cdots + b_k f_k)(x_i) = 0(x_i) = 0$$

but $(b_1 f_1 + \cdots + b_k f_k) x_i = b_i = 0$ for $i = 1, \cdots, k$ implies that $f_1, f_2, \cdots, f_n$ are linearly independent. Hence $\{f_1, f_2, \cdots, f_n\}$ is a basis for $M^*$. Since $M$ is free

$$\begin{tikzcd} B \arrow[r, "i"] \arrow[dr, "\varphi"'] & M \arrow[d, "f"] \\ & K \end{tikzcd}$$

there exists a unique $f$ such that the diagram is commutative.

So let $K = M^*$, $\varphi(x_i)) = f_i$ is a map then there exists a unique map $f : M \to M^*$ such that $fi = \varphi$

Claim: $f$ is an isomorphism.

$$\begin{tikzcd} B \arrow[r, "i"] \arrow[dr, "\varphi"'] & M \arrow[d, "f"] \\ & M^* \end{tikzcd}$$

$$\begin{aligned}
f(i(x_i)) &= \varphi(x_i) \\
f(x_i) &= \varphi(x_i) = f_i \\
\ker f &= \{x \in M | f(x) = 0\} \\
&= \{a_1x_1 + a_2x_2 + \ldots + a_nx_n \in M \mid f(a_1x_1 + a_2x_2 + \cdots + a_nx_n) = 0\} \\
&= \{a_1x_1 + a_2x_2 + \ldots + a_nx_n \in M \mid a_1f_1 + a_2f_2 + \cdots a_nf_n = 0\}.
\end{aligned}$$

So $a_i = 0$ since $f_1, f_2, \cdots, f_n$ is a basis therefore $x = 0$ hence $\ker f = 0$.

**Claim:** $f$ is onto let $a_1f_1 + a_2f_2 + \cdots + a_kf_k \in M^*$ then there exists $x \in M$ such that $x = a_1x_1 + \cdots + a_kx_k$, then

$$\begin{aligned} f(x) &= f(a_1x_1 + a_2x_2 + \cdots + a_kx_k) \\ &= a_1f(x_1) + \cdots + a_kf(x_k) \\ &= a_1f_1 + \cdots + a_kf_k \end{aligned}$$

therefore $f$ is an isomorphism.

Hence $M^*$ is isomorphic to $M$ and $M^*$ is a free module with basis $\{f_1, f_2, \cdots, f_n\}$.

(126) If $R$ is a commutative ring with 1 and $M$ is an $R$-module define a function.

$$\begin{aligned} \phi : M &\to M^{**} \\ x &\to \hat{x} \end{aligned}$$

$$\hat{x}f = f(x)$$

for all $f \in M^*$. Show that $\phi$ is an $R$-homomorphism. Under what circumstances is $\phi$ a monomorphism?

**Solution:** Clearly $\hat{x} \in M^{**}$. Let $x_1, x_2 \in M, \quad f \in M^*$.

$$\phi(x_1 + x_2)f = (\widehat{x_1 + x_2})f = f(x_1 + x_2)$$

since $f \in M^*$

$$f(x_1 + x_2) = f(x_1) + f(x_2) = \widehat{x}_1f + \hat{x}_2f = \phi(x_1)f + \phi(x_2)f$$

$f$ is arbitrary in $M^*$ hence

$$\phi(x_1 + x_2) = \phi(x_1) + \phi(x_2)$$

Let $r \in R$ and $x \in M$ and $f \in M^*$. Then

$$\phi(rx)f = (\widehat{rx})f = f(rx) = rf(x) = r\hat{x}f = r\phi(x)f$$

again as above this implies

$$\phi(rx) = r\phi(x).$$

$$\begin{aligned}\ker\phi = \{x\in M \mid \phi(x)=0\} \\ &= \{x\in M \mid f(x)=0 \quad \text{for all} \quad f\in M^*\} \\ &= \{x\in M \mid x\in Ker(f) \text{ for all } \ f\in M^*\} \\ &= \cap_{f\in M^*}\ker f\end{aligned}$$

if this is zero, then $\phi$ is 1-1.

(127) Use invariant factors to describe all abelian groups of orders 144, 168.

$$144 = 72.2 = 36.2.2 = 18.2.2.2$$

$$144 = 36.4 = 12.12 = 6.6.2.2 = 24.6 = 48.3 = 12.6.2$$

$\mathbf{Z}_{144}$, $\mathbf{Z}_{72}\oplus\mathbf{Z}_2$, $\mathbf{Z}_{36}\oplus\mathbf{Z}_2\oplus\mathbf{Z}_2$, $\mathbf{Z}_{18}\oplus\mathbf{Z}_2\oplus\mathbf{Z}_2\oplus\mathbf{Z}_2$
$Z_{36}\oplus\mathbf{Z}_4$, $\mathbf{Z}_{12}\oplus\mathbf{Z}_{12}$, $\mathbf{Z}_6\oplus\mathbf{Z}_6\oplus\mathbf{Z}_2\oplus\mathbf{Z}_2$, $\mathbf{Z}_{24}\oplus\mathbf{Z}_6$,
$\mathbf{Z}_{48}\oplus Z_3$, $\mathbf{Z}_{12}\oplus\mathbf{Z}_6\oplus\mathbf{Z}_2$

$$168 = 84.2 = 42.2.2$$

$\mathbf{Z}_{168}$, $\mathbf{Z}_{84}\oplus\mathbf{Z}_2$, $\mathbf{Z}_{42}\oplus\mathbf{Z}_2\oplus\mathbf{Z}_2$.

(128) Suppose $R$ is a PID and $M = R < a >$ is a cyclic $R$-module of order $r, 0\neq r\in R$. Show that if $N$ is a submodule of $M$, then $N$ is cyclic of order $s$ for some divisor $s$ of $r$. Conversely, $M$ has a cyclic submodule $N$ of order $s$ for each divisor $s$ of $r$ in $R$.

**Solution:** Let $\varphi : R \to M \quad k\to ka$. As $M$ is a unitary $R$-module, it is easy to see that $\varphi$ is an $R$-module epimorphism. Hence by isomorphism theorems $R/\ker\varphi \cong M$. Order of a is $r$ implies that $\ker\varphi = (r)$. Then we get $R/(r)\cong M$. Since $R$ is a commutative ring, there is a $1-1$ correspondence between submodules of $M$ and ideals of $R/(r)$.

Then the inverse image of $N$ in $R/(r)$ is a ideal of $R/(r)$. Since $R$ is a PID then the ideal corresponding to $N$ is generated by one element i.e., it is cyclic $R$-module this implies $N$ is cyclic $R$-module of order $s$ with $s|r$.

Conversely assume that $s|r$. Then consider the submodule $N = R < \frac{r}{s}a >$ . The module $N$ is a cyclic submodule of $M$. Exponent of $N$ is $s$. Certainly $s.\frac{r}{s}a = 0$. Any element $x$ satisfying $x\frac{r}{s}a = 0$ must be divisible by $s$ otherwise order of $a$ will not be $r$. If $x\frac{r}{s}a = 0$, then $r|x\frac{r}{s}$. Since $R$ is an integral domain $\frac{xr}{s} = rt$. Then $xr = srt$ and $r \neq 0, x = st$. So $s|x$. Thus $s$ is the order of $\frac{r}{s}a$. Hence order of $N$ is $s$.

(129) Suppose $W = R < v >$ is a cyclic submodule of $V_T$, and that $W$ has order $f(x) \in F[x]$, where $\deg f(x) = k > 0$. Show that the set $\{v, Tv, T^2v_1, \cdots, T^{k-1}v\}$ is a (vector space) basis for $W$. We call $v$ a **cyclic vector** for $W$.

**Solution:** Let $w$ be a vector in $W$. Then there exists $g(x) \in F[x]$ such that $g(x).v = w$ since $W$ is a cyclic submodule of $V_T$. $W$ has order $f(x)$, it follows that $f(x).\alpha = 0$ for all $\alpha \in W$. We may assume that $\deg[g(x)] \lneqq \deg f(x) = k$. Otherwise write $g(x) = f(x)q(x) + r(x)$ where $\deg(r(x)) < \deg f(x)$ or $r(x) = 0$. Hence $g(x)v = r(x)v$. Therefore $r(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$, we get $r(x).v = a_0I.v + a_1Tv + \cdots + a_{k-1}T^{k-1}v = w$. Hence $\{v, Tv, \cdots, T^{k-1}v\}$ spans $W$. If $b_0+b_1Tv+\cdots+b_{k-1}T^{k-1}v = 0$, then $(b_0+b_1x+\cdots+b_{k-1}x^{k-1}).v = 0$ this implies $f(x)|b_0+\cdots+b_{k-1}x^{k-1}$ which implies $b_0 = b_1 = \cdots = b_{k-1} = 0$ as $\deg(f(x)) = k$.

(130) Use elementary divisors to describe all abelian groups of order 144 and 168.

**Solution:** a) $144 = 2^4.3^2$

| | |
|---|---|
| $\mathbf{Z}_{2^4} \oplus Z_{3^2}$ | $\mathbf{Z}_{2^4} \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$ |
| $Z_{2^3} \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_{3^2}$ | $\mathbf{Z}_{2^3} \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$ |
| $\mathbf{Z}_{2^2} \oplus \mathbf{Z}_{2^2} \oplus \mathbf{Z}_{3^2}$ | $\mathbf{Z}_{2^2} \oplus \mathbf{Z}_{2^2} \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$ |
| $\mathbf{Z}_{2^2} \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_{3^2}$ | $\mathbf{Z}_{2^2} \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$ |
| $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_{3^2}$ | $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$ |

b) $168 = 2^3.3.7.$

$$\mathbf{Z}_{2^3} \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_7$$
$$\mathbf{Z}_{2^2} \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_7$$
$$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_7$$

(131) If $p$ and $q$ are distinct primes use invariant factors to describe all abelian groups of order

(i) $p^2q^2$ (ii) $p^4q$ (iii) $p^n$ $1 \leq n \leq 5$

**Solution:** (i) $p^2q^2 = pq.pq = p^2q.q = q^2p.p$

$\mathbf{Z}_{p^2q^2}$, $\mathbf{Z}_{pq} \oplus \mathbf{Z}_{pq}$, $\mathbf{Z}_{p^2q} \oplus \mathbf{Z}_q$, $\mathbf{Z}_{q^2p} \oplus \mathbf{Z}_p$

(ii) $p^4q = p^3q.p = p^2q.p^2 = p^2q.p.p = pq.p.p.p$

$\mathbf{Z}_{p^4q}$, $\mathbf{Z}_{p^3q} \oplus \mathbf{Z}_p$, $\mathbf{Z}_{p^2q} \oplus \mathbf{Z}_{p^2}$, $\mathbf{Z}_{p^2q} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$ and $\mathbf{Z}_{pq} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$

(iii) $n = 1$, $\mathbf{Z}_p$

$n = 2$ $p^2 = p.p$

$\mathbf{Z}_{p^2}$ $\mathbf{Z}_p \oplus \mathbf{Z}_p$

$n = 3$ $p^3 = p^2.p = p.p.p$

$\mathbf{Z}_{p^3}$, $\mathbf{Z}_{p^2} \oplus \mathbf{Z}_p$, $\mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$

$n = 4$ $p^4 = p^3.p = p^2.p^2 = p^2.p.p = p.p.p.p$

$\mathbf{Z}_{p^4}$, $\mathbf{Z}_{p^3} \oplus \mathbf{Z}_p$, $\mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2}$, $\mathbf{Z}_{p^2} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$, $\mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$

$n = 5$ $p^5 = p^4.p = p^3.p^2 = p^3p.p = p^2.p^2.p = p^2.p.p.p = p.p.p.p.p$

$\mathbf{Z}_{p^5}$, $\mathbf{Z}_{p^4} \oplus \mathbf{Z}_p$, $\mathbf{Z}_{p^3} \oplus \mathbf{Z}_{p^2}$, $\mathbf{Z}_{p^3} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$, $\mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2} \oplus \mathbf{Z}_p$, $\mathbf{Z}_{p^2} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$, $\mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p$

(132) If $p$ and $q$ are distinct primes use elementary divisors to describe all abelian groups of order $p^3q^2$

**Solution:** $p^3q^2 = p^2pq^2 = pppq^2 = p^2pqq = pppqq = p^3qq$

$\mathbf{Z}_{p^3} \oplus \mathbf{Z}_{q^2}, \quad \mathbf{Z}_{p^2} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_{q^2}, \quad \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_{q^2}$

$\mathbf{Z}_{p^2} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_q \oplus \mathbf{Z}_q, \quad \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_q \oplus \mathbf{Z}_q$ and $\mathbf{Z}_{p^3} \oplus \mathbf{Z}_q \oplus \mathbf{Z}_q$.

(133) Find all solutions $X \in \mathbf{Z}^3$ to the system of equations $AX = 0$ if $A$ is

i) $\begin{bmatrix} 1 & -1 & 1 \\ 1 & 0 & 2 \end{bmatrix}$

(ii) $\begin{bmatrix} 0 & 2 & -1 \\ 1 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix}$

**Solution:** $\begin{bmatrix} 1 & -1 & 1 \\ 1 & 0 & 2 \\ & & \end{bmatrix} \overset{-R_1+R_2}{\longrightarrow} \begin{bmatrix} 1 & -1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \overset{R_2+R_1}{\longrightarrow}$

$$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ & & \end{bmatrix} \begin{matrix} {\scriptstyle -2C_1+C_3} \\ -c_2 + C_3 \end{matrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ & & \end{bmatrix}$$

$$P_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \\ & \end{bmatrix} \quad P_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ & \end{bmatrix} \quad P = P_2P_1 = \begin{bmatrix} 0 & 1 \\ -1 & 1 \\ & \end{bmatrix}$$

$$Q_1 = \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad Q_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \quad Q = Q_1Q_2 = \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

Let

$Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$ and $X = QY$, then

$$PAX = PAQY = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ implies}$$

$y_1 = 0 \quad y_2 = 0$ and $y_3$ free. Hence $X = QY$ implies

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ c \end{bmatrix}$$

Solution set

$$\{(-2,-1,1)c \mid c \in \mathbf{Z} \ \}$$

$\{(-2,-1,1)\}$ is a basis for the solution set.

(ii) $$\begin{bmatrix} 0 & 2 & -1 \\ 1 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix} \xrightarrow{-2r_2+r_3} \begin{bmatrix} 0 & 2 & -1 \\ 1 & -1 & 0 \\ 0 & 2 & -1 \end{bmatrix} \xrightarrow[r_2 \leftrightarrow r_1]{-r_1+r_3}$$

$$\begin{bmatrix} 1 & -1 & 0 \\ 0 & 2 & -1 \\ 0 & 0 & 0 \end{bmatrix} \xrightarrow{C_1+C_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & 0 & 0 \end{bmatrix} \xrightarrow{C_2 \leftrightarrow C_3} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 2 \\ 0 & 0 & 0 \end{bmatrix} \xrightarrow{2C_2+C_3}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$P_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix} P_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} P_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$Q_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} Q_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} Q_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

$$P = P_3P_2P_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ -1 & -2 & 1 \end{bmatrix}$$

$$Q = Q_1Q_2Q_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix}$$

$X = QY,\quad AX = 0$ if and only if $AQY = 0$ if and only if $PAQY = 0$

But $PAQ = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

This gives $y_1 = 0\ \ y_2 = 0$ and $y_3$ is free.

$$X = QY = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$x_1 = y_3,\quad x_2 = y_3,\quad x_3 = 2y_3$ Hence $\{(1,1,2)c \mid c \in \mathbf{Z}\}$ is the integer solution set of the given system.

(134) Find all solutions to the following systems $AX = B$ of equations:

(i) $A = \begin{bmatrix} 1 & -1 & 1 \\ 1 & 0 & 2 \end{bmatrix} \quad B = \begin{bmatrix} 4 \\ 5 \end{bmatrix}$

(ii) $A = \begin{bmatrix} 0 & 2 & -1 \\ 1 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix} \quad B = \begin{bmatrix} 5 \\ 1 \\ 7 \end{bmatrix}$

**Solution:** Then $\begin{bmatrix} 1 & -1 & 1 \\ 1 & 0 & 2 \\ & & \end{bmatrix} \xrightarrow{-r_1+r_2} \begin{bmatrix} 1 & -1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{R_2+R_1}$

$$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{bmatrix} \overset{-2C_1+C_3}{-C_2+C_3} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$P_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$, $P_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $Q_1 = \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ $Q_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$

$P = P_2P_1 = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$ $Q = Q_1Q_2 = \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$

$QY = X$ and $AX = B$ implies $AQY = B$ and $PAQY = PB$. Hence

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 1 \end{bmatrix}$$

$y_1 = 5, \quad y_2 = 1, \quad y_3$ is free

$QY = X$ implies $\begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 5 \\ 1 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$

So $x_1 = 5 - 2y_3, \quad x_2 = 1 - y_3, \quad x_3 = y_3$

Solution set

$$\{(5 - 2c, 1 - c, c) \mid c \in \mathbf{Z}\ \}$$

ii) $A = \begin{bmatrix} 0 & 2 & -1 \\ 1 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix}$ $\quad B = \begin{bmatrix} 5 \\ 1 \\ 7 \end{bmatrix}$

$$\begin{bmatrix} 0 & 2 & -1 \\ 1 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix} \overset{-2r_2+r_3}{\longrightarrow} \begin{bmatrix} 0 & 2 & -1 \\ 1 & -1 & 0 \\ 0 & 2 & -1 \end{bmatrix} \overset{\substack{-R_1+R_3 \\ R_1 \leftrightarrow R_2}}{\longrightarrow}$$

$$\begin{bmatrix} 1 & -1 & 0 \\ 0 & 2 & -1 \\ 0 & 0 & 0 \end{bmatrix} \overset{C_2 \leftrightarrow C_3}{\longrightarrow} \begin{bmatrix} 1 & 0 & -1 \\ 0 & -1 & 2 \\ 0 & 0 & 0 \end{bmatrix} \underset{2C_2 + C_3}{\overset{C_1+C_3}{\rightarrow}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$P_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix}$ $P_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$ $P_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$Q_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ $Q_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ $Q_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$

$P = P_3P_2P_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ -1 & -2 & 1 \end{bmatrix}$

$Q = Q_1Q_2Q_3 == \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix}$

$PAQ = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ $AX = B$ implies $PAQY = PB$. So

$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ -1 & -2 & 1 \end{bmatrix} \begin{bmatrix} 5 \\ 1 \\ 7 \end{bmatrix} = \begin{bmatrix} 1 \\ 5 \\ 0 \end{bmatrix}$

$y_1 = 1, \quad y_2 = -5, \quad y_3$ is free.

$QY = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ implies $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ -5 \\ y_3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ $x_1 = 1 + y_3, \quad x_2 = y_3, \quad x_3 = -5 + 2y_3$

$$\{(1 + c, c, -5 + 2c) \mid c \in \mathbf{Z}\}$$

(135) If $a$ matrix $A$ over a field $F$ has a minimal polynomial $m(x)$ and characteristic polynomial $f(x)$ show that $f(x)$ is a divisor of $m(x)^k$ in $F[x]$ for some positive integer $k$.

**Solution:** Recall that $m(x)$ divides $f(x)$ and every irreducible factor of $f(x)$ appear as a product in $m(x)$. Let $m(x) = p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k}$

where $p_i$ are irreducible monic polynomials in $F[x]$. By Cayley-Hamilton Theorem $f(x) = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ where $e_i \leq t_i$. Assume that least common multiple of $t_1, t_2, \cdots t_k$ is $n$. Then $m(x)^n$ is divisible by $f(x)$ since $p_i^{t_i} \mid p_i^{e_i n}$

**Remark.** The above $n$ is not the smallest number.

(136) Determine whether or not $A = \begin{bmatrix} 3 & 0 & 2 \\ 0 & 1 & -1 \\ -4 & 0 & 3 \end{bmatrix}$ and $B = \begin{bmatrix} 5 & -8 & 4 \\ 6 & -11 & 6 \\ 6 & -12 & 7 \end{bmatrix}$ are similar over $\mathbf{Q}$.

**Solution:** $A = \begin{bmatrix} 3 & 0 & 2 \\ 0 & 1 & -1 \\ -4 & 0 & 3 \end{bmatrix} \overset{R_3+R_1}{\longrightarrow} \begin{bmatrix} -1 & 0 & 5 \\ 0 & 1 & -1 \\ -4 & 0 & 3 \end{bmatrix}$

$\overset{-4R_1+R_3}{\longrightarrow} \begin{bmatrix} -1 & 0 & 5 \\ 0 & 1 & -1 \\ 0 & 0 & -17 \end{bmatrix}$

$\overset{5C_1+C_3}{\longrightarrow} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & -17 \end{bmatrix} \overset{C_2+C_3}{\longrightarrow} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -17 \end{bmatrix}$ Smith normal form of $A$.

For $B = \begin{bmatrix} 5 & -8 & 4 \\ 6 & -11 & 6 \\ 6 & -12 & 7 \end{bmatrix} \overset{-R_2+R_1}{\longrightarrow}$

$\begin{bmatrix} -1 & 3 & -2 \\ 6 & -11 & 6 \\ 6 & -12 & 7 \end{bmatrix} \overset{6R_1+R_2}{\underset{6R_1+R_3}{\longrightarrow}} \begin{bmatrix} -1 & 3 & -2 \\ 0 & 7 & -6 \\ 0 & 6 & -5 \end{bmatrix}$

$\overset{3C_1+C_2}{\underset{-2C_1+C_3}{\longrightarrow}} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 7 & -6 \\ 0 & 6 & -5 \end{bmatrix}$

$$\xrightarrow{C_3+C_2} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & -6 \\ 0 & 1 & -5 \end{bmatrix} \xrightarrow{-R_2+R_3} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & -6 \\ 0 & 0 & 1 \end{bmatrix} \xrightarrow{6C_2+C_3}$$

$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ Smith normal form of $B$

So these matrices are not similar. One can observe that these matrices are not similar in advance because $\det A = 17$ and $\det B = -1$.

(137) Find the characteristic polynomial, invariant factors, elementary divisors , rational canonical form, and Jordan canonical form (when possible ) over $\mathbf{Q}$, for the matrix $A = \begin{bmatrix} 3 & -2 & -4 \\ 0 & 2 & 4 \\ 0 & -1 & -2 \end{bmatrix}$.

**Solution** $xI - A = \begin{bmatrix} x-3 & 2 & 4 \\ 0 & x-2 & -4 \\ 0 & 1 & x+2 \end{bmatrix} \underset{R_{2\leftrightarrow R_3}}{\xrightarrow{R_3 \leftrightarrow R_1}}$

$$\begin{bmatrix} 0 & 1 & x+2 \\ x-3 & 2 & 4 \\ 0 & x-2 & -4 \end{bmatrix}$$

$$\xrightarrow{C_2 \leftrightarrow C_1} \begin{bmatrix} 1 & 0 & x+2 \\ 2 & x-3 & 4 \\ x-2 & 0 & -4 \end{bmatrix} - \underset{-(x-2)R_1+R_3}{2R_1 + R_2}$$

$$\begin{bmatrix} 1 & 0 & x+2 \\ 0 & x-3 & -2x \\ 0 & 0 & -(x-2)(x+2)-4 \end{bmatrix}$$

$$\xrightarrow{(-x-2)C_1+C_3} \begin{bmatrix} 1 & 0 & 0 \\ 0 & x-3 & -2x \\ 0 & 0 & -x^2 \end{bmatrix} \xrightarrow{C_2+C_3}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & x-3 & -x-3 \\ 0 & 0 & -x^2 \end{bmatrix} \xrightarrow{C_3+C_2}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -6 & -x-3 \\ 0 & -x^2 & -x^2 \end{bmatrix} \xrightarrow{(\frac{-1}{6})R_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \frac{x+3}{6} \\ 0 & -x^2 & -x^2 \end{bmatrix} \xrightarrow{x^2R_2+R_3}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \frac{x+3}{+6} \\ 0 & 0 & \frac{x^2(x+3)}{6} - x^2 \end{bmatrix} \xrightarrow{\frac{-(x+3)}{6}C_2+C_3} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^2(\frac{x+3}{6} - 1) \end{bmatrix}$$

Hence the invariant factor of the matrix $A$ is $x^2(x-3) = x^3 - 3x^2 + 0x + 0$ Then $x^3 = 3x^2 + 0x + 0$ Therefore the rational form of $A$ is
$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 3 \end{bmatrix}.$$
Since minimal polynomial is not a product of distinct polynomials of degree one we have the matrix is not diagonalizable. Elementary divisors of the matrix are $x^2$ and $x-3$.

Hence the Jordan form of $A$ is $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 3 \end{bmatrix}$

(138) An $n \times n$ matrix $A$ over a field $F$ is called idempotent if $A^2 = A$

(i) What are the possible minimal polynomials for an idempotent matrix?

(ii) Show that an idempotent matrix is similar over $F$ to a diagonal matrix.

(iii) Show that idempotent $n \times n$ matrices $A$ and $B$ are similar over $F$ if and only if they have the same rank.

**Solution** (i) $A^2 = A$ implies $A^2 - A = 0$ Then $A(A - I) = 0$ Hence $A$ satisfies the polynomial $f(x) = x^2 - x$ . Therefore the minimal polynomial of $A$ divides $f(x)$ so they are $x, (x-1)$, or $x(x-1)$.

(ii) Since all possible minimal polynomials are product of different linear factors $A$ is a diagonalizable matrix.

(iii) The uniqueness of the Jordan form gives the result.

(139) An $n \times n$ matrix $A$ over a field $F$ is called nilpotent if $A^k = 0$ for some positive integer $k$

(i) If $A$ is nilpotent and $A \neq 0$ show that $A$ is not similar to a diagonal matrix.

(ii) Show that a nilpotent matrix $A$ has a jordan canonical form over $F$ and list all possible jordan forms for $A$

**Solution.** Since $A^k = 0$, the matrix $A$ satisfies the polynomial $f(x) = x^k$ so minimal polynomial of $x$ is of this form but $A \neq 0$ implies minimal polynomial is $\neq x$ hence it is not product of different linear factors. Which implies that $A$ is not diagonalizable.

**ii.** By part (i) minimal polynomial of $A$ is $x^m$ for some $m \leq k$ hence minimal polynomial is a product of linear polynomials. Then as the minimal polynomial is a product of linear factors it has a Jordan canonical form. The possibilities consists of block diagonal Jordan matrices of possibly different size $\begin{bmatrix} 0 & & & \\ 1 & 0 & & \\ & 1 & \ddots & \\ & & 1 & 0 \end{bmatrix}$

$$\begin{pmatrix}
0 & & & & & & & & & \\
1 & 0 & & & & & & & & \\
 & 1 & 0 & & & & & & & \\
 & & 1 & 0 & & & & & & \\
 & & & & \ddots & & & & & \\
 & & & & 1 & 0 & & & & \\
 & & & & & 0 & 0 & & & \\
 & & & & & & & 0 & & \\
 & & & & & & & & \ddots & \\
 & & & & & & & & & 0 \\
 & & & & & & & & & 
\end{pmatrix}$$

(140) Show that characteristic polynomial of a companion matrix $C(f)$ is $\pm f(x)$.

**Proof.** By induction on degree of $f(x)$. If $\deg(f(x)) = 2$ and $f(x) = x^2 + a_1x + a_0$, then $C(f) = \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix}$ .

Then $\det(xI - C(f)) = \det\begin{pmatrix} x & -a_0 \\ -1 & x + a_1 \end{pmatrix} = x^2 + a_1x + a_0 = f(x)$

Now assume that determinant of companion matrices of size $\leqslant n - 1$ is the corresponding polynomial. Let $C(f) = \begin{pmatrix}
0 & & & & & -a_0 \\
1 & 0 & & & & -a_1 \\
 & 1 & 0 & & & -a_2 \\
 & & & \ddots & & \vdots \\
 & & & & 0 & \\
 & & & & 1 & -a_{n-1}
\end{pmatrix}$ be an $n \times n$ matrix.

Then $\det(xI - C(f) = \det \begin{pmatrix} x & & & & & a_0 \\ -1 & x & & & & a_1 \\ & -1 & x & & & a_2 \\ & & & \ddots & & \vdots \\ & & & & x & \\ & & & & -1 & x + a_{n-1} \end{pmatrix}$

$$= x \det \begin{pmatrix} x & & & & \\ -1 & x & & & \\ & & x & & \\ & & & \ddots & \\ & & & -1 & x + a_{n-1} \end{pmatrix} + (-1)^{n+1} a_0 \det \begin{pmatrix} -1 & x & & & \\ & -1 & x & & \\ & & -1 & x & \\ & & & \ddots & x \\ & & & & -1 \end{pmatrix}$$

By induction we have $\det(xI - C(f) = x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2x + a_1) + ((-1)^{n-1}a_0(-1)^{n-1} = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = f(x)$

(141) (a) If $R$ has an identity and $A$ is an $R$-module, then there are submodules $B$ and $C$ of $A$ such that $B$ is unitary $RC = 0$ and $A = B \oplus C$

(b) Let $A_1$ be another $R$-module with $A_1 = B_1 \oplus C_1$where $B_1$ is unitary and $RC_1 = 0$. If $f : A \to A_1$ is an $R$-module homomorphism, then $f(B) \subseteq B_1$ and $f(C) \subseteq C_1$.

(c) If the map $f$ of part (b) is an epimorphism [resp. isomorphism], then so are $f|_B : B \to B_1$ and $f|_C : C \to C_1$.

**Solution.** Let $B = \{1_R a \mid \ a \in A\}$ and $C = \{a \in A \mid 1_R a = 0\}$. Now clearly $B$ is a unitary $R$-module. $C$ is a submodule, $RC = 0$ and for any $a \in A$ the element $a - 1_R a \in C$. Indeed

$$1_R(a - 1_R a) = 1_R a - 1_R a = 0.$$

Hence

$$a = 1_R a + c \quad \text{for some} \quad c \in C.$$

$a = 1_R a + a - 1_R a$ where $c = a - 1_R a$. Hence we have $A = B + C$. If $x \in B \cap C$, then $x = 1_R a \in B$ and $x \in C$. This implies that $x = 1_R a = 1_R(1_R a) = 1_R x = 0$ since $x \in C$. It follows that $B \cap C = 0$. Hence $A = B \oplus C$.

Observe that $B$ and $C$ are unique submodules of $A$ satisfying the above properties. $B$ is the largest unitary submodule of $A$ and $C$ is the largest submodule satisfying $RC = 0$.

**(b)** Let $c \in C$. Then $1_R\ c = 0$. It follows that $f(1_R c) = 1_R f(c) = 0$. Hence $f(C) = \{f(c) \mid c \in C\} \subseteq C_1$.

Let $1_R b \in B$. Then

$$f(1_R b) = 1_R f(b) \in B_1 \quad \text{as} \quad B_1 = \{1_R b \mid b \in B\}.$$

**(c)** Assume that $f$ is an epimorphism. Then for any $c_1$ in $C_1$, there exists $a \in A$ such that $f(a) = c_1$. Then by (a) there exists $b \in B$ and $c \in C$ such that $a = b + c$ where $b \in B$ and $c \in C$. Then

$$\begin{array}{lrcl} & f(a) & = & f(b) + f(c) = c_1 \quad \text{where} \quad f(b) \in B_1 \text{ and } \quad f(c) \in C_1 \quad \text{by (b).} \\ \text{Then} & f(b) & = & 0 \qquad \text{because of the direct sum.} \end{array}$$

Hence $f(c) = c_1$ and $c$ is the required element in $C$.

It follows that $f|_C$ is an epimorphism.

If $f$ is a monomorphism, then $\ker(f) = 0$. Since $f\ _{|C}$ is a map from $C$ to $C_1$ the map is a monomorphism on $C$. By above it is an epimorphism hence it becomes an isomorphism. It follows that $f_{|C}$ is an isomorphism. Similarly for $f|_B$ is an isomorphism.

(142) Suppose $R$ is a ring, $M_1$ and $M_2$ are right $R$-modules $N_1$ and $N_2$ are left $R$-modules, $f \in Hom_R(M_1, M_2)$ an $g \in Hom_R(N_1, N_2)$.

(1) Show that there exists a unique $h \in Hom_Z(M_1 \otimes_R N_1, M_2 \otimes_R N_2)$ such that $h(x \otimes y) = f(x) \otimes g(y)$ for all $x \in M_1, y \in N_1$.

Hint: Define a balanced map from $M_1 \times N_1$ to $M_2 \otimes_R N_2$ via $(x, y) \mapsto f(x) \otimes g(y)$ and see the definition of the tensor product.)

The unique homomorphism $h$ is denoted by $f \otimes g$.

(2) Suppose further that $f' \in Hom_R(M_2, M_3)$ and $g' \in Hom_R(N_2, N_3)$ show that $(f' \otimes g')(f \otimes g) = f'f \otimes g'g$.

**Solution:** Let $b : \begin{array}{c} M_1 \times N_1 \to M_2 \otimes_R N_2 \\ (x, y) \mapsto f(x) \otimes g(y) \end{array}$

$b$ is a balanced map. Indeed

$$\begin{aligned} b(x_1 + x_2, y) = f(x_1 + x_2) \otimes g(y) &= (f(x_1) + f(x_2)) \otimes g(y) \\ &= f(x_1) \otimes g(y) + f(x_2) \otimes g(y) \\ &= b(x_1, y) + b(x_2, y) \end{aligned}$$

and

$$\begin{aligned} b(x, y_1 + y_2) = f(x) \otimes g(y_1 + y_2) &= f(x) \otimes (g(y_1) + g(y_2)) \\ &= f(x) \otimes g(y_1) + f(x) \otimes g(y_2) \\ &= b(x, y_1) + b(x, y_2) \end{aligned}$$

and finally

$$\begin{aligned} b(xr, y) = f(xr) \otimes g(y) = f(x).r \otimes g(y) &= f(x) \otimes rg(y) \\ &= f(x) \otimes g(ry) \\ &= b(x, ry) \end{aligned}$$

Hence $b$ is a balanced map.

There exists a canonical balanced map $t : M_1 \times N_1 \to M_1 \otimes_R N_1$. Hence by definition of the tensor product we have a unique group homomorphism $h : M_1 \otimes_R N_1$ to $M_2 \otimes_R N_2$ such that

$$\begin{tikzcd} M_1 \times N_1 \arrow[rr, "t"] \arrow[dr, "b"'] & & M_1 \otimes N_1 \arrow[dl, "h"] \\ & M_2 \otimes N_2 & \end{tikzcd}$$

$ht = b$ i.e. $ht(m_1, n_1) = b(m_1, n_1)$ It follows that
$h(m_1 \otimes n_1) = f(m_1) \otimes g(n_1)$
$h$ is denoted by $f \otimes g$.

**(2).** The composition of $R$-module homomorphism $f'f$ is an $R$-module homomorphism from $M_1$ into $M_3$ and $g'g$ is an $R$-module homomorphism from $N_1$ into $N_3$. Then by the first part $f'f \otimes g'g$ is a unique group homomorphism from $M_1 \otimes_R N_1$ into $M_3 \otimes N_3$

$$\begin{tikzcd} M_1 \times N_1 \arrow[r, "t"] \arrow[dr] & M_1 \otimes_R N_1 \arrow[d, "f \otimes g"] \arrow[dr, "f'f \otimes g'g"] & \\ & M_2 \otimes_R N_2 \arrow[r, "f' \otimes g'"] & M_3 \otimes_R N_3 \end{tikzcd}$$

$f \otimes g, f' \otimes g'$ and $f'f \otimes g'g$ are unique group homomorphisms. Such that the corresponding diagrams are commutative. i.e., for any $m_1 \in M_1$ and $n_1 \in N_1$

$(f' \otimes g')(f \otimes g)t(m_1, n_1) = (f'f \otimes g'g)t(m_1, n_1)$. Since $t(m_1, n_1)$ generates $M_1 \otimes_R N_1$ we get $(f' \otimes g')(f \otimes g) = f'f \otimes g'g$

(143) If $R$ is a commutative ring and $M, N$ are $R$-modules then we can see $M$ and $N$ as $R$-bimodules with the natural action from right.($r.m = m.r$). Show that $M \otimes_R N$ and $N \otimes_R M$ are isomorphic as $R$-modules.

**Solution:** Define a map $f : M \times N \mapsto N \otimes_R M$, $f(m, n) = n \otimes m$.

$$\begin{tikzcd} M \times N \arrow[r, "t"] \arrow[dr, "f"'] & M \otimes_R N \arrow[d, shift left, "h"] \\ & N \otimes_R M \arrow[u, shift left, "\gamma"] \end{tikzcd}$$

Then $f$ is a balanced map. Indeed

$$f(m_1+m_2,n) = n \otimes (m_1+m_2) = n \otimes m_1 + n \otimes m_2 = f(m_1,n) + f(m_2,n)$$

$$f(m,n_1+n_2) = (n_1+n_2) \otimes m = n_1 \otimes m + n_2 \otimes m = f(m,n_1) + f(m,n_2)$$

$$f(mr,n) = n \otimes mr = n \otimes rm = nr \otimes m = f(m,nr) = f(m,rn)$$

Hence by definition there exists a unique group homomorphism $h$ such that the above diagram commutes. i.e., $ht = f$.

Observe that whenever $f$ is $R$-bilinear map $h$ and $\gamma$ are $R$-linear map

Similarly there exist a unique homomorphism $\gamma$ from $N \otimes_R M \to M \otimes_R N$ such that

$$\gamma f = t$$

By the uniqueness of $\gamma$ and $h$ we get the map $m : M \otimes N \to M \otimes N$ such that $mt = t$ and $\gamma h t = t$. We obtain

we obtain $\gamma h = id_{M \otimes_R N}$ similary $\quad h\gamma = id_{N \otimes_R M}$.

Hence $h$ and $\gamma$ are invertible $R$-homomorphisms. This shows $M \otimes_R N \cong N \otimes_R M$

(144) Suppose $A$ is a finitely generated abelian group.

i) compute $A \otimes_Z Q$

ii) Define $f : A \to A \otimes_Z Q$ by setting $f(a) = a \otimes 1$ for all $a \in A$. Show that $f$ is a homomorphism. Under what circumstances is $f$ a monomorphism?

**Solution:** Recall that every finitely generated abelian group can be written as a direct sum of its cyclic subgroups say $A_1, \cdots, A_k, A_{k+1}, \cdots, A_m$ where $A_i$, is finite for $i = 1, \cdots, k$ and $A_{k+1}, \cdots, A_m$ are infinite cyclic groups. Then as every abelian group is a $Z$-module we get

$$\begin{aligned} A \otimes_Z Q &= (A_1 \oplus + \cdots + \oplus A_k \oplus A_{k+1} \oplus \cdots \oplus A_m) \otimes Q \\ &\cong (\oplus_{i=1}^{k}(A_i \otimes_Z Q)) \oplus \oplus_{i=k+1}^{m}(A_i \otimes Q) \end{aligned}$$

For $i = 1, \cdots, k$ $A_i \otimes_Z Q = 0$ and for $i = k+1, \cdots, m$, $A_i \cong Z$. Hence

$$A \otimes_Z Q \cong \oplus_{k+1}^{m}(Z \otimes_Z Q) \cong \oplus_{k+1}^{m} Q \cong Q^{(m-k)}$$

ii) $f(a+b) = (a+b) \otimes 1 = a \otimes 1 + b \otimes 1 = f(a) + f(b)$

$f(a) = 0$ implies that $a \otimes 1 = 0$. If $a$ has finite order $q$, then $a \otimes 1 = aq \otimes \frac{1}{q} = 0$. Hence $f$ is not a monomorphism whenever $A$ has a non-trivial element of finite order. On the other hand if $A$ is a finitely generated torsion free abelian group, then $A \cong Z^n$ and $A \otimes_Z Q \cong Q^n$. let $\{x_1, \ldots x_n\}$ be a basis for $A$ over $\mathbb{Z}$. Then the map

$A \times \mathbb{Q} \to A \otimes \mathbb{Q}$ $l(\sum a_i x_i, q) = \sum a_i q$

then $f$ is a monomorphism.

(145) If $A$ is an abelian group show that

$$Z_n \otimes_Z A \cong A/nA$$

**Solution:** Define $g : \begin{array}{c} Z_n \times A \to A/nA \\ (\overline{m}, a) \to ma + nA \end{array}$

$g$ is well defined because

$(\overline{m}_1, a) = (\overline{m}_2, a)$ we get $m_1 - m_2 = kn$ for some $k \in Z$. Then

$$\begin{aligned} g(\overline{m}_1, a) = m_1 a + nA = (m_2 + kn)a + nA &= m_2 a + kna + nA \\ &= m_2 a + nA \\ &= g(\overline{m}_2, a) \end{aligned}$$

Now we show that $g$ is a balanced map.

$$\begin{aligned} g(\overline{m_1 + m_2}, a) &= (m_1 + m_2)a + nA \\ &= m_1 a + m_2 a + nA = m_1 a + nA + m_2 a + nA \end{aligned}$$

$$\begin{aligned} g(\overline{m}_1, a_1 + a_2) = m_1(a_1 + a_2) + nA &= m_1 a_1 + m_1 a_2 + nA \\ &= g(\overline{m}_1,\ a_1) + g(\overline{m}_1,\ a_2). \end{aligned}$$

$$\begin{aligned} g(\overline{m}k, a) = g(\overline{mk}, a) = &= mka + nA \\ &= g(\overline{m}, ka). \end{aligned}$$

Hence there exists a unique homomorphism $h : Z_n \otimes_Z A \to A/nA$ such that $ht = g$.

$$ht(\overline{m}, a) = h(m \otimes a) = ma + nA.$$

$h(\overline{m} \otimes a) = 0$ implies $ma + nA = nA$. This is true if and only if $ma \in nA$. But this implies that $n|m$. Hence $\overline{m} = 0$. But then $\overline{m} \otimes a = 0 \otimes a = 0$. The map $h$ is onto since for any $a + nA \in A/nA$, $h(1 \otimes a) = a + nA$.

(146) Let $V$ be a vector space of dimension 2. Let $\mathcal{B}_V = \{x_1, x_2\}$ be a basis of $V$. Let $W$ be a vector space of dimension 3 and $\mathcal{B}_W = \{y_1, y_2, y_3\}$. Let $S : V \to V$ and $T : W \to W$ be linear transformations given by

$$\begin{aligned} Sx_1 &= a_{11} x_1 + a_{21} x_2 \\ Sx_2 &= a_{12} x_1 + a_{22} x_2 \end{aligned}$$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.$$

$$\begin{aligned} Ty_1 &= b_{11}y_1 + b_{21}y_2 + b_{31}y_3 \\ Ty_2 &= b_{12}y_1 + b_{22}y_2 + b_{32}y_3 \\ Ty_3 &= b_{13}y_1 + b_{23}y_2 + b_{33}y_3 \end{aligned}$$

$$B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}.$$

Find the matrix representing $S \otimes T$ in the ordered basis

$\{x_1 \otimes y_1, x_1 \otimes y_2, x_1 \otimes y_3, x_2 \otimes y_1, x_2 \otimes y_2, x_2 \otimes y_3\}$

**Solution.**

$$\begin{aligned} (S \otimes T)(x_1 \otimes y_1) &= \\ S(x_1) \otimes T(y_1) &= (a_{11}x_1 + a_{21}x_2) \otimes (b_{11}y_1 + b_{21}y_2 + b_{31}y_3) \\ &= a_{11}(x_1 \otimes (b_{11}y_1 + b_{21}y_2 + b_{31}y_3)) + \\ &\quad a_{21}(x_2 \otimes (b_{11}y_1 + b_{21}y_2 + b_{31}y_3)) \\ &= a_{11}b_{11}(x_1 \otimes y_1) + a_{11}b_{21}(x_1 \otimes y_2) + a_{11}b_{31}(x_1 \otimes y_3) \\ &+ a_{21}b_{11}(x_2 \otimes y_1) + a_{21}b_{21}(x_2 \otimes y_2) + a_{21}b_{31}(x_2 \otimes y_3). \end{aligned}$$

For a general element

$$\begin{aligned} (S \otimes T)(x_i \otimes y_j) = S(x_i) \otimes T(y_j) &= (a_{1i}x_1 + a_{2i}x_2) \otimes (b_{1j}y_1 + b_{2j}y_2 + b_{3j}y_3) \\ &= a_{1i}b_{1j}(x_1 \otimes y_1) + a_{1i}b_{2j}(x_1 \otimes y_2) \\ &+ a_{1i}b_{3j}(x_1 \otimes y_3) + a_{2i}b_{1j}(x_2 \otimes y_1) \\ &+ a_{2i}b_{2j}(x_2 \otimes y_2) + a_{2i}b_{3j}(x_2 \otimes y_3) \end{aligned}$$

Then

$$A\otimes B = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{11}b_{13} & a_{12}b_{11} & a_{12}b_{12} & a_{12}b_{13} \\ a_{11}b_{21} & a_{11}b_{22} & a_{11}b_{23} & a_{12}b_{21} & a_{12}b_{22} & a_{12}b_{23} \\ a_{11}b_{31} & a_{11}b_{32} & a_{11}b_{33} & a_{12}b_{31} & a_{12}b_{32} & a_{12}b_{33} \\ a_{21}b_{11} & a_{21}b_{12} & a_{21}b_{13} & a_{22}b_{11} & a_{22}b_{12} & a_{22}b_{13} \\ a_{21}b_{21} & a_{21}b_{22} & a_{21}b_{23} & a_{22}b_{21} & a_{22}b_{22} & a_{22}b_{23} \\ a_{21}b_{31} & a_{21}b_{32} & a_{21}b_{33} & a_{22}b_{31} & a_{22}b_{32} & a_{22}b_{33} \end{bmatrix} = \begin{bmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{bmatrix}.$$

(147) If $F$ is a field and $K$ is an extension field of $F$ show that $M_n(K) \cong K \otimes_F M_n(F)$ as $F$-algebras.

**Solution:** Recall that $K$ is an $F$-$F$-bimodule and moreover $K$ is an $F$-algebra. $M_n(F)$ is an $F$-algebra. Hence $K \otimes_F M_n(F)$ is an $F$-algebra

$$\begin{tikzcd} K \times M_n(F) \arrow[rr, "t"] \arrow[dr, "f"'] & & K \otimes_F M_n(F) \arrow[dl, shift left, "h"] \\ & M_n(K) \cong K \otimes M_n(K) \arrow[ur, shift left, "\gamma"] & \end{tikzcd}$$

$f(k, A) = kA$, where $k \in K, A \in M_n(F)$.

$$f(k_1 + k_2, A) = (k_1 + k_2)A = k_1A + k_2A = f(k_1, A) + f(k_2, A)$$

$$f(k, A_1 + A_2) = k(A_1 + A_2) = kA_1 + kA_2 = f(k, A_1) + f(k, A_2)$$

$$f(kc, A) = (kc)A = k(cA) = f(k, cA) \quad \text{for all} \quad c \in F.$$

Hence $f$ is a balanced map. Then by definition of the tensor product there exists a unique group homomorphism $h$ such that the above diagram commutes i.e., $ht = f$, $h(k \otimes A) = kA$

$h(s(k \otimes A)) = skA = sh(k \otimes A)$, $s \in F$. So $h$ is a module homomorphism. Moreover

$$h((k\otimes A)(s\otimes B)) = h(ks\otimes AB) = ks(AB) = (kA)(sB) = h(k\otimes A)h(s\otimes B)$$

Hence $h$ is an algebra homomorphism we assumed above $M_n(K)$ is an algebra and the product on the algebra $K \otimes_F M_n(F)$ are known.

$K \otimes M_n(K) \cong M_n(K)$ isomorphism of algebras

Hence we may consider $f$ as a balanced map from $K \times M_n(F) \to K \otimes M_n(K)$. Then the exists a unique homomorphism from $\gamma : K \otimes M_n(K) \to K \otimes_F M_n(F)$ such that diagram commutes. Then $\gamma f = t, \qquad ht = f, \quad h\gamma f = f$.

Since $imf$ generates as an algebra $M_n(K)$ and the uniqueness of maps hence $\gamma$ gives the map $h\gamma$ is unique from $M_n(K) \to M_n(K)$. Since we have identity map from $M_n(K)$ to $M_n(K)$ we get $h\gamma = id$ i.e., hence $\gamma$ are bijective in particular $h$ and $\gamma$ are isomorphisms of algebras.

(148) Suppose $R$ is a ring with 1. A unitary $R$-module $P$ is called projective if given an exact sequence $M \xrightarrow{g} N \to 0$ of $R$-modules and an $R$-homomorphism $f : P \to N$, then there is an $R$-homomorphism $h : P \to M$ such that $f = gh$ i.e., the diagram

$$\begin{tikzcd} & P \arrow[dl, "h"'] \arrow[d, "f"] & \\ M \arrow[r, "g"'] & N \arrow[r] & 0 \end{tikzcd}$$

is commutative.

**(i)** Show that free modules are projective.

**(ii)** If $P = P_1 \oplus P_2$ show that $P$ is projective if and only if both $P_1$ and $P_2$ are projective.

**Solution:** Let $F$ be a free module on a set $X$. Then for any map and any $R$-module $T$ such that $f : X \to T$ there exists unique $R$-module homomorphism $h : F \to T$ such that diagram

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[dr, "f"'] & F \arrow[d, "h"] \\
& T
\end{tikzcd}$$

commutes. So assume that $F$ is free on $X$ and we have the exact sequence $M \xrightarrow{g} N \to 0$ with the $R$-module homomorphism $\alpha : F \to N$. Then

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[d, "\beta"'] & F \arrow[dl, "\exists! h"'] \arrow[d, "\alpha"] & \\
M \arrow[r, "g"] & N \arrow[r] & 0
\end{tikzcd}$$

$\alpha i$ is a map from $X$ into $N$. Since $g$ is onto we may define a map $\beta : X \to M$ such that $\alpha i(x) = g\beta(x)$. Then there exists a unique module homomorphism $h : F \to M$ (by the freeness of $F$) such that $hi = \beta$. Then $ghi = g\beta = \alpha i$. Since $i(X)$ generates $F$ as a free module we get $gh = \alpha$ and $h$ is unique. Hence $F$ is projective

ii) If $P$ is projective and $M \to N \to 0$ is an exact sequence, then

$$\begin{tikzcd}
& P \arrow[dl, "h"'] \arrow[d, "f"] & \\
M \arrow[r, "g"'] & N \arrow[r] & 0
\end{tikzcd}$$

the restriction of $h$ to $P_i$ gives a homomorphism such that the diagrams

$$\begin{tikzcd} & P_i \arrow[dl] \arrow[d, "f\,|_{P_i}"] & \\ M \arrow[r, "g"'] & N \arrow[r] & 0 \end{tikzcd}$$

commutes. Let $f' : P_i \to N$. Let $f'\pi = f$, $\pi_i : P \to P_i$ projection.

Conversely assume that $P_1$ and $P_2$ are projective and $M \to N \to 0$ be an exact sequence and $f : P = P_1 \oplus P_2 \to N$ be a module homomorphism. Then $f|_{P_i}$ gives a homomorphism of $R$-modules hence there exists $h_i$ such that

$$gh_i = f_i$$

Let $h : P \to M$ such that $h(x, y) = h_1(x) + h_2(y)$. Then $h$ is a homomorphism of $R$-modules and

$$\begin{aligned} gh(x,y) = g(h_1(x) + h_2(y)) &= gh_1(x) + gh_2(y) \\ &= f_1(x,0) + f_2(0,y) \\ &= f(x,0) + f(0,y) \\ &= f(x,y) \end{aligned}$$

(149) Show that an $R$-module $P$ is projective if and only if $P$ is a direct summand of some free module $F$.

**Solution:** Assume that $P$ is a direct summand of a free module $F = P \oplus K$ where $F$ is a free module. Let $M \xrightarrow{g} N \to 0$ be an exact sequence with a map $f : P \to N$. Then we can extend $f : F \to N$ by defining zero on $K$. Hence we have the following diagram

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[d, "h"'] & F = P \oplus K \arrow[d, "\tilde{f}"] \arrow[dl, "\gamma"'] & \\ M \arrow[r, "g"] & N \arrow[r] & O \end{tikzcd}$$

$\tilde{f} = f\pi$ where $\pi$ is the projection map from $F$ to $P$. Let $F$ be a free module on the set $X$ and $i : X \to F$, and $fi(x) \in N$ and $g$ is onto. Hence for any $x \in X$ define $h$ from $X$ into $M$ to satisfy $fi(x) = gh(x)$. Since $F$ is a free module there exists a unique homomorphism $\gamma : F \to M$ such that diagram commutes. i.e. $\gamma i = h$. Then $g\gamma i = gh = fi$. This implies $g\gamma = f$.

Let $\gamma\Big|_P = \gamma'$ restriction of $\gamma$ to $P$. Then $g\gamma'(x,0) = g\gamma(x,0) = f(x,0)$. Hence $g\gamma' = f$ and $\gamma' : P \to M$ is a module homomorphism.

Conversely assume that $P$ is a projective module. Let $X$ be a generating set of $P$ and $F$ be a free module on a set $X$. Then by definition of a free module

$$\begin{tikzcd} X \arrow[rr, "i"] \arrow[dr, "id"'] & & F \arrow[dl, "!h"] \\ & P & \end{tikzcd}$$

there exists unique module homomorphism $h : F \to P$ such that diagram commutes. i.e., $hi = id$

Since image of $h$ contains $X$ and $Im\ h$ is a submodule of $P$ we get $h$ is onto.

(**Remark:** This explanation shows that every module is an epimorphic image of a free module.)

Since $P$ is projective there exists $f : P \to F$ such that the following diagram is commutative.

$$\begin{tikzcd} & & P \arrow[dll, "f"'] \arrow[d, "1_p"] & \\ F \arrow[rr, "h"] & & P \arrow[r] & 0 \end{tikzcd}$$

Verify $F = fh(F) \oplus (1_F - fh)(F)$ and $fh(F) \cong P$.

(150) An additive abelian group $A$ is called divisible if $nA = A$ for all non-zero $n \in Z$.

i) Show that $A = Q$ is divisible

ii) Show that any homomorphic image of a divisible group is divisible. Thus for example $Q/Z$ is divisible.

iii) Show that no finitely generated abelian group $A(\neq 0)$ can be divisible.

**Solution:** (i) It is clear that $nQ \subseteq Q$. Now for any $x \in Q$ and any $0 \neq n \in Z$, $\frac{x}{n} \in Q$ hence $x \in nQ$. It follows that $Q \subseteq nQ$ and hence $Q = nQ$.

(ii) Any homomorphic image of $A$ is isomorphic to $A/K$ where $K$ is the kernel of the epimorphism. Hence it is enough to show that $A/K$ is divisible whenever $A$ is divisible. For any $a+K \in A/K$ and $n \neq 0$ there exists $b \in A$ such that $nb = a$. Hence $nb + K = a + K$. This implies $n(A/K) = A/K$ for any nonzero $n \in Z$.

Therefore $Q/Z$ is a divisible abelian group.

(iii) Recall that every finitely generated abelian group can be written as a direct sum of finite cyclic groups $A_1, \cdots, A_m$ and infinite cyclic groups $A_{m+1}, \cdots, A_n$ where $A_i \cong Z$ for $i \geq m+1$.

$$A = A_1 \oplus \cdots \oplus A_m \oplus A_{m+1} \oplus \cdots \oplus A_n.$$

Assume $\max\{|A_i| \quad i = 1, \cdots, m\} = k$. Then

$kA = kA_{m+1} \oplus \cdots \oplus kA_n$ which is a proper subgroup of $A$. Hence $A$ is not divisible as $A/kA$ is a non-trivial finite group and a divisible group can not have a subgroup of finite index grater than or equal to two.