Algebra Qualifying Exams Solutions

Jing YE

June 11, 2021

This document was created to help the author prepare for the Qualifying Examinations in Algebra. This file of solutions is likely filled with abundance of inelegance and inaccuracies. Please use with caution. The solutions written up here are to the problems in past Qualifying Examinations at Texas A&M University up to 2021 Spring. Please let me know if you find any mistakes or typos. If you have any comments or errata, please feel free to contact me via the email yej@tamu.edu.

Contents

1 Groups

Problem 1 (09J·1). Prove that a group of order 182 is solvable. (Note that $182 = 2 \cdot 7 \cdot 13$.)

Proof. Let G be a group of order 182 and n_7 be the number of Sylow 7-subgroups of G. Then, by third Sylow's theorem, we have $n_7 = 7t + 1$ for some $t \in \mathbb{N}$ and $n_7 || G|$, i.e. $(7t + 1)|182$. Thus, $(7t + 1)|26$ as $(7t + 1) \nmid 7$. So, $t = 0$.

So, G has only one Sylow 7-subgroup, say H, which is of order 7. Hence, H is solvable. By second Sylow's theorem, we see that $H \lhd G$. Note that G/H has order 26. It remains to prove that $P := G/H$ is solvable. Let n_{13} be the number of Sylow 13-subgroups of P. For the same reason, we see that $n_{13} = 13k + 1$ for some $k \in \mathbb{N}$. Then, $(13k + 1)|2$ by Sylow's theorem. So, $k = 0$ and $n_{13} = 1$. Hence, there are only one Sylow 13-subgroup of P, say Q. Then we have $Q \lhd P$. We see that P/Q is of order 2 and Q is of order 13, which are both solvable. Hence, P is also solvable. As H is solvable, we see that G is solvable. □

Problem 2 (09J·2). Let G be a finite group and N a normal subgroup of G. Let $\mathcal{C}$ be a conjugacy class of G that is contained in N. Prove that if $|G : N| = p$ is prime, then either $\mathcal{C}$ is a conjugacy class of N or $\mathcal{C}$ is a union of p distinct conjugacy classes of N.

Proof. We first claim that $g^{-1}x^N g = (g^{-1}xg)^N$ for each $x \in \mathcal{C}$ and $g \in G$, where $x^N = \{h^{-1}xh | h \in N\}$. Indeed, any $y \in g^{-1}x^N g$ is of the form $g^{-1}h^{-1}xhg$ for some $h \in N$. Since N is a normal subgroup of G, we have $g^{-1}hg = k$ for some $k \in N$. Thus, $hg = gk$. Thus, $y = k^{-1}g^{-1}xgk \in (g^{-1}xg)^N$. Conversely, take $z \in (g^{-1}xg)^N$ we have $z = h^{-1}g^{-1}xgh$ for some $h \in N$. For the same reason, $gh = ng$ for some $n \in N$. Thus, $z = g^{-1}n^{-1}xng \in g^{-1}x^N g$. So, $g^{-1}x^N g = (g^{-1}xg)^N$.

Decompose $\mathcal{C} = \mathcal{A}_1 \cup \cdots \cup \mathcal{A}_n$ as union of conjugacy classes of N. Let $X = \{\mathcal{A}_1, \cdots, \mathcal{A}_n\}$. Consider an action of G on X by $g \cdot \mathcal{A} := g^{-1}\mathcal{A}g$, where $\mathcal{A} \in X$. This action is well-defined as we have $g^{-1}x^N g = (g^{-1}xg)^N$. Moreover, G acts transitively on X as G acts transitively on $\mathcal{C}$. Indeed, let $\mathcal{A}_i = x^N$ and $\mathcal{A}_j = y^N$, then there exists $g \in G$ such that $y = g^{-1}xg$. So, $g \cdot \mathcal{A}_i = g^{-1}x^N g = (g^{-1}xg)^N = y^N = \mathcal{A}_j$. Note that $n \cdot \mathcal{A} = \mathcal{A}$ if $n \in N$. So we have an induced action of G/N on X and this action is also transitive. Thus, $n \Big| |G/N|$ by Orbits-Stabilizer theorem. Thus, $n = 1$ or p.

Thus, we conclude that $\mathcal{C}$ is a conjugacy class of N or $\mathcal{C}$ is a union of p distinct conjugacy classes of N. □

Problem 3 (09A·1). Prove that there are no simple groups of order 124.

Proof. Let G be a group of order 124. Note that $124 = 31 \cdot 2^2$. Let n_{31} be the number of Sylow 31-subgroups of G. By third Sylow's theorem, $n_{31} = 31t + 1$ for some $t \in \mathbb{N}$ and $(31t + 1)|4$. Thus, $t = 0$ and $n_{31} = 1$. So, G has only one subgroup of order 31, say H. By 2nd Sylow's theorem, $H \lhd G$. So, G is not simple. □

Problem 4 (09A·2). Let G be a group of order $1995 = 3(5)(7)(19)$. Show that G has a normal cyclic subgroup of index 3.

Proof. We first show that G has a subgroup of index 3. Let n_{19} be the number of Sylow 19-subgroups of G. By 3rd Sylow theorem, we have $n_{19} = 19t + 1$ with $t \in \mathbb{N}$ and $n_{19} \Big| |G|$. Thus, we have $(19t + 1)|3 \cdot 5 \cdot 7$, which implies that $t = 0$ and $n_{19} = 1$. Thus, G has exactly one Sylow 19-subgroup, say P, which implies that $P \lhd G$ by 2nd Sylow theorem.

Next, we want to show that there exists a normal subgroup of order 5 or 7. Consider the quotient group G/P, which is of order 105. Let n_5, n_7 be the number of Sylow 5-subgroups and Sylow 7-subgroups of G/P respectively. Then, for the same reason, we have $n_5 = 1$ or 21; $n_7 = 1, 15, 57$. If $n_5 = 1$, we are done. If $n_5 = 21$, then there are $21 \times (5 - 1) = 84$ elements of order 5. If $n_7 > 1$, then there are at least $15 \times (7 - 1) = 90$ elements of order 7, which is impossible as G/P is of order 105. Thus, there are exactly one Sylow 7-subgroup in this case. This lifts to a normal subgroup H of G, with $H/P \lhd G/P$. We may assume that H/P is of order 5, then H is also of order 5. Then take K to be a subgroup of G of order 7. (If $|H| = 7$, then we take K such that $|K| = 5$.) Since $H \cap K = 1$, we see that $|HK| = |H||K| = 35$ and HK is a subgroup of G as $H \lhd G$. Moreover, $HK \cap P = 1$ as HK cannot contain elements of order 19. Thus, $Q := HKP$ is a group of index 3.

We now show that $Q \lhd G$. Consider the action of G on $X := G/Q$ by left translation, we obtain a homomorphism

$$\rho : G \to S(X) \cong S_3,$$

where

$$\rho(g) : X \to X$$

is given by $hQ \mapsto ghQ$. We see that

$$\begin{aligned} g \in \ker\rho &\Leftrightarrow \rho(g)(hQ) = hQ \text{ for all } h \in G \\ &\Leftrightarrow ghQ = hQ \text{ for all } h \in G \\ &\Leftrightarrow h^{-1}gh \in Q \text{ for all } h \in G \\ &\Leftrightarrow g \in hQh^{-1} \text{ for all } h \in G \\ &\Leftrightarrow g \in \bigcap_{h\in G} hQh^{-1} \end{aligned}$$

Thus, $\ker\rho = \bigcap_{h\in G} hQh^{-1} \leqslant Q$ and by first isomorphism theorem, we have

$$G/\ker\rho \hookrightarrow S_3.$$

Thus, $|\ker\rho|\,\Big|\,|Q|$ and $|G/\ker\rho|\,\Big|\,6$. By $|\ker\rho|\,\Big|\,|Q|$, we see that $|Q| = |\ker\rho| \cdot t$ for some $t \in \mathbb{N}^*$. So, $|G/Q| \cdot t = |G/\ker\rho|$. Hence, we see that $3\,\Big|\,|G/\ker\rho|$ and $|G/\ker\rho|\,\Big|\,6$. So, $|G/\ker\rho| = 3$ or 6. If $|G/\ker\rho| = 6$, we see that $|\ker\rho| = |G|/6 = \frac{5\cdot7\cdot19}{2} \notin \mathbb{Z}$, contradiction. Thus, $|G/\ker\rho| = 3$, i.e. $|\ker\rho| = |Q|$, which implies that $\ker\rho = Q$. Thus, $hQh^{-1} = Q$ for all $h \in G$. Thus, $Q \lhd G$.

It remains to show that Q is cyclic. Since $P \lhd Q$, recall that $P \cong \mathbb{Z}_{19}$ is the normal Sylow 19-subgroup of G, we have $N_Q(P) = Q$. So, we can consider a well-defined homomorphism

$$\gamma : Q \to \operatorname{Aut}(P)$$

by

$$g \mapsto \gamma_g,$$

where $\gamma_g : P \to P$ is given by $\gamma_g(x) = g^{-1}xg$. We see that $\ker\gamma = \{g \in Q : g^{-1}xg = x, \forall x \in P\} = C_Q(P)$. Thus, $Q/C_Q(P) \hookrightarrow \operatorname{Aut}(P) \cong U(\mathbb{Z}_{19}) \cong \mathbb{Z}_{18}$. Let $T = Q/C_Q(P)$, then we have $|T|\,\Big|\,18$ and $|T|\,\Big|\,|Q|$, i.e. $|T|\,\Big|\,5\cdot7\cdot19$. Thus, $|T| = 1$, i.e. $Q = C_Q(P)$. Thus, $P \subseteq Z(Q)$. Thus, $|P|\,\Big|\,|Z(Q)|$ and $|Z(Q)|\,\Big|\,|Q|$. Thus, $Z(Q) = 19, 5\cdot19, 7\cdot19$ or $5\cdot7\cdot19$. So, $|Q/Z(Q)| = 35, 7, 5$ or 1. Recall that groups of order 35 is cyclic because $35 = 5 \times 7$ and $5 \nmid (7-1)$. Thus, $Q/Z(Q)$ is cyclic. So, Q is abelian. Thus, by the classification theorem of finite abelian groups, we have $Q \cong \mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{19} \cong \mathbb{Z}_{665}$, which is cyclic. □

Remark. A simple way to prove that groups of order 665 is cyclic: show that there are exact one Sylow 5-subgroup, 7-subgroup and 19-subgroup, say H, K, L. Then, show that $HKL \cong H \times K \times L \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{19}$ by normality.

Problem 5 (10J·1). The exponent $\exp(G)$ of a group G is the smallest $k \in \{1, 2, \cdots\} \cup \{\infty\}$ such that $g^k = e$ for all $g \in G$.

(a) Show that a finitely generated abelian group A with $\exp(A) < \infty$ is finite.

(b) Give an example of an infinite group of finite exponent.

(c) Give an example of a group G in which every element has finite order but $\exp(G) = \infty$.

Proof. (a) By the classification theorem of finitely generated abelian groups, we see that $A \cong$

$\mathbb{Z}^{\oplus r} \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$ with $d_1|\cdots|d_n$. Since $\exp(A) < \infty$, we see that $r = 0$ and $A \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$. So, $|A| = d_1 \cdots d_n$ is finite.

(b) Let $G = \bigoplus_{i \in \mathbb{N}^*} G_i$, where $G_i = \mathbb{Z}/2\mathbb{Z}$ for all $i \in \mathbb{N}^*$. Then, we see that G is infinite and $\exp(G) = 2$.

(c) Let $G = \bigoplus_{n \in \mathbb{N}^*} \mathbb{Z}/n\mathbb{Z}$. Let $g \in G$, then we see that all components of g are zero except finitely many elements, i.e. $g = (a_1, \cdots, a_n, 0, \cdots)$, where $a_n \in \mathbb{Z}/n\mathbb{Z}$. We see that $n!g = 0$ so g has finite order. Moreover, $\exp(g) \geqslant n$. Thus, we see that $\exp(G) = \infty$. □

Problem 6 (10J·5). Show that a group of order 80 cannot be simple.

Proof. Let G be a group of order 80, then $|G| = 80 = 2^4 \times 5$. Let n_2 be the number of Sylow 2-subgroups of G. By third Sylow's theorem, we have $n_2 = 2t + 1$ for some $t \in \mathbb{N}^*$.and $n_2\Big||G|$. So, $(2t + 1)|5$, i.e. $t = 0, 1$. If $t = 0$, then $n_2 = 1$, i.e. G has exactly one Sylow 2-subgroup, which must be normal in G by second Sylow' s theorem. If $t = 1$, then G has 5 Sylow 2-subgroups. In this case, G contains $(2^4 - 1) \times 5 = 75$ elements whose order is 2^k, where $1 \leqslant k \leqslant 4$. By first Sylow's theorem, G has a subgroup of order 5. By cardinality counting, we see that G has exact one subgroup of order 5, which is a Sylow 5-subgroup of G, say H. By second Sylow's theorem, we see that $H \lhd G$.

We see that in either cases, G has a nontrivial normal subgroup. Thus, G cannot be simple. □

Problem 7 (10J·7). Let G be a finite group and H a Sylow p-subgroup of G. Show that $N_G(N_G(H)) = N_G(H)$, where

$$N_G(K) := \{g \in G : gKg^{-1} = K\}.$$

(You may use the Sylow theorems, but you may **not** state a theorem from a text that is identical to the content of the problem).

Proof. Let $P = N_G(H)$, then we see that $H \lhd P$ and H is clearly a Sylow p-subgroup of P. Let $x \in N_G(P)$, then $x^{-1}Px = P$ and so $x^{-1}Hx \leqslant x^{-1}Px = P$. Thus, we see that $x^{-1}Hx$ is also a Sylow p-subgroup of P. By second Sylow's theorem, we see that P has exactly one Sylow p-subgroup as $H \lhd P$. It follows that $x^{-1}Hx = H$, i.e. $x \in N_G(H) = P$. So, $N_G(P) \subseteq P$. $P \subseteq N_G(P)$ is trivial, so $N_G(P) = P$. Thus, $N_G(N_G(H)) = N_G(H)$. □

Problem 8 (10A·1). Suppose G is a group with $|G| = 60$ and $|Z(G)|$ is divisible by 4. Show that G is abelian.

Proof. First, $Z(G) \lhd G$, so $G/Z(G)$ is a well-defined quotiet group. Let $Z(G) = 4t$ for some $t \in \mathbb{N}^*$. Then, $|G/Z(G)| = 15/t = 1, 3, 5$ or 15. If $|G/Z(G)| = 1, 3, 5$, then $G/Z(G)$ is cyclic. In the case that $|G/Z(G)| = 15$, let $H = G/Z(G)$. Let n_3, n_5 be the number of Sylow 3-subgroups and Sylow 5-subgroups of H respectively. By third Sylow's theorem, $n_3 = 3t + 1$ and $n_3|15$, so $n_3 = 1$. Similarly, $n_5 = 1$. Thus, H contains exact one subgroup of order 3 and exact one subgroup of order 5, denoted by K, L respectively. So, $K \lhd H$ and $L \lhd H$. Thus, $H \cong K \times L \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$ is also cyclic. Thus, $G/Z(G)$ is cyclic. Let $G/Z(G) = \langle gZ(G) \rangle$, then for any $a, b \in G$, we have $aZ(G) = g^nZ(G)$, i.e. $a = g^nx$ for some $x \in Z(G)$. Similarly, $b = g^my$ for some $y \in Z(G)$. So, $ab = (g^nx)(g^my) = g^{m+n}xy = g^{m+n}yx = (g^my)(g^nx) = ba$. Thus, G is abelian. □

Problem 9 (10A·8). Let $p < q$ be primes and G a group of order pq^n. Show that G is solvable, that is, there exists subgroups N_i such that

$$G = N_0 \rhd N_1 \rhd \cdots \rhd N_r = (e)$$

such that N_{i-1}/N_i is abelian.

Proof. Let n_q be the number of Sylow q-subgroups of G. Then, we have $n_q = qt + 1$ for some $t \in \mathbb{N}^*$ and $n_q \big| |G|$ by third Sylow's theorem. Thus, $(qt+1)|p$. So, $n_q = 1$ as $p < q$. We see that there is exact one Sylow q-subgroup of G, say H. We have $|H| = q^n$ and $H \lhd G$. Consider the quotient group G/H, we see that $|G/H| = p$. Recall that p-groups are solvable. Thus, H and G/H are solvable. So, G is solvable. □

Problem 10 (11J·1).

• Show that the set theoretic union of two subgroups cannot be a subgroup, unless one of the subgroups is contained in the other.

• Show that every vector space over GF(2) of finite dimension $d > 1$ can be written as the set theoretic union of three of its proper subspaces.

Proof. • Let G and H be two distict groups such that $G \cup H$ is a group. We may assume that there exists $h \in H - G$. For any $g \in G$, we have $gh \in G \cup H$. Thus, if $gh \in G$, then $h = g^{-1}(gh) \in G$. Contradiction. Thus, we must have $gh \in H$. So, $g = (gh)h^{-1} \in H$. Thus, $G \subseteq H$.

• Let V be a vector space over GF(2) of dimension $d > 1$. We prove it by induction on d. If $d = 2$, then, $V = \{(0,0),(1,0),(0,1),(1,1)\} = \{(0,0),(1,0)\} \cup \{(0,0),(0,1)\} \cup \{(0,0),(1,1)\}$. Suppose the statement holds for $2, 3, \cdots, d-1$. Then $V = \mathrm{GF}(2)^d = \mathrm{GF}(2)^{d-1} \times \mathrm{GF}(2)$. By induction hypothesis, we see that $\mathrm{GF}(2)^{d-1} = W_1 \cup W_2 \cup W_3$, where W_1, W_2, W_3 are 3 proper subspaces of $\mathrm{GF}(2)^{d-1}$. Thus, $V_i := W_i \times \mathrm{GF}(2)$ is a proper subspaces of V. Clearly, we have $V = V_1 \cup V_2 \cup V_3$. □

Problem 11 (11J·2). Let A be a free Abelian group of finite rank.

• (a) Let B be a subgroup of A such that $A = B + pA$ for some prime number p. Prove that B is a subgroup of finite index in A.

• (b) Let B be a subgroup of A such that $A = B + pA$ for any prime number p. Prove that $A = B$.

Proof. (a) Let $G = A/B$. We see that $A/B = (B + pA)/B = p(A/B)$, i.e. $G = pG$. Since A is a free abelian group of finite rank, suppose $x_1, \cdots, x_n$ is a $\mathbb{Z}$-basis of A. Then, there exists positive integers $d_1|d_2|\cdots|d_r$, $r \leqslant n$ such that $d_1x_1, \cdots, d_rx_r$ is a $\mathbb{Z}$-basis of B. So, $A/B \cong \mathbb{Z}^{n-r} \oplus \mathbb{Z}/(d_1) \oplus \cdots \oplus \mathbb{Z}/(d_r)$, i.e. G is a finitely generated abelian group.

Suppose that $\{y_1, \cdots, y_s\}$ is a set of generators of G. Then, $y_i \in G = pG$. So,

$$y_i = \sum_{j=1}^{s} a_{ij} y_j,$$

where $a_{ij} \in p\mathbb{Z}$. Equivalently,

$$\sum_{j=1}^{s} (\delta_{ij} - a_{ij}) y_j = 0$$

for all $i = 1, \cdots, s$, where $\delta_{ij} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$. Let $Y = (y_1, \cdots, y_s)^T$ and $M = (a_{ij})$. Then, $(I - M)Y = 0$. Let M' be the adjugate matrix of $I - M$, by Cramer's rule, we have $\det(I - M) = M'(I - A)$. Thus, we see that $\det(I - M)y_i = 0$ for all i. So, $\det(I - M) \cdot G = 0$. Thus, G is torsioned. By classification theorem of finitely generated abelian groups, we see that G must be finite, i.e. B has finite index in A.

(b) Keep the notation as in (a), we see that $pG = G$ for all prime number p. Let n be any positive integer, express $n = p_1 p_2 \cdots p_k$, then $nG = (p_1 p_2 \cdots p_k)G = (p_1 p_2 \cdots p_{k-1})(p_k G) = (p_1 p_2 \cdots p_{k-1})G = \cdots = p_1 G = G$. In particular, take $n = \det(I - M)$, then $G = nG = 0$. Hence, $A = B$. □

Problem 12 (11J·3). Prove that a group of order 616 is solvable.

Proof. Let G be a group of order 616. Note that $616 = 2^3 \times 7 \times 11$.

We first show that there exists a normal Sylow subgroup.Let n_{11} be the number of Sylow 11-subgroups of G. Then, by third Sylow's theorem, we see that $n_{11} = 11t + 1$ for some $t \in \mathbb{N}^*$ and $n_{11} | 616$, i.e. $(11t + 1) | 2^3 \times 7$. Thus, $t = 0$ or 5. If $t = 0$, then there exists exactly one subgroup of order 11, which must be normal by second Sylow's theorem. We are done. If $t = 1$, then $n_{11} = 56$, so there are $56 \times (11 - 1) = 560$ elements of order 11. Let n_7 be the number of Sylow 7-subgroups of G. Then, similarly, $n_7 = 7s + 1$ for some $s \in \mathbb{N}^*$. And $(7s + 1) | 88$, so $s = 0, 1, 3$. If $s = 0$, we are done. If $s = 1$, then $n_7 = 8$. There are $8 \times (7 - 1) = 48$ elements. Since $616 - 560 - 48 = 8$. There are exactly one Sylow 2-subgroup of G, which must be normal. We are done in this case. If $s = 3$, then there are $(3 \times 7 + 1)(7 - 1) = 22 \times 6 = 132$ elements of order 7. But, $560 + 132 > 616$, this is a contradiction.

Let P the the normal Sylow subgroup above. Since P is a p-group, P must be solvable. It remains to show that $H := G/P$ is solvable. Moreover, $|G/P| = 2^3 \times 7, 2^3 \times 11$ or 7×11.

If $|H| = 2^3 \times 7$, let m_7 be the number of Sylow 7-subgroups of H. Then, by using similar arguments as above, we see that $m_7 = 1$ or 8. If $m_7 = 1$, then H has exactly one Sylow 7-subgroup, say K_1. We have $K_1 \lhd H$ and $|H/K_1| = 2^3$, which implies that H/K_1 and K_1 are solvable. Thus H is solvable in this case. If $m_7 = 8$, then there are $8 \times (7 - 1) = 48$ elements of order 7. So, there are $56 - 48 = 8$ elements left. So, there exists exactly one Sylow 2-subgroup, say K_2. We have $K_2 \lhd H$ and $|H/K_2| = 7$, which implies that H/K_2 and K_2 are solvable. Thus H is solvable.

If $|H| = 2^3 \times 11$ or 7×11, let m_{11} be the number of Sylow 11-subgroups of H. Then, by using similar arguments as above, we see that $m_{11} = 1$. Thus, H has exactly one Sylow 11-subgroup, say L. We have $L \lhd H$ by second Sylow's theorem. We see that L and H/L are solvable as they are p-groups. Thus, H is solvable. □

Problem 13 (11A·1). Show that any group of order 455 is cyclic.

Proof. Note that $455 = 5 \times 7 \times 13$. Let G be a group of order 455. Let n_5 be the number of Sylow 5-subgroups of G. Then, by third Sylow's theorem, we see that $n_5 = 5t + 1$ for some $t \in \mathbb{N}$ and $n_5 \big| 7 \times 13$. So, $t = 0$ or 18. Thus, $n_5 = 1$ or 91. Let n_7 and n_{13} be the numbers of Sylow 7-subgroups and 13-subgroups of G respectively. Similarly, we see that $n_7 = n_{13} = 1$.

Let H be the Sylow 13-subgroup of G, then $H \lhd G$. Consider a homomorphism $\gamma : N_G(H) \to \text{Aut}(H)$ given by $g \mapsto \gamma_g$, where $\gamma_g : H \to H$ is given by $h \mapsto g^{-1}hg$. Then, $\ker \gamma = C_G(H)$. We see that $N_G(H)/C_G(H) \hookrightarrow \text{Aut}(H)$. Since $\text{Aut}(H) \cong \mathbb{Z}_{12}$. So, $|N_G(H)/C_G(H)|$ can be $1, 2, 3, 4, 6, 12$. Again, note that $H \lhd G$, we see that $N_G(H)/C_G(H) = G/C_G(H)$. Then, the only possible value of $|G/C_G(H)|$ is 1 as 455 is not divisible by $2, 3, 4, 6, 12$. It follows that $C_G(H) = G$, i.e. $\forall h \in H$, we have $hg = gh$ for all $g \in G$. Thus, $H \subseteq Z(G)$. Recall that $G/Z(G) \cong \text{Inn}(G)$, so we have $|Z(G)| \big| |G|$. Thus, we see that $|Z(G)| = 13, 13 \times 5, 13 \times 7$ or $13 \times 5 \times 7$. Correspondingly, $|G/Z(G)| = 5 \times 7, 7, 5, 1$. If $|G/Z(G)| = 1, 5, 7$, $G/Z(G)$ is cyclic. If $|G/Z(G)| = 5 \times 7$, by third Sylow's theorem, $G/Z(G)$ has exactly one Sylow 5-subgroup and one 7-subgroup. Hence $G/Z(G) \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$, which is again cyclic. Thus, we see that

$G/Z(G)$ is cyclic. So, we may assume that $G/Z(G) = \langle gZ(G)\rangle$. Thus, for any $x, y \in G$, we see that $xZ(G) = g^m Z(G)$ and $yZ(G) = g^n Z(G)$, i.e. $x = g^m a$ and $g^n b$ for some $a, b \in Z(G)$. So, $xy = (g^m a)(g^n b) = g^{m+n}ab = (g^n b)(g^m a) = yx$. Thus, G is abelian. By the classification theorem of finite abelian groups, we see that $G \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{13} \cong \mathbb{Z}_{455}$. □

Problem 14 (12J·3). *a*) Let G be a simple group of order n with a proper subgroup H of index $k > 1$,i.e. $[G : H] = k > 1$. Show that G is isomorphic to a subgroup of S_k, the symmetric group on k letters.

b) Suppose P is a Sylow p-subgroup of G where we view G as a subgroup of S_k as above. Show that if P is also a Sylow p-subgroup of S_k then the order of the normalizer of P in G, i.e. $|N_G(P)|$, divides $|N_{S_k}(P)|$.

c) Use 3*a* and 3*b* above to show that a group of order 396 cannot be simple. (Hint: Let $p = 11$ and $H = N_G(P)$.)

Proof. Let X be the set of left cosets of H in G. For any $g \in G$, we can define a map $L_g : X \to X$ by $aH \mapsto gaH$. This map is bijective as $L_{g^{-1}}L_g = L_g L_{g^{-1}} = \mathrm{id}_X$. Define a map $L : G \to S(X)$ by $g \mapsto L_g$. Then, $L_{gh}(aH) = ghaH = L_g L_h(aH)$ for all $aH \in X$, i.e. $L_{gh} = L_g L_h$ for all $g, h \in G$. Thus, L is a group homomorphism. Let $g \in \ker L$, then $L_g(aH) = aH$ for all $a \in G$, i.e. $gaH = aH$. Thus, $g \in \bigcap_{a\in G} aHa^{-1}$. Note that $\bigcap_{a\in G} aHa^{-1} \lhd G$ and G is simple, we see that $\bigcap_{a\in G} aHa^{-1} = 1$ as $|\bigcap_{a\in G} aHa^{-1}| \leqslant |H| < |G|$. It follows that $g = 1$. Thus, L is injective. Since $|X| = [G : H] = k > 1$, we have $S(X) \cong S_k$. Thus, $G \cong L(G) \leqslant S(X) \cong S_k$, i.e. G is isomorphic to a subgroup of S_k.

(*b*) By viewing G as a subgroup of S_k, we have $N_G(P) \leqslant N_{S_k}(P)$. Thus, by Langrange's theorem, we have $|N_G(P)|$ divides $|N_{S_k}(P)|$.

(*c*) Let G be a group of order 396. Note that $396 = 11 \times 36$. Let $p = 11$ and P be a Sylow 11-subgroup of G and $H = N_G(P)$. Then $k = [G : H] = [G : N_G(P)]$, which is the number of conjugate subgroups of P in G. By third Sylow's theorem, $k = 11t + 1|36$, so, we see that $k = 1$ or 12. If $k = 1$, then, $P \lhd G$, i.e. G is not simple. It suffices to deal with the case that $k = 12$. Suppose G is simple, we see that $|N_G(P)| = 33$. Note that $|S_k| = 12!$, so P is a Sylow 11-subgroup of S_k. Then by 3*a* and 3*b*, we see that $|N_{S_{12}}(P)| = 33n$ for some $n \in \mathbb{N}^*$.

Similarly, $n_{11} := [S_k : N_{S_k}(P)]$ is the number of Sylow 11-subgroups. Then, there are $n_{11} \times (11 - 1) = 10n_{11}$ elements of order 11 in S_{12}. Note that an element of order 11 must be a 11-cycle in S_12. The number of 11-cycles is $P_{11}^{12}/11 = 12!/11 = 12 \times 10!$. Thus, we see that $n_{11} := [S_{12} : N_{S_{12}}(P)] = 12 \times 10!/10 = 12 \times 9!$. So, $|N_{S_{12}}(P)| = 110$. But, $33 \nmid 110$, contradiction. □

Problem 15 (12J·6). *a*) Consider the symmetric group S_n with $n \geqslant 3$. Suppose N is a normal subgroup of S_n that contains a 3-cycle. Show N contains every 3-cycle.

b) Show that $N = A_n$ or S_n.

Proof. (*a*) Let $\tau \in S_n$ and $(abc) \in N$ be a 3-cycle, where a, b, c are distinct elements in $\{1, \cdots, n\}$. Then, we find that $\tau(abc)\tau^{-1} = (\tau(a)\tau(b)\tau(c))$ is also a 3-cycle. Let $(def) \in S_n$, where d, e, f are distinct elements in $\{1, \cdots, n\}$, be another 3-cycle, we can find a map $\tau \in S_n$ such that $\tau(a) = d$, $\tau(b) = e$,$\tau(c) = f$. Then $(def) = \tau(abc)\tau^{-1} \in N$ as N is normal in S_n. Thus, N contains every 3-cycles.

(*b*) Note that every element of A_n is a product of terms of the form $(ab)(cd)$ or $(ab)(ac)$, where a, b, c, d are distinct elements of $\{1, 2, \cdots, n\}$. Since $(ab)(cd) = (acb)(acd)$ and $(ab)(ac) = (acb)$, we see that A_n is generated by the set of all 3-cycIes. Thus, $A_n \leqslant N \leqslant S_n$. So, $[N : A_n] \leqslant [S_n : A_n] = 2$, i.e. $[N : A_n] = 1$ or 2. So, $N = A_n$ or S_n. □

Problem 16 (12A·1). Let N be a normal subgroup of a finite group G. Suppose $|N| = 5$ and that $|G|$ is odd. Prove N is contained in $Z(G)$, the center of G.

Proof. Consider a homomorphism $\varphi : N_G(N) \to \operatorname{Aut}(N)$ given by $g \mapsto \gamma_g$, where $\gamma_g : N \to N$ is an inner automorphism, i.e. $\gamma_g(n) = g^{-1}ng$ for all $n \in N$. Then, $g \in \ker\varphi$ if and only if $\gamma_g = \mathrm{id}_N$ if and only if $g^{-1}ng = n$ for all n if and only if $g \in C_G(N)$. Thus, we see that $G/C_G(N) = N_G(N)/C_G(N) \hookrightarrow \operatorname{Aut}(N)$. Since $|N| = 5$, we must have $N \cong \mathbb{Z}_5$, so $\operatorname{Aut}(N) \cong \operatorname{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$. So, $|G/C_G(N)| = 1, 2, 4$. But $|G|$ is odd, it follows that $|G/C_G(N)| = 1$, i.e. $G = C_G(N)$. Thus, for any $g \in G$, we have $gn = ng$ for all $n \in N$. This implies that $N \subseteq Z(G)$. □

Problem 17 (12A·2). Show that no group of order p^2q is simple where p and q are distinct primes. (Hint: Consider two cases $q < p$ and $p < q$. You may assume known that no group of order 12 is simple.)

Proof. Let G be a group of order p^2q where p, q are distinct primes.

Case I: $q < p$. Let n_p be the number of Sylow p-subgroups of G. Then, by third Sylow's theorem, we have $n_p = pt + 1$ for some $t \in \mathbb{N}$ and $n_p | p^2q$. Clearly, $n_p \nmid p$, we must have $n_p | q$, i.e. $(pt + 1)|q$. It follows that $t = 0$ and $pt + 1 = 1$ as $q < p$. In this case, G has exact one Sylow p-subgroups, say P. By second Sylow's theorem, we see that $P \lhd G$. Thus, G is not simple.

Case II: $p < q$. Let n_q be the number of Sylow q-subgroups of G. Then, by third Sylow's theorem, we have $n_q = qt + 1$ for some $t \in \mathbb{N}$ and $n_q | p^2q$. Clearly, $n_q \nmid q$, we must have $n_q | p^2$, i.e. $(qt + 1)|p^2$. Since $p < q$, $qt + 1 = 1$ or p^2. If $qt + 1 = 1$, then G has exact one Sylow q-subgroups, say P. By second Sylow's theorem, we see that $P \lhd G$. Thus, G is not simple. If $qt + 1 = p^2$, then $q|(p + 1)(p - 1)$. Since $p < q$, we see that $q \nmid (p - 1)$, so $q|(p + 1)$. So, $p < q \leqslant p + 1$. Thus, $q = p + 1$. If p is an odd prime, then $q = p + 1$ is even, which contradicts that q is a prime number. Thus, $p = 2$ and $q = 3$. Thus, $|G| = 12$. Since no group of order 12 is simple, we see that G is not simple in this case. □

Problem 18 (13J·1). Let G be a group of order $56 = 2^3 \cdot 7$. Show that G is not simple.

Proof. Let n_7 be the number of Sylow 7-subgroups of G. By third Sylow's theorem, $n_7 = 7t + 1$ for some $t \in \mathbb{N}$ and $n_7 \big| |G|$. So, we see that $7t + 1 | 8$. It follows that $t = 0$ or $t = 1$ and correspondingly $n_7 = 1$ or 8. If $n_7 = 1$, G has exactly one Sylow 7-subgroup, say P. By second Sylow's theorem, we have $P \lhd G$. In this case, G is not simple. If $n_7 = 8$, then there are $8 \times (7 - 1) = 48$ elements of order 7. By first Sylow's theorem, G has a subgroup of order $2^3 = 8$. By cardinality counting, $56 = 48 + 8$, we see that G has exact one subgroup of order 8, say H. By second Sylow's theorem, we have $H \lhd G$. Thus, G is not simple. □

Problem 19 (13J·2). Let G be a group of order $200 = 2^3 \cdot 5^2$, and let S_8 be the symmetric group on $\{1, \cdots, 8\}$. Show that there exists a group homomorphism $\psi : G \to S_8$ with proper non-trivial kernel. (Hint: Find a set with 8 elements on which G acts.)

Proof. Let n_5 be the number of Sylow 5-subgroups of G. By third Sylow's theorem, we have $n_5 = 5t + 1$ for some $t \in \mathbb{N}$ and $n_5 | 200$. Thus, $(5t + 1)|8$. So, $t = 1$ and $n_5 = 1$. It follows that G has exactly one Sylow 5-subgroup, say P. By second Sylow's theorem, we see that $P \lhd G$. Let $X = \{$ left cosets of P in $G\}$. Then $|X| = |G/P| = 200/25 = 8$. Consider the action of G on X by left translation, i.e. $\psi : G \to S(X) \cong S_8$, $g \mapsto \gamma_g$, where $\gamma_g : X \to X$ is given by $hP \mapsto ghP$.

We see that

$$\begin{aligned} g \in \ker\psi &\Leftrightarrow \gamma_g = \mathrm{id}_X \\ &\Leftrightarrow ghP = hP \text{ for all } h \in G \\ &\Leftrightarrow h^{-1}gh \in H, \forall h \in G \\ &\Leftrightarrow g \in \bigcap_{h\in G} hPh^{-1} = P \end{aligned}$$

Thus, $\ker\psi = P$ is non-trivial. □

Problem 20 (13A·2). Let G be a group of order $132 = 11 \cdot 12$. Show that G has a normal subgroup of order 11 or a normal subgroup of order 12. (Hint: In the case that G does not have a normal subgroup of order 11, show that for an element $x \in G$ of order not 1 or 11, the centralizer $C_G(x)$ of x has order 12.)

Proof. Let n_{11} be the number of Sylow 11-subgroups of G. By third Sylow's theorem, we see that $n_{11}|132$ and $n_{11} = 11t + 1$ for some $t \in \mathbb{N}$. Thus, $(11t + 1)|12$. So, $n_{11} = 1$ or 12. If $n_{11} = 1$, G has exactly one Sylow 11-subgroup, say H. By second Sylow's theorem, we see that $H \lhd G$. In this case, G has a normal subgroup of order 11.

If $n_{11} = 12$, then there are $12 \times (11-1) = 120$ elements of order 11. Let $x \in G$ be an element of order not 1 or 11. Let $X = \{g \in G : g \text{ is a non-identity element whose order is not } 11\}$. Let P be a Sylow 11-subgroup. Consider the conjugation action of P on X. By orbit-stablizer theorem, we see that $|\mathcal{O}(x)| \mid |P| = 11$. Thus, $|\mathcal{O}(x)| = 1$ or 11. If $|\mathcal{O}(x)| = 1$, then by $[P : C_P(x)] = |\mathcal{O}(x)|$, we see that $C_P(x) = P$, i.e. $xp = px$ for all $p \in P$. Thus, $x^{-1}Px = P$ and $x \in N_G(P)$. Consider $n_{11} = [G : N_G(P)]$, we see that $|N_G(P)| = 11$, so $P = N_G(P)$. It follows that $x \in P$, contradiction. Thus, $|\mathcal{O}(x)| = 11$. So, $\mathcal{O}(x) = X$, which implies that the elelments in X have the same order. However, X must contain an element of order 2 and an element of order 3 by first Sylow's theorem, contradition.

Thus, $n_{11} = 1$ and G must have a normal subgroup of order 11. □

Remark. Suppose $|G| = p(p + 1)$. If $p + 1$ is not a prime power, then G has a normal subgroup of order p by using the same method. In the case of $n_p = p + 1$, there are $p + 1$ elements whose order are not p. One can show that they form a group, say H. (In fact, $H = C_G(x)$ in the hint.) Then, for any $h \in H$, $g^{-1}hg$ and h have the same order, thus $g^{-1}hg \in H$. So $H \lhd G$. Then G has a normal subgroup of order p or a normal subgroup of order $p + 1$. One can also show that $p + 1 = q^n$ for some prime q, then by Sylow I, G has exactly one Sylow q-subgroup, which is the above H.

Problem 21 (13A·8). Let G be a group, and let V be a 2-dimensional vector space over a field K. Suppose we have an action of G on V, $(g, v) \to g \cdot v$, defined in such a way that for all $g \in G$, $c \in K$, and $v, w \in V$,

$$g \cdot (cv) = c(g \cdot v)$$
$$g \cdot (v + w) = g \cdot v + g \cdot w.$$

(*a*) Use the action of G to define a group homomorphism $\rho : G \to \mathrm{GL}_2(K)$, where $\mathrm{GL}_2(K)$ is the group of invertible 2×2 matrices with entries in K.

(*b*) Suppose there exist functions $\beta : G \to K$ and $\delta : G \to K^\times$ so that for all $g \in G$,

$$\rho(g) = \begin{pmatrix} 1 & \beta(g) \\ 0 & \delta(g) \end{pmatrix}$$

Show that V has a 1-dimensional subspace W that is fixed by G.

(c) Show that δ from (b) is a group homomorphism and that $\beta(g_1g_2) = \beta(g_2) + \beta(g_1)\delta(g_2)$ for all g_1, $g_2 \in G$.

(d) Fix $v = \begin{pmatrix} a \\ b \end{pmatrix} \in K^2$, with $b \neq 0$, and let $U = Kv$ be the 1-dimensional space spanned by v. Suppose further that for all $g \in G$,

$$\rho(g)(U) \subseteq U.$$

Show that there is some $c_0 \in K$ so that for all $g \in G$ we have $\beta(g) = \delta(g)c_0 - c_0$. Check that β in this form satisfies the condition in (c).

Proof. (a) Define a group homomorphism

$$\phi : G \to \mathrm{GL}(V)$$

by

$$g \mapsto \phi(g),$$

where $\phi(g) : V \to V$ is given by $\phi(g)(v) = g \cdot v$. Note that there exists a group isomorphism $\mathcal{M} : \mathrm{GL}(V) \to \mathrm{GL}_2(K)$ because $V \cong K^2$ as K-vector spaces. More precisely, $\mathcal{M}$ is the map that takes an automorphism T of V to its matrix representation $\mathcal{M}(T)$ under standard basis. Then $\rho = \mathcal{M} \circ \phi$ is a group homomorphism as desired.

(b) Let $v \in V$ be the vector having matrix representation $\mathcal{M}(v) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ under stadard basis. Then, we see that

$$\begin{pmatrix} 1 & \beta(g) \\ 0 & \delta(g) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

for all $g \in G$. Then, we see that $g \cdot v = v$ for all $g \in G$. Let W be the 1-dimensional subspace of V spanned by v, we see that W is fixed by G as $g \cdot (cv) = c(g \cdot v) = cv$ for all $c \in K$.

(c) Since ρ is a group homomorphism. Thus, $\rho(g_1g_2) = \rho(g_1)\rho(g_2)$ for all $g_1, g_2 \in G$. Thus,

$$\begin{pmatrix} 1 & \beta(g_1g_2) \\ 0 & \delta(g_1g_2) \end{pmatrix} = \begin{pmatrix} 1 & \beta(g_1) \\ 0 & \delta(g_1) \end{pmatrix} \begin{pmatrix} 1 & \beta(g_2) \\ 0 & \delta(g_2) \end{pmatrix} = \begin{pmatrix} 1 & \beta(g_2) + \beta(g_1)\delta(g_2) \\ 0 & \delta(g_1)\delta(g_2) \end{pmatrix}$$

Thus, we see that $\beta(g_1g_2) = \beta(g_2) + \beta(g_1)\delta(g_2)$ and $\delta(g_1g_2) = \delta(g_1)\delta(g_2)$ for all g_1, $g_2 \in G$. Thus, δ is a group homomorphism.

(d) Since $\rho(g)(U) \subseteq U$ for all $g \in G$, we see that $\rho(g)(v) = cv$ for some $c \in K$. Thus, v is an eigenvector of $\rho(g)$ corresponding to eigenvalue c. Since the eigenvalues of $\rho(g)$ are 1 and $\rho(g)$.

Case I: $\rho(g)(v) = v$, then

$$\begin{pmatrix} 1 & \beta(g) \\ 0 & \delta(g) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

or equivalently,

$$\begin{pmatrix} 0 & \beta(g) \\ 0 & \delta(g) - 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

So, $\begin{cases} \beta(g)b = 0 \\ (\delta(g) - 1)b = 0 \end{cases}$, which implies that $\beta(g) = 0$ and $\delta(g) = 1$ for all $g \in G$ as $b \neq 0$. We can take $c_0 = 1$ in this case, then $\beta(g) = \delta(g)c_0 - c_0$ holds for all $g \in G$.

Case II: $\rho(g)v = \delta(g)v$, then

$$\begin{pmatrix} 1 & \beta(g) \\ 0 & \delta(g) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \delta(g) \begin{pmatrix} a \\ b \end{pmatrix}$$

or equivalently,

$$\begin{pmatrix} 1-\delta(g) & \beta(g) \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

So, $(1-\delta(g))a + \beta(g)b = 0$. Take $c_0 = a/b$, we see that $\beta(g) = c_0(\delta(g)-1) = \delta(g)c_0 - c_0$ for all $g \in G$.

So, we see that there exists $c_0 \in K$ such that $\beta(g) = \delta(g)c_0 - c_0$ for all $g \in G$.

For any $g_1, g_2 \in G$, we have $\beta(g_1g_2) = \delta(g_1g_2)c_0 - c_0 = \delta(g_1)\delta(g_2)c_0 - c_0$ and $\beta(g_2) + \beta(g_1)\delta(g_2) = \delta(g_2)c_0 - c_0 + [\delta(g_1)c_0 - c_0]\delta(g_2) = \delta(g_2)c_0 - c_0 + \delta(g_1)\delta(g_2)c_0 - \delta(g_2)c_0 = \delta(g_1)\delta(g_2)c_0 - c_0$. Thus, $\beta(g_1g_2) = \beta(g_2) + \beta(g_1)\delta(g_2)$ for all $g_1, g_2 \in G$. □

Problem 22 (14J·1). A subgroup H of a group G is characteristic if $\varphi(H) = H$ for any automorphism φ of G. Show that a characteristic subgroup is normal. Suppose that $G = HK$, where H and K are characteristic subgroups of G with $H \cap K = \{e\}$. Show that $\operatorname{Aut}(G) \cong \operatorname{Aut}(H) \times \operatorname{Aut}(K)$. (Here, $\operatorname{Aut}(L)$ is the group of automorphisms of L.

Proof. Take an inner automorphism $\gamma_g \in \operatorname{Inn}(G)$, then $\gamma_g(H) = g^{-1}Hg = H$ since H is characteristic. Thus, $H \lhd G$.

Consider a map

$$\Psi : \operatorname{Aut}(G) \to \operatorname{Aut}(H) \times \operatorname{Aut}(K)$$

given by

$$\varphi \mapsto (\varphi|_H, \varphi|_K).$$

Then,

$$\Psi(\varphi\psi) = ((\varphi\psi)|_H, (\varphi\psi)|_K) = (\varphi|_H\psi|_H, \varphi|_K\psi|_K) = (\varphi|_H, \varphi|_K)(\psi|_H, \psi|_K) = \Psi(\varphi)\Psi(\psi).$$

So, Ψ is a group homomorphism.

Let $\varphi \in \ker\Psi$, then $\Psi(\varphi) = (\varphi|_H, \varphi|_H) = (\mathrm{id}_H, \mathrm{id}_K)$. So, $\varphi|_H = \mathrm{id}_H$ and $\varphi|_K = \mathrm{id}_K$. For any $g \in G$, $g = hk$ for some $h \in H$ and $k \in K$. Then, $\varphi(g) = \varphi(hk) = \varphi(h)\varphi(k) = \varphi|_H(h)\varphi|_K(k) = hk = g$. Thus, $\varphi = \mathrm{id}_G$, i.e. Ψ is injective.

To show Ψ is surjective, we first prove that for any $g \in G$, g can be written as $g = hk$ for some $h \in H, k \in K$ uniquely. Indeed, suppose $g = hk = ab$ for some $h, a \in H$ and $k, b \in K$. Then, $a^{-1}h = bk^{-1} \in H \cap K = \{e\}$. So, $a = h$ and $b = k$. Let $(\sigma, \tau) \in \operatorname{Aut}(H) \times \operatorname{Aut}(K)$, we define $\varphi : G \to G$ by $g \mapsto \sigma(h)\tau(k)$, where $g = hk$. We first show that φ is a homomorphism of G. Let $g_1, g_2 \in G$ with $g_1 = h_1k_1$, $g_2 = h_2k_2$, $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

Since $H \lhd G$, we see that $khk^{-1} = h_0$ for some $h_0 \in H$, i.e. $kh = h_0k$. Similarly, $h^{-1}kh = k_0 \in K$, i.e. $kh = hk_0$ for some $k_0 \in K$. Thus, $h_0k = hk_0$, Thus, $h_0 = h$ and $k_0 = k$. So, we see that $kh = hk$ for any $h \in H$ and $k \in K$.

Then, $g_1g_2 = h_1k_1h_2k_2 = h_1h_2k_1k_2$. So, $\varphi(g_1g_2) = \sigma(h_1h_2)\tau(k_1k_2) = \sigma(h_1)\sigma(h_2)\tau(k_1)\tau(k_2) = \sigma(h_1)\tau(k_1)\sigma(h_2)\tau(k_2) = \varphi(g_1)\varphi(g_2)$. Thus, $\varphi : G \to G$ is a homomorphism. Let $\varphi(hk) = 1$, then $\sigma(h)\tau(k) = 1$, so $\sigma(h) = \tau(k)^{-1} \in K \cap H = \{1\}$. Thus, $\sigma(h) = \tau(k) = 1$, which means that $h = k = 1$ and $hk = 1$ as $\sigma \in \operatorname{Aut}(H)$ and $\tau \in \operatorname{Aut}(K)$. Thus, we see that $\varphi : G \to G$ is injective. Let $g \in G$, then $g = hk$ for some $h \in H$, $k \in K$. Take $h_0 = \sigma^{-1}(h)$ and $k_0 = \tau^{-1}(k)$ and $g_0 = h_0k_0$, we see that $\varphi(g_0) = \sigma(h_0)\tau(k_0) = hk = g$. Thus, $\varphi : G \to G$ is surjective. So, $\varphi \in \mathrm{Aut}(G)$. Clearly, $\Psi(\varphi) = (\sigma, \tau)$ as $\varphi(h) = \sigma(h)$ and $\varphi(k) = \tau(k)$ for all $h \in H, k \in K$ by our definition.

Thus, $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. □

Problem 23 (14J·2). Show that any group of order $2014 = 2\cdot19\cdot53$ has a normal cyclic subgroup of index 2. Use this to classify all groups of order 2014.

Proof. Let G be a group of order 2014. Recall that a subgroup of index 2 must be normal, it suffices to show that G has a cyclic subgroup of index 2. Let n_{53} be the number of Sylow 53-subgroups of G. By third Sylow's theorem, $n_{53} = 53t + 1$ for some $t \in \mathbb{N}$ and $n_{53} \mid |G|$. So, $(53t + 1)|2 \cdot 19$. Thus, $t = 0$ and $n_{53} = 1$. Thus, G has only one subgroup of order 53, say P. Then, by second Sylow's theorem, we have $P \lhd G$. Let n_{19} be the number of Sylow 19-subgroups of G. Similarly, we have $n_{19} = 19s + 1$ for some $s \in \mathbb{N}$ and $n_{19} \mid |G|$, i.e. $(19s + 1)|2 \cdot 53$, which implies that $s = 0$ and $n_{19} = 1$. Thus, G has only one subgroup of order 19, say Q, which must be normal in G. Then, $K := PQ$ is a subgroup of G and $K = PQ \cong P \times Q \cong \mathbb{Z}_{19} \times \mathbb{Z}_{53} \cong \mathbb{Z}_{1007}$ as $P \lhd K$ and $Q \lhd K$.

Let $T := G/K \cong \mathbb{Z}_2$, we see that $K \cap T = \{1_G\}$ and $|KT| = |K||T|/|K \cap T| = |K||T| = |G|$. Thus, $G = KT$. Thus, G is a semidirect product of K by T. Since $K \cong \mathbb{Z}_{19} \times \mathbb{Z}_{53}$, we have $G \cong (\mathbb{Z}_{19} \times \mathbb{Z}_{53}) \rtimes_\theta \mathbb{Z}_2$, where $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_{19} \times \mathbb{Z}_{53})$ is a group homomorphism. By Problem 1, $\mathrm{Aut}(\mathbb{Z}_{19} \times \mathbb{Z}_{53}) \cong \mathrm{Aut}(\mathbb{Z}_{19}) \times \mathrm{Aut}(\mathbb{Z}_{53}) \cong \mathbb{Z}_{18} \times \mathbb{Z}_{52}$. So, we only need to determine

$$\theta : \mathbb{Z}_2 \to \mathbb{Z}_{18} \times \mathbb{Z}_{52}.$$

Since $1 \in \mathbb{Z}_2$ has order 2, we see that $2\theta(1) = \theta(2) = 0$. Thus, $\theta(1) = (0, 0), (9, 0), (0, 26)$ or $(9, 26)$. So, there are 4 groups of order 2014, $(\mathbb{Z}_{19} \times \mathbb{Z}_{53}) \rtimes_\theta \mathbb{Z}_2$, where $\theta : \mathbb{Z}_2 \to \mathbb{Z}_{18} \times \mathbb{Z}_{52}$ is given by $\theta(1) = (0, 0), (9, 0), (0, 26)$ or $(9, 26)$. □

Problem 24 (14A·3). Show that no group of order 90 is simple. (Hint: consider the normalizer of the intersection of two subgroups of order 9.)

Proof. Let G be a group of order 90. Argue by contradiction, we assume that G is simple. Then let n_3, n_5 be the number of Sylow 3-subgroups and Sylow 5-subgroups of G. Then, $n_3 = 3t + 1|10$ by thrid Sylow's theorem. Thus, $n_3 = 10$ as G is simple. Similarly, we have $n_5 = 6$. We claim that any intersection of two subgroups of order 9 cannot be trivial. Otherwise, there are $(9-1)\times 10 = 80$ elements of order 3 or 9 and $(5 - 1) \times 6 = 24$ elements of order 5. Since $80 + 24 > 90$, this is a contradiction. Thus, there exist two subgroups of order 9, say H, K such that $H \cap K$ is of order 3. Let $L = H \cap K$. Note that $[H : L] = [K : L] = 3$ is the smallest prime factor of $|H|$ and $|K|$, we see that $L \lhd H$ and $L \lhd K$. So, $H \subseteq N_G(L)$ and $K \subseteq N_G(L)$. It follows that $HK \subseteq N_G(L)$. Note that $|HK| = |H||K|/|H \cap K| = 27$. We conclude that $9 \mid |N_G(L)|$, $|N_G(L)| \geqslant 27$ and $|N_G(L)| \mid 90$. Thus, $|N_G(L)| = 45$ or 90. Thus, $N_G(L) \lhd G$. Contradiction. Hence, G is not simple.

We conclude that no groups of order 90 is simple. □

Problem 25 (14A·6). (a) Let H be a finite p-group (p prime) acting on a finite set X with fixed points $X_0 \subset X$. Show that $|X| \equiv |X_0| \pmod{p}$.

(b) Use part (a) to prove the second Sylow theorem: any two Sylow p-subgroups of a finite group G are conjugate. (Hint: let H and P be two Sylow p-subgroups, and let H act by translation on the cosets G/P.)

Proof. (a) Note that X can be written as a union of finitely many orbits. Let $\mathcal{O}_1, \cdots, \mathcal{O}_n$ be the orbits not containing any fixed points. Then, $X = X_0 \cup \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_n$. Thus, $|X| =$

$|X_0|+|\mathcal{O}_1|+\cdots+|\mathcal{O}_n|$. By orbit-stabilizer theorem, we see that $|\mathcal{O}_i| \mid |H|$. Thus, $|\mathcal{O}_i| \equiv 0 \pmod{p}$ as $\mathcal{O}_i$ does not contain fixed points. So, $|X| \equiv |X_0| \pmod{p}$.

(b) Suppose $|G| = p^n m$ with $(p, m) = 1$. Let H, P be two Sylow p-subgroups of G and $X = G/P$ be set of all left cosets. Consider the action of H on X by left translation, i.e. $h \cdot (gP) = hgP$. Note that $|X| = [G : P] = m$ and so $|X| \not\equiv 0 \pmod{p}$, we see that $|X_0| \neq 0$. Thus, there exists $gP \in X_0$, i.e. $h \cdot (gP) = gP$ for all $h \in H$, i.e. $hgP = gP$. Thus, $g^{-1}hg \in P$ for all $h \in H$. So, $g^{-1}Hg \subseteq P$. Since $|g^{-1}Hg| = |H| = |P| = p^n$, we have $g^{-1}Hg = P$.

We conclude that any two Sylow p-subgroups of a finite group G are conjugate. □

Problem 26 (15J·1). (a) Let G be a group and A and B abelian subgroups of G. Prove that $A \cap B$ is a normal subgroup of $\langle A \cup B\rangle$.

(b) Let G be a finite group which is not cyclic of prime order and in which every proper subgroup is abelian. Prove that G contains a nontrivial, proper, normal subgroup.

Proof. (a) Let $a \in A \cap B$, then for any $g \in A \cup B$ we have $g^{-1}ag = a \in A \cap B$ as A and B are abelian. Thus, $A \cap B \lhd \langle A \cup B\rangle$ as an element of $\langle A \cup B\rangle$ can be written as a product of elements in $A \cup B$.

(b) Let H be a maximal subgroup of G. Consider that $H \leqslant N_G(H)$ and the maximality of H, we see that $N_G(H) = H$ or G. If $N_G(H) = G$, then $H \lhd G$, we are done. If $H_G(H) = H$, then consider the conjugates of H. The number of conjugates of H in G is $[G : N_G(H)] = [G : H] = |G|/|H|$. If there exists two conjuagates of H, say H_1 and H_2, such that $H_1 \cap H_2 \neq \{1\}$, then $H_1 \cap H_2 \lhd \langle H_1 \cup H_2\rangle = G$ as H_1, H_2 are maximal. Thus, $H_1 \cap H_2$ is a desired normal subgroup of G. Suppose now for any two conjugates of H, say H_1, H_2, we have $H_1 \cap H_2 = \{1\}$. There are $(|H|-1)[G : H] = |G|-|G|/|H|$ non-identity elements in conjugates of H. Take a non-identity $x \in G$ such that x is not in any conjugates of H. Then there exists a maximal subgroup K containing x. Then K cannot be contained in any conjugates of H as x is not in any conjugates of H. We claim that there exists a conjugate of K, say K' and a conjugate of H, say H', such that $K' \cap H' \neq \{1\}$. Otherwise, for all conjugates of K and all conjugates of H, they have trivial intersections, which implies that G contains at least $(|G| - |G|/|H|) + (|G| - |G|/|K|) + 1$ elements. Since H, K are non-trivial, we see that $|H| \geqslant 2$, $|K| \geqslant 2$. Thus, $(|G| - |G|/|H|) + (|G| - |G|/|K|) + 1 \geqslant |G| + 1$, contradiction. Thus, $K' \cap H' \lhd \langle K' \cup H'\rangle = G$ as K' and H' are abelian. □

Problem 27 (15J·2). Let G be a group of order 45. Prove that G is abelian.

Proof. Let n_p be the number of Sylow p-subgroup of G, where p is a prime factor of $|G|$. Then by third Sylow's theorem, we see that $n_3 = 3t + 1$ for some $t \in \mathbb{N}$ and $n_3 \mid |G|$, i.e. $(3t + 1)|5$. Thus, $n_3 = 1$. Thus, G has exactly one subgroup of order 9, say H. Similarly, $n_5 = 1$ and G has exactly one subgroup of order 5, say K. Then, we have $H \lhd G$ and $K \lhd G$. We must have $H \cap K = \{1\}$ as $(|H|, |K|) = 1$. Thus, HK is a subgroup of order $|H||K|/|H \cap K| = 45$. So, $G = HK \cong H \times K$ is abelian as H and K are abelian. □

Problem 28 (15A·1). Please prove that, up to isomorphism, there are at most 4 groups of order 306 containing an element of order 9.

Proof. Let G be a group of order 306 containing an element of order 9. Note that $306 = 17 \times 2 \times 3^2$.

We claim that G has a subgroup of index 2. Let n_p be the number of Sylow p-subgroups of G, where p is a prime factor of $|G|$. Then, $n_{17} = 17t + 1$ for some $t \in \mathbb{N}$ and $n_{17} \mid |G|$ by third Sylow's theorem. So, $(17t + 1)|18$ and $n_{17} = 1$ or 18. If $n_{17} = 1$, then G has exactly one subgroup of order 17, say H_1. By second Sylow's theorem, we see that $H_1 \lhd G$. By first Sylow's theorem,

G has a subgroup of order 9, say K_1, then H_1K_1 is a subgroup of G, which is of index 2. Suppose now $n_{17} = 18$. Then, there $(17-1) \times 18 = 288$ elements of order 17 in G. Similarly, $n_3 = 1$ or 34. If $n_3 = 1$, then G has exactly one subgroup of order 9, say K_2. We must have $K_2 \lhd G$ by second Sylow's theorem. Let H_2 be a subgroup of order 17, then H_2K_2 is a subgroup of index 2. If $n_3 = 34$, by counting the cardinality of G, we see that there exists two subgroup of order 9, say H, K such that $|H \cap K| = 3$. Let $L = H \cap K$. We see that $[H : L] = [K : L] = 3$ is the smallest prime factor of $|H| = |K|$. Thus, $L \lhd H$ and $L \lhd K$. So, $H \subseteq N_G(L)$ and $K \subseteq N_G(L)$. Thus, $HK \subseteq N_G(L)$. Note that $|HK| = |H||K|/|H \cap K| = 27$, we see that $9 \mid |N_G(L)|$, $|N_G(L)| \geqslant 27$ and $|N_G(L)| \mid 306$. Thus, $|N_G(L)| = 9 \times 17$ or 306. If $|N_G(L)| = 9 \times 17$, we are done. Thus we may assume that $|N_G(L)| = 306$, i.e. $N_G(L) = G$ or $L \lhd G$. Let $P = G/L$, then $|P| = 17 \cdot 3 \cdot 2$. Let m_p be the number of Sylow p-subgroups of P, where p is a prime factor of $|P|$. We see that $m_{17} = 1$ by third Sylow's theorem. Thus, P has exactly one subgroup of order 17, say Q. Then $Q \lhd P$. By first Sylow's theorem, P has a subgroup of order 3, say T. Then, QT is a subgroup of P. Then, there is a subgroup A of G such that $A \supseteq L$ and $A/L = QT$. Thus, we see that $|A| = |L||QT| = 3 \times 17 \times 3$. So, we see that A is a subgroup of G of index 2.

Let K be a subgroup of G of index 2, then $K \lhd G$. Let $Q = G/K \cong \mathbb{Z}_2$. Then, we see that $K \cap Q = \{1\}$ as $(|K|, |Q|) = 1$. So, $|KQ| = |K||Q|/|K \cap Q| = |G|$, i.e. $G = KQ$. Thus, Q is a complement of K in G. Thus, G is a semidirect product of K by Q, i.e. $G \cong K \rtimes_\theta \mathbb{Z}_2$, where $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(K)$ is a homomorphism. Similarly, by Sylow's theorem, K has exactly one subgroup of order 17, say $\mathbb{Z}_{17}$, which is normal in K by second Sylow's theorem. Note that K contains an element of order 9, we see that $K/\mathbb{Z}_{17} \cong \mathbb{Z}_9$. Using the same argument, we have $K \cong \mathbb{Z}_{17} \rtimes_\phi \mathbb{Z}_9$, where $\phi : \mathbb{Z}_9 \to \mathrm{Aut}(\mathbb{Z}_{17}) \cong \mathbb{Z}_{16}$. Since $9\phi(1) = \phi(9) = 0$, we see that $\phi(1) = 0$. So, $K \cong \mathbb{Z}_{17} \times \mathbb{Z}_9$. Note that $\mathrm{Aut}(K) = \mathrm{Aut}(\mathbb{Z}_{17}) \times \mathrm{Aut}(\mathbb{Z}_9) \cong \mathbb{Z}_{16} \times \mathbb{Z}_6$. Thus, $\theta : \mathbb{Z}_2 \to \mathbb{Z}_{16} \times \mathbb{Z}_6$ and $\theta(1) = (0,0), (0,3), (8,0), (8,3)$.

Thus, we see that there are at most 4 groups of order 306 containing an element of order 9. □

Problem 29 (15A·2). Suppose $A \in \mathbb{Z}^{n\times n}$ has (i,j)-entry $a_{i,j}$ for all i, j, and $x = (x_1, \cdots, x_n)$. Let us then define x^A to be the vector of (formal) monomials $(x_1^{a_{1,1}} \cdots x_n^{a_{n,1}}, \cdots, x_1^{a_{1,n}} \cdots x_n^{a_{n,n}})$. One can prove (and you may assume) that $x^{AB} = (x^A)^B$ for any $B \in \mathbb{Z}^{n\times n}$.

(a) Please prove that when $\det(A) \in \{-1, 1\}$, and K is a field, the function $m_A(x) := x^A$ defines an automorphism of $(K^*)^n$.

(b) For arbitrary $A \in \mathbb{Z}^{n\times n}$ the function $m_A(x) := x^A$ happens to define an endomorphism of the subgroup $\{-1, 1\}^n$ of $(\mathbb{Q}^*)^n$. Please find, and prove, an explicit formula for the cardinality of the quotient group $\{-1, 1\}^n/\ker(m_A)$ as a function of the $(\mathbb{Z}/2\mathbb{Z})$-rank of the mod 2 reduction of A.

Proof. (a) Let $I \in \mathbb{Z}^{n\times n}$, then we see that $m_I(x) = x^I = (x_1, \cdots, x_n) = x$. Since $\det(A) \in \{-1, 1\}$, we see that A is invertible by Cramer's rule. Then, $m_{A^{-1}} m_A(x) = (x^A)^{A^{-1}} = x^{AA^{-1}} = x^I = x$ for all $x \in (K^*)^n$. Thus, $m_{A^{-1}} m_A = \mathrm{id}$. Similarly, $m_A m_{A^{-1}} = \mathrm{id}$. Thus m_A is bijective

Take $x, y \in (K^*)^n$, then $m_A(xy) = (xy)^A = ((x_1y_1)^{a_{1,1}} \cdots (x_ny_n)^{a_{n,1}}, \cdots, (x_1y_1)^{a_{1,n}} \cdots (x_ny_n)^{a_{n,n}}) = (x_1^{a_{1,1}} \cdots x_n^{a_{n,1}}, \cdots, x_1^{a_{1,n}} \cdots x_n^{a_{n,n}})(y_1^{a_{1,1}} \cdots y_n^{a_{n,1}}, \cdots, y_1^{a_{1,n}} \cdots y_n^{a_{n,n}}) = m_A(x)m_A(y)$.

Thus, m_A is an automorphism of the group $(K^*)^n$.

(b) By the theory of Smith canonicla form, there exists invertible matrices U, V such that $A = UDV$, where $D = \mathrm{diag}(d_1, \cdots, d_m, 0, \cdots, 0)$. Since U, V are invertible, we must have $\det(U), \det(V)$ are units in $\mathbb{Z}$, i.e. $\det(U) = \pm 1$ and $\det(V) = \pm 1$. Thus, by (a), m_U and m_V are automorphism of $(K^*)^n$. Note that $m_A(x) = x^A = x^{UDV} = ((x^U)^D)^V = m_V(m_D(m_U(x)))$. Thus, $x \in \ker(m_A) \Leftrightarrow m_V(m_D(m_U(x))) = 0 \Leftrightarrow m_D(m_U(x)) = 0 \Leftrightarrow m_U(x) \in \ker(m_D)$. Thus, we have a map

$$m_U|_{\ker(m_A)} : \ker(m_A) \to \ker(m_D)$$

obtained from the automorphism $m_U : (K^*)^n \to (K^*)^n$. Again, by $x \in \ker(m_A) \Leftrightarrow m_U(x) \in \ker(m_D)$, we see that $m_U|_{\ker(m_A)}$ is still an automorphism. Thus, $|\ker(m_A)| = |\ker(m_D)|$. So, it suffices to find the cardinality of $\{-1, 1\}^n / \ker(m_D)$.

Note that for any $x \in \{-1, 1\}$, $a \in \mathbb{Z}$, we have $x^a = x^{\overline{a}}$, where $\overline{a} \in \mathbb{Z}/2\mathbb{Z}$ is the mod 2 reduction of a in $\mathbb{Z}/2\mathbb{Z}$, as $(-1)^2 = 1^2 = 1$. So, to find the cardinality of $\{-1, 1\}^n / \ker(m_D)$, it suffices to replace D with its mod 2 reduction, i.e. $\overline{D} := D \mod 2$.

Suppose the rank of $\overline{D} = \operatorname{diag}(\overline{d_1}, \overline{d_2}, \cdots, \overline{d_m}, 0, \cdots, 0)$ is r, where $r \leqslant m$, then there exist $i_1, \cdots, i_r$ such that $\overline{d_{i_1}} = \cdots = \overline{d_{i_r}} = 1$ and $\overline{d_k} = 0$ if $k \neq i_1, \cdots, i_r$. So, $x^D = (x_1^{d_1}, \cdots, x_m^{d_m}, 1, \cdots, 1) = (x_1^{\overline{d_1}}, \cdots, x_m^{\overline{d_m}}, 1, \cdots, 1) = (y_1, \cdots, y_m, 1, \cdots, 1)$, where $y_{i_1} = x_{i_1}, \cdots, y_{i_r} = x_{i_r}$ and $y_k = 1$ for all $k \neq i_1, \cdots, i_r$. Thus, $x \in \ker(m_D) \Leftrightarrow x = (x_1, \cdots, x_n)$ with $x_{i_1} = \cdots = x_{i_r} = 1$. So, $|\ker(m_D)| = 2^{n-r}$.

We conclude that if the $(\mathbb{Z}/2\mathbb{Z})$-rank of the mod 2 reduction of A is r, then $|\{-1, 1\}^n / \ker(m_A)| = |\{-1, 1\}^n / \ker(m_D)| = 2^n / 2^{n-r} = 2^r$. □

Problem 30 (16J·1). Prove that every group of order 255 is cyclic.

Proof. Let G be a group of order 255. Note that $255 = 3 \cdot 5 \cdot 17$. Let n_{17} be the number of Sylow 17-subgroups of G. By third Sylow's theorem, $n_{17} = 17t + 1$ for some $t \in \mathbb{N}$ and $n_{17}|255$. Thus, $(17t + 1)|15$ and hence $t = 0$, $n_{17} = 1$. Thus, G has exactly one subgroup of order 17, say H. By 2nd Sylow's theorem, $H \lhd G$. Consider the quotient group $P := G/H$, it is of order $15 = 3 \cdot 5$. Let m_3 be the number of Sylow 3-subgroups of P. Then, by using the same argument, we see that $m_3 = 1$. Hence, P has a subgroup of order 3, say K, which is normal in P by 2nd Sylow's theorem. Similarly, P has a normal subgroup of order 5, say L. Since $(|K|, |L|) = 1$, we see that $K \cap L = \{1\}$. Thus, $|KL| = |K||L| = 15 = |P|$ and it follows that $P = KL \cong K \times L \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. Similarly, $G = HP$ and $H \cap P = \{1\}$. Thus, G is a semidirect product of H by P, i.e. $G \cong \mathbb{Z}_{17} \rtimes_\theta \mathbb{Z}_{15}$, where $\theta : \mathbb{Z}_{15} \to \operatorname{Aut}(\mathbb{Z}_{17}) \cong \mathbb{Z}_{16}$ is a homomorphism. Since $15\theta(1) = \theta(15) = 0$, we see that $\theta(1) = 0$ as $\gcd(15, 16) = 1$. This means that θ is trivial. So, $G \cong \mathbb{Z}_{17} \times \mathbb{Z}_{15} \cong \mathbb{Z}_{255}$. □

Problem 31 (16J·2). If H is a finite normal subgroup of a group G, then the index of its centralizer $C_G(H)$ is finite.

Proof. Consider a homomorphism $\gamma : N_G(H) \to \operatorname{Aut}(H)$ given by $g \mapsto \gamma_g$, where $\gamma_g : H \to H$ is given by $h \mapsto g^{-1}hg$. Then, $\ker \gamma = C_G(H)$. We see that $N_G(H)/C_G(H) \hookrightarrow \operatorname{Aut}(H)$. Since H is finite, we see that $\operatorname{Aut}(H)$ is finite. Note that $H \lhd G$, we have $N_G(H) = G$. Thus, $G/C_G(H) = N_G(H)/C_G(H)$ is finite as it is isomorphic to a subgroup of $\operatorname{Aut}(H)$. So, $[G : C_G(H)] < \infty$. □

Problem 32 (16J·3).

(a) Show that any subgroup of finite index in a finitely generated group is itself finitely generated.

(b) A group is said to be **locally finite** if every finitely generated subgroup of the group is finite. Suppose that G is a group containing a normal subgroup K such that K and G/K are both locally finite. Show that G is locally finite.

Proof. (a) Suppose G is a finitely generated group, say $G = \langle g_1, \cdots, g_r \rangle$ for some $g_1, \cdots, g_r \in G$. Let H be a subgroup of finite index, say $[G : H] = n < \infty$. Write

$$G = t_1 H \cup t_2 H \cup \cdots \cup t_n H$$

with $t_1 = 1$. Let $I = \{1, \cdots, r\}$ and $J = \{1, \cdots, n\}$. We see that $t_i \notin H$ for all $2 \leqslant i \leqslant r$. Then, for any $(i, j) \in I \times J$, we have $g_i t_j \in t_{k_{ij}} H$ for some $k_{ij} \in J$. So, $g_i t_j = t_{k_{ij}} h_{ij}$, for all $(i, j) \in I \times J$.

We claim that $\langle \{h_{ij}\}_{(i,j)\in I\times J} \rangle = H$. Let $h \in H \subseteq G$, then $h = g_{i_1} \cdots g_{i_m}$ for some $i_1, \cdots, i_m \in I$. Note that $g_{i_\ell} t_j = t_{k_{i_\ell j}} h_{i_\ell j}$, and in particular, $g_{i_m} = g_{i_m} t_1 = t_{k_{i_m 1}} h_{i_m 1}$. So, $h = g_{i_1} \cdots g_{i_m} = g_{i_1} \cdots (g_{i_m} t_1) = g_{i_1} \cdots (g_{i_{m-1}} t_{k_{i_m 1}}) h_{i_m 1} = g_{i_1} \cdots (g_{i_{m-2}} t_{k_{i_{m-1} k_{i_m 1}}}) h_{i_{m-1} k_{i_m 1}} h_{i_m 1} = \cdots = t_j \cdot h'$, where $j \in J$ and h is a product of finitely many h_{ij}. So, we see that $t_j \in H$ and hence $j = 1$, i.e. $t_j = 1$. So, $h = h' \in \langle \{h_{ij}\}_{(i,j)\in I\times J} \rangle$. Thus, $\langle \{h_{ij}\}_{(i,j)\in I\times J} \rangle = H$ and we see that H is finitely generated.

(b) Let H be a finitely generated subgroup of G, then we see that $K \cap H \lhd H$ as $K \lhd G$. So, $H/K \cap H$ is a group. Since H is finitely generated, we see that $H/K \cap H$ is also finitely generated. Indeed, if H is generated by $h_1, \cdots, h_m$, then $H/K \cap H$ is generated by $\overline{h_1}, \cdots, \overline{h_m}$. By second isomorphism theorem, we see that $HK/K \cong H/K \cap H$ is also finitely generated. Since $HK/K \leqslant G/K$ and G/K is locally finite, we see that $H/K \cap H \cong HK/K$ is a finite group. Thus, $K \cap H$ is a subgroup of H of finite index. By (a), we see that $K \cap H$ is a finitely generated subgroup of K. Since K is also locally finite, we see that $K \cap H$ is finite. Thus, $|H| = [H : K \cap H]|K \cap H|$ is finite. We conclude that G is also locally finite. □

Problem 33 (16A·1). Let G be a group of order 140. Prove that G has a cyclic normal subgroup of order 35.

Proof. Note that $140 = 2^2 \cdot 7 \cdot 5$. Let n_p be the number of Sylow p-subgroups of G, where p is a prime factor of $|G|$. Then, by thrid Sylos's theorem, $n_7 = 7t + 1$ for some $t \in \mathbb{N}$ and $n_7 \mid |G|$. Thus, $(7t + 1)|2^2 \cdot 5$. Thus, $t = 0$ and $n_7 = 1$. So, G has exactly one subgroup of order 7, say H. Then, $H \lhd G$ by the 2nd Sylow's theorem. Similarly, $n_5 = 1$ and G has exactly one subgroup of order 5, say K. Then, $K \lhd G$ by 2nd Sylow's theorem. Let $L = HK$. Since $\gcd(|H|, |K|) = 1$, we have $H \cap K = \{1\}$ and $|L| = |HK| = |H||K|/|H \cap K| = 5 \times 7 = 35$. So, $L = HK \cong H \times K \cong \mathbb{Z}_7 \times \mathbb{Z}_5 \cong \mathbb{Z}_{35}$.

It remains to show that $L \lhd G$. Let M be a subgroup of order 35. Then, by first Sylow's theorem, M has a subgroup of order 5, which is a subgroup of G. We have seen that G has exactly one subgroup K of order 5. Thus, $K \subseteq M$. Similarly, $H \subseteq M$. So, we see that $M = HK = L$. Thus, G has exactly one subgroup of order 35. So, for all $g \in G$, $g^{-1}Lg = L$ as $|g^{-1}Lg| = |L| = 35$. Thus, $L \lhd G$. □

Problem 34 (16A·6). (a) Let F_m be a free group of rank $m \geqslant 2$. Show that a nontrivial normal subgroup of F_m cannot be cyclic.

(b) Show that a solvable group cannot contain F_2 as a subgroup.

(Hint: A subgroup of a free group is free. You may also use part (a).)

Proof. (a) Let N be a nontrivial normal subgroup of F_m. Then, $N \cong F_n$ with $1 \leqslant n < m$. If N is cyclic, then $n = 1$. In this case $N = \langle x \rangle$. Let y be a generator which is independent on x. Then, $y^{-1}xy = x^k$ for some $k \geqslant 1$. So, $xy = yx^k$. Contradiction. Thus, $n > 1$, i.e. N cannot be cyclic.

(b) Let G be a solvable group containing F_2 as a subgroup. Then, F_2 is solvable. Let N be a proper normal subgroup of F_2. By (a), we see that $N = \{1\}$. In particular, the derived subgroup $F_2' = \{1\}$. Thus, F_2 is abelian. Contradiction. □

Problem 35 (17J·1). Prove that the quotient of S_4 by the Klein's group $\{e, (12)(34), (13)(24), (14)(23)\}$ is isomorphic to S_3.

Proof. Note that $S_3 = \{e, (123), (132), (12), (13), (23)\}$ can be regarded as a subgroup of S_4. Since $S_3 \cap V = \{e\}$, where V is the Klein's group, we see that $|S_3V| = |S_3||V|/|S_3 \cap V| = 24 = |S_4|$. Thus, $S_4 = S_3V$. So, $S_4/V = S_3V/V \cong S_3/S_3 \cap V \cong S_3$. □

Problem 36 (17J·2). How many Sylow 2-subgroups and Sylow 5-subgroups there are in a non-commutative group of order 20?

Proof. Let G be a non-commutative group of order 20. Let n_p be the number of Sylow p-subgroups of G, where p is a prime factor of $|G|$. Then, by third Sylow's theorem, $n_5 = 5t + 1$ for some $t \in \mathbb{N}$ and $n_5 \mid |G|$. Thus, $(5t + 1)|4$. So, $t = 0$ and $n_5 = 1$. Thus, G has exactly one Sylow 5-subgroup, say H. By second Sylow's theorem, we see that $H \lhd G$.

Similarly, $n_2 = 1$ or 5. If $n_2 = 1$, then G has exactly one Sylow 2-subgroup, say K. By second Sylow's theorem, we see that $K \lhd G$. Note that $\gcd(|H|, |K|) = 1$, we have $H \cap K = \{1\}$. Then, $|HK| = |H||K|/|H \cap K| = 20 = |G|$. So, $G = HK$. Thus, $G = HK \cong H \times K$ is abelian. Contradiction. Then, $n_2 = 5$. □

Problem 37 (17J·3). Consider the group $T = \{z \in \mathbb{C} : |z| = 1\}$ with respect to multiplication. Prove that every finite subgroup of T is cyclic.

Proof. Let G be a finite subgroup of T and $n = |G|$. Then, for any $z \in G$, we have $z^n = 1$. Note that $x^n - 1$ has exactly n roots over $\mathbb{C}$ and if z is a root, then $|z|^n = |z^n| = 1$, i.e. $|z| = 1$. Thus, $G = \{z \in \mathbb{C} : z^n = 1\} = \langle e^{2\pi i/n} \rangle$ is cyclic. □

Problem 38 (17A·1). Let p and q be distinct prime numbers, and let G be a group of order p^2q. Prove that G has a normal Sylow subgroup. (Note: the cases $p > q$ and $p < q$ should be treated separately.)

Proof. Case I: $q < p$. Let n_p be the number of Sylow p-subgroups of G. Then, by third Sylow's theorem, we have $n_p = pt + 1$ for some $t \in \mathbb{N}$ and $n_p|p^2q$. Clearly, $n_p \nmid p$, we must have $n_p|q$, i.e. $(pt + 1)|q$. It follows that $t = 0$ and $pt + 1 = 1$ as $q < p$. In this case, G has exact one Sylow p-subgroups, say P. By second Sylow's theorem, we see that $P \lhd G$.

Case II: $p < q$. Let n_q be the number of Sylow q-subgroups of G. Then, by third Sylow's theorem, we have $n_q = qt + 1$ for some $t \in \mathbb{N}$ and $n_q|p^2q$. Clearly, $n_q \nmid q$, we must have $n_q|p^2$, i.e. $(qt + 1)|p^2$. Since $p < q$, $qt + 1 = 1$ or p^2. If $qt + 1 = 1$, then G has exact one Sylow q-subgroups, say P. By second Sylow's theorem, we see that $P \lhd G$.

If $qt + 1 = p^2$, then $q|(p + 1)(p - 1)$. Since $p < q$, we see that $q \nmid (p - 1)$, so $q|(p + 1)$. So, $p < q \leqslant p + 1$. Thus, $q = p + 1$. If p is an odd prime, then $q = p + 1$ is even, which contradicts that q is a prime number. Thus, $p = 2$ and $q = 3$. Thus, $|G| = 12$. In this case, we see that $n_3 = 4$ and there are $(3 - 1) \times 4 = 8$ elements of order 3. By first Sylow's theorem, G has one Sylow 2-subgroup, which is of order 4. By counting the cardinality of G, we see that G has exactly one Sylow 2-subgroup, say Q. By second Sylow's theorem, we see that $Q \lhd G$. □

Problem 39 (17A·2). Let G be a group of order $375 = 3 \cdot 5^3$. Let H be a Sylow 3-subgroup, let K be a Sylow 5-subgroup, and suppose that K is cyclic.

(a) According to the Sylow theorems, what are the possible numbers of conjugates of H? And of K?

(b) Let $X = \{g \in K | K = \langle g \rangle\}$. Show that H acts on X by conjugation. What are the possible sizes of orbits of this action? What is the size of the set of generators of K?

(c) Prove that G must be cyclic.

Proof. (a) Let n_3 be the numbers of conjugates of H. By third Sylow's theorem, $n_3 = 3t + 1$ for some $t \in \mathbb{N}$ and $n_3 \mid |G|$. Thus, $(3t + 1) \mid 5^3$. So, $t = 0$ or 8 and $n_3 = 1$ or 25.

Let n_5 be the numbers of conjugates of K. By third Sylow's theorem, $n_5 = 5t + 1$ for some $t \in \mathbb{N}$ and $n_5 \mid |G|$. Thus, $(5t + 1) \mid 3$. So, $t = 0$ and $n_5 = 1$.

(*b*) By (*a*), we see that $K \lhd G$. Since $h^{-1}gh$ and g have the same order for all $h \in H$, we see that $\langle h^{-1}gh \rangle = \langle g \rangle = K$. Thus, H acts on X by conjugation. By Orbit-Stabilizer theorem, the size of an orbit is a factor of $|H|$. Thus, the possible sizes of orbits can be 1 or 3 as $|H| = 3$.

$|X| = \varphi(5^3) = 5^3(1 - \frac{1}{5}) = 100$.

(*c*) Note that $G/K \cong H$ and $K \cap H = \{1\}$ as $\gcd(|K|, |H|) = 1$. Thus, we see that $|KH| = |K||H|/|K \cap H| = 375 = |G|$. Thus, $G = KH$. So, $G \cong K \rtimes_\theta H$, where $\theta : H \to \mathrm{Aut}(K)$ is a homomorphism. By (*b*), we see that $|\mathrm{Aut}(K)| = |X| = 100$. Since $3 \nmid 100$, we see that θ is trivial. It follows that $G = K \times H \cong \mathbb{Z}_{125} \times \mathbb{Z}_3 \cong \mathbb{Z}_{375}$. □

Remark. Another way for (*c*) using group actions: Since $3 \nmid 100$, there exists an orbit whose size is 1. Thus, there exists $g \in X$ such that $h^{-1}gh = g$ for all $h \in H$. Thus, $hg^n = g^n h$ for all n, i.e. H commutes with K. So, $KH \cong K \times H \cong \mathbb{Z}_{125} \times \mathbb{Z}_3 \cong \mathbb{Z}_{375}$ is a subgroup of G.

Problem 40 (18J·3). Prove: If a group G contains a proper subgroup of finite index, then it contains a proper normal subgroup of finite index.

Proof. Suppose H is a proper subgroup of G of finite index.

Let $X = G/H$ to be the set of left cosets of H in G, then $|X| = [G : H] < \infty$. Consider a map

$$\Psi : G \to S_X$$

by

$$g \mapsto \sigma_g,$$

where $\sigma_g : X \to X$ is given by left translation, i.e. $\sigma_g(kH) = gkH$. Since $\sigma_{gh}(kH) = ghkH = \sigma_g(hkH) = \sigma_g\sigma_h(kH)$ for all $kH \in X$, we see that $\Psi(gh) = \sigma_{gh} = \sigma_g\sigma_h = \Psi(g)\Psi(h)$. Thus, we see that Ψ is a group homomorphism. Then, $g \in \ker\Psi \Leftrightarrow \sigma_g(kH) = gkH = kH$ for all $k \in G$ $\Leftrightarrow k^{-1}gk \in H$ for all $k \in G \Leftrightarrow g \in kHk^{-1}$ for all $k \in H \Leftrightarrow g \in \bigcap_{k \in G} k^{-1}Hk =: N$. Thus, $N = \ker\Psi \lhd G$. Since $N \subseteq H$ and H is proper, we see that N is proper. It remains to show that $[G : N] < \infty$. Indeed, $G/N \hookrightarrow S_X$ by first isomorphism theorem and $|S_X| = [G : H]! < \infty$, so we see that $[G : N] = |G/N| \leqslant |S_X| < \infty$. □

Problem 41 (18J·4). How many elements of order 7 are there in a simple group of order 168?

Proof. Let G be a simple group of order 168. Note that $168 = 2^3 \cdot 3 \cdot 7$. Let n_p be the number of Sylow p-subgroups of G, where p is a prime factor of $|G|$. By third Sylow's theorem, we see that $n_7 = 7t + 1$ for some $t \in \mathbb{N}$ and $n_7 \mid |G|$. Thus, $(7t + 1) \mid 24$. Then, $t = 0$ or 1 and $n_7 = 1$ or 8. If $n_7 = 1$, then G has exactly one subgroup of order 7, which must be normal by second Sylow's theorem. But G is simple, a contradiction. Thus, $n_7 = 8$ and there are $8 \times (7 - 1) = 48$ elements of order 7. □

Problem 42 (18A·1). Let G be a finite group. Prove that the number of ordered pairs $(g, h) \in G^2$ such that g and h commute is equal to $k|G|$, where k is the number of conjugacy classes in G.

Proof. Let $\mathcal{O}_1, \cdots, \mathcal{O}_k$ be all conjugacy classes in G and $\mathrm{Cl}(g)$ be the conjugacy class containing g. Note that (g, h) is a pair such that g and h commute if and only if $gh = hg \Leftrightarrow g = h^{-1}gh \Leftrightarrow$

$h \in C_G(g)$. Thus, the number of ordered pairs $(g, h) \in G^2$ such that g and h commute is equal to

$$\begin{aligned}\sum_{g \in G} |C_G(g)| &= \sum_{g \in G} \frac{|G|}{[G : C_G(g)]} \\ &= \sum_{g \in G} \frac{|G|}{|\operatorname{Cl}(g)|} \\ &= \sum_{i=1}^{k} \sum_{g \in \mathcal{O}_i} \frac{|G|}{|\operatorname{Cl}(g)|} \\ &= \sum_{i=1}^{k} |\mathcal{O}_i| \frac{|G|}{|\mathcal{O}_i|} \\ &= \sum_{i=1}^{k} |G| = k|G|.\end{aligned}$$

□

Problem 43 (18A·2). Here S_n and A_n are the symmetric and the alternating groups on n objects. You may use the fact that A_n is simple for $n \geqslant 5$ and that if H is a simple subgroup of S_n of order more than 2, then $H \subseteq A_n$.

(a) Show that every homomorphism $A_6 \to S_4$ is trivial.

(b) Show that A_6 has no subgroups of index 4.

(c) Let G be a group of order 90 with no normal subgroups of order 5. Show that there is a non-trivial homomorphism $G \to S_6$. (Hint: consider the Sylow 5-subgroups.)

(d) Show that there are no simple groups of order 90.

Proof. (a) Let $f : A_6 \to S_4$ be a group homomorphism, then $\ker f = 0$ or A_6 as A_6 is a simple group. If $\ker f = A_6$, then f is trivial, we are done. If $\ker f = 0$ and in this case, we see that A_6 is isomorphic to a subgroup of S_4. However, $|A_6| = 360 > 24 = |S_4|$. Contradiction. Thus, every homomorphism $A_6 \to S_4$ is trivial.

(b) Assume H is a subgroup of A_6 such that $[A_6 : H] = 4$. Let X be the set of left cosets of H in G. Then, there is a group homomorphism

$$\Psi : A_6 \to S_X \cong S_4$$

given by

$$g \mapsto \Psi_g,$$

where $\Psi_g : X \to X$ is given by $hH \mapsto ghH$. Then, $g \in \ker \Psi \Leftrightarrow ghH = hH$ for all $h \in A_6 \Leftrightarrow h^{-1}gh \in H$ for all $h \in A_6 \Leftrightarrow g \in hHh^{-1}$ for all $h \in A_6 \Leftrightarrow g \in \bigcap_{h \in A_6} hHh^{-1}$. Thus, $\ker \Psi = \bigcap_{h \in A_6} hHh^{-1} \subseteq H$. By ($a$), we see that Ψ is trivial, i.e. $\ker \Psi = A_6$. Contradiction. Thus, A_6 has no subgroups of index 4.

(c) Let n_5 be the number of Sylow 5-subgroups of G. Then, by third Sylow's theorem, we see that $n_5 = 5t + 1$ for some $t \in \mathbb{N}$ and $n_5 \mid |G|$. Thus, $(5t + 1)|18$. Then $t = 1$ and $n_5 = 6$ as G has no normal subgroups of order 5. Let H be a Sylow 5-subgroup, then $[G : H] = 6$. So, there is a group homomorphism

$$\Psi : G \to S_{G/H} \cong S_6$$

given by

$$g \mapsto \Psi_g,$$

where $\Psi_g : G/H \to G/H$ is given by $hH \mapsto ghH$.

Then, $g \in \ker \Psi \Leftrightarrow ghH = hH$ for all $h \in G \Leftrightarrow h^{-1}gh \in H$ for all $h \in G \Leftrightarrow g \in hHh^{-1}$ for all $h \in G \Leftrightarrow g \in \bigcap_{h\in G} hHh^{-1}$. Thus, $\ker \Psi = \bigcap_{h\in G} hHh^{-1} \subseteq H$. This means that Ψ is non-trivial.

(d) Suppose G is a simple group of order 90. Then, G cannot have normal subgroups of order 5. By (c), we have a non-trivial homomorphism $\Psi : G \to S_6$. Then, $\ker \Psi = 0$ as G is simple. Then, G can be regarded as a simple subgroup of S_6. Since $|G| > 2$, we see that $G \subseteq A_6$ by the fact that if G is a simple subgroup of S_n of order more than 2, then $G \subseteq A_n$. Note that $[A_6 : G] = 360/90 = 4$, which contradicts (b).

Thus, there are no simple groups of order 90. □

Problem 44 (19J·2). Let G be a finite group acting on a finite set X. Assume that each point in X is fixed by at least one nonidentity element of G, and that each nonidentity element of G fixes at most two points of X. Prove that the action has at most three orbits.

Proof. We denote $\{x \in X : g \cdot x = x\}$ by $\operatorname{Fix}(g)$, where $g \in G$. We claim that $n|G| = \sum_{g\in G} |\operatorname{Fix}(g)|$, where n is the number of orbits. Indeed, if $\mathcal{O}_1, \cdots, \mathcal{O}_n$ are the orbits and $\mathcal{O}(x)$ is the orbit containing x, then

$$\begin{aligned}
\sum_{g\in G} |\operatorname{Fix}(g)| &= \#\{(g,x) \in G \times X : g \cdot x = x\} \\
&= \sum_{x\in X} |G_x| \\
&= \sum_{x\in X} \frac{|G|}{[G : G_x]} \\
&= \sum_{x\in X} \frac{|G|}{|\mathcal{O}(x)|} \\
&= \sum_{i=1}^{n} \sum_{x\in \mathcal{O}_i} \frac{|G|}{|\mathcal{O}(x)|} \\
&= \sum_{i=1}^{n} |\mathcal{O}(x)| \frac{|G|}{|\mathcal{O}(x)|} \\
&= n|G|.
\end{aligned}$$

By our hypothesis, we see that $|G_x| \geqslant 2$ for all $x \in X$ and then $|\mathcal{O}(x)| = [G : G_x] \leqslant \frac{|G|}{2}$. Thus, $|X| = \sum_{i=1}^{n} |\mathcal{O}_i| \leqslant \sum_{i=1}^{n} \frac{|G|}{2} = \frac{n|G|}{2}$. We also have $|\operatorname{Fix}(g)| \leqslant 2$ for all non-identity $g \in G$. Thus,

$$n|G| = \sum_{g\in G} |\operatorname{Fix}(g)| \leqslant 2(|G| - 1) + |X| \leqslant 2(|G| - 1) + \frac{n|G|}{2}.$$

Thus, $\frac{n|G|}{2} \leqslant 2|G| - 2$, or $n|G| \leqslant 4|G| - 4 < 4|G|$. Thus, $n < 4$. Therefore, the action has at most three orbits. □

Problem 45 (19J·3). Let n be a positive integer and let $G = D_{2^{n+1}} := \langle r, s | r^{2^n} = s^2 = 1, sr = r^{-1}s\rangle$.

(a) Find the ascending central series $(C_n(G))_{n\geqslant 0}$ of G. Explain your answer.

(Recall that, by definition, $C_0(G)$ is the trivial group and $C_{n+1}(G)$ is the inverse image of the center of $G/C_n(G)$ under the quotient map $G \to G/C_n(G)$.)

(b) Is G nilpotent? Justify your answer.

(c) Is G solvable? Justify your answer.

Proof. (a) We prove that $C_m(G) = \langle r^{2^{n-m}} \rangle \cong \mathbb{Z}_{2^m}$ for all $0 \leqslant m \leqslant n$ by induction on m.

By definition, $C_1(G) = Z(G) = \{1, r^{2^{n-1}}\} = \langle r^{2^{n-1}} \rangle \cong \mathbb{Z}_2$. Suppose $C_m(G) = \langle r^{2^{n-m}} \rangle$ for all $m = 1, 2, \cdots, k$. Then, $G/C_k(G) \cong D_{2^{n+1-k}}$ and $Z(G/C_k(G)) = \{1, r^{2^{n-k-1}}\}$. Thus, by definition, $C_{k+1}(G) = C_k(G) \cup r^{2^{n-k-1}} C_k(G) = \langle r^{2^{n-k-1}} \rangle \cong \mathbb{Z}_{2^{k+1}}$.

Thus, we see that $C_k(G) = \langle r^{2^{n-k}} \rangle \cong \mathbb{Z}_{2^k}$ for all $0 \leqslant k \leqslant n$. Note that $G/C_n(G) = \langle s \rangle \cong \mathbb{Z}_2$ and $Z(G/C_n(G)) = \langle s \rangle$, so $C_{n+1}(G) = C_n(G) \cup sC_n(G) = G$. Then, we see that $C_k(G) = G$ for all $k \geqslant n+1$.

(b) G is nilpotent as the ascending central series $(C_n(G))_{n \geqslant 0}$ of G stabilizes after finitely many steps by (a).

(c) G is solvable as nilpotent groups are all solvable. □

Problem 46 (19A·1). Let G be a group of order 91. Prove that G is abelian. (Note that $91 = 7 \cdot 13$.)

Proof. Let n_p be the number of Sylow p-subgroups of G, where p is a prime factor of $|G|$. Then, by third Sylow's theorem, we see that $n_{13} = 13t + 1$ for some $t \in \mathbb{N}$ and $n_{13} \mid |G|$, i.e. $(13t + 1) \mid 7$. Thus, $t = 0$ and $n_{13} = 1$. Thus, G has exactly one subgroup of order 13, say H. By second Sylow's theorem, $H \lhd G$. Similarly, $n_7 = 1$ and G has exactly one subgroup of order 7, say K. By second Sylow's theorem, $K \lhd G$. We see that $G = HK \cong H \times K \cong \mathbb{Z}_{13} \times \mathbb{Z}_7$ is abelian. □

Problem 47 (19A·2). Let G be a group and let $Z(G)$ be the center of G. Let $n = [G : Z(G)]$.

(a) Prove that every conjugacy class of G has at most n elements.

(b) Suppose $n > 1$. Is there an example of a group G with $[G : Z(G)] = n$ and an element $g \in G$ such that the conjugacy class of g has exactly n elements? Justify your answer.

Proof. (a) For any $x \in G$, by Orbit-Stabilizer theorem, we have $[G : C_G(x)] = |\operatorname{Cl}(x)|$. Note that $Z(G) \subseteq C_G(x)$ for all $x \in G$. We have that $[G : C_G(x)] \leqslant [G : Z(G)] = n$, i.e. $|\operatorname{Cl}(x)| \leqslant n$.

(b) No. If $|\operatorname{Cl}(g)| = n$ for some $g \in G$, then $C_G(g) = Z(G)$. Thus, we see that $g \in Z(G)$, i.e. $gh = hg$ for all $h \in G$. Thus, $h \in C_G(g)$ for all $h \in G$. So, we see that $C_G(g) = G = Z(G)$. Then, $n = 1$. Contradiction. □

Problem 48 (20J·1). Let H be a subgroup of a group G. Consider the normalizer and centralizer (respectively) of H:

$$N_G(H) := \{g \in G | gHg^{-1} = H\} \quad \text{and} \quad C_G(H) := \{g \in G | gh = hg \text{ for all } h \in H\}.$$

(a) Prove that both the normalizer and centralizer are subgroups of G.

(b) Prove that the centralizer is a normal subgroup of the normalizer.

(c) Prove that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\operatorname{Aut}(H)$ (the group of automorphisms of H, that is, bijective group homomorphisms from H to itself).

(d) Assume additionally that H is a normal subgroup of G, and that H is finite. Prove that the index of $C_G(H)$ in G is finite.

Proof. (a) Let $g, h \in N_G(H)$, then $(gh^{-1})H(gh^{-1})^{-1} = g(h^{-1}Hh)g^{-1} = gHg^{-1} = H$. Thus, $gh^{-1} \in N_G(H)$. So, $N_G(H)$ is a subgroup of G. Let $a, b \in C_G(H)$, then $(ab^{-1})h = ahb^{-1} = hab^{-1}$ for all $h \in H$. Thus, $ab^{-1} \in C_G(H)$. Thus, $C_G(H)$ is a subgroup of G.

(b) Let $a \in C_G(H)$, then $ah = ha$ for all $h \in H$. Let $g \in N_G(H)$, then for any $h \in H$, we have $ghg^{-1} = h'$ for some $h' \in H$. Then $(g^{-1}ag)h = g^{-1}ah'g = g^{-1}h'ag = hg^{-1}ag = h(g^{-1}ag)$ for all $h \in H$. Thus, we see that $g^{-1}ag \in C_G(H)$. So, $C_G(H) \lhd N_G(H)$. □

Problem 49 (20J·8). Is the symmetric group S_4 the internal direct sum of two or more nontrivial subgroups? Prove your answer.

Proof. We first find all conjugacy classes of S_4:

(i) The conjugacy class of (1234), there are $P_4^4/4 = 3! = 6$ elements.

(ii) The conjugacy class of (123), there are $P_4^3/3 = 8$ elements.

(iii) The conjugacy class of (12), there are $\binom{4}{2} = 6$ elements.

(iv) The conjugacy class of $(12)(34)$, there are $\binom{4}{2}/2 = 3$ elements.

(v) The conjugacy class of (1), one element in total.

Note that a subgroup is a normal subgroup if and only if it is a subgroup and it is a union of some conjugacy classes. By Lagrange's theorem, if N is a non-trivial proper normal subgroup of S_4, then $|N| = 2, 3, 4, 6, 8, 12$. By investigating the conjugacy classes, we see that $|N| \neq 2, 3, 6, 8$. If $|N| = 4$, then $N = \{(1), (12)(34), (13)(24), (14)(23)\} := V$. If $|N| = 12$, then N is the union of $(ii), (iv)$ and (v), i.e. $N = A_4$.

Thus, $\{1\}, V, A_4, S_4$ are the only normal subgroups of S_4.

Note that a direct summand of S_4 must be a normal subgroup of S_4. If S_4 is the internal direct sum of two or more nontrivial subgroups, then the only possibility is $S_4 = V \oplus A_4$, which is absurd as $|V||A_4| = 4 \times 12 = 48$.

Thus, S_4 cannot be the internal direct sum of two or more nontrivial subgroups. □

Problem 50 (20A·1). Let p be a prime number, and let G be a finite group of order p^n for some $n \geqslant 1$. Suppose G acts on a finite set X, and let

$$Y = \{x \in X : \forall \sigma \in G, \sigma \cdot x = x\}.$$

You may recall a lemma that states that $|X| \equiv |Y| \pmod{p}$. Prove that this is true.

Proof. Let $\mathcal{O}_1, \cdots, \mathcal{O}_k$ be the distinct orbits of the action of G on X. We may assume that $|\mathcal{O}_i| = 1$ for $i = 1, 2, \cdots, s$ and $|\mathcal{O}_i| \geqslant 2$ for $i = s + 1, \cdots, k$. Then, we see that Y is the disjoint union of those orbits whose length is 1, i.e. $Y = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_s$. Then, $X = Y \cup \mathcal{O}_{s+1} \cup \cdots \cup \mathcal{O}_k$ as a disjoint union. Thus, $|X| = |Y| + \sum_{i=s+1}^{k} |\mathcal{O}_i|$. Recall that by Orbit-Stabilizer theorem, we have $[G : G_x] = |\mathcal{O}(x)|$, where G_x is the stabilizer of x and $\mathcal{O}(x)$ is the orbit containing x. So, we see that $|\mathcal{O}_i| \mid p^n$ for all i. Since $|\mathcal{O}_i| \geqslant 2$ for $i = s + 1, \cdots, k$, we have $|\mathcal{O}_i| = p^m$ with $1 \leqslant m \leqslant n$ for $i = s + 1, \cdots, k$. Thus, $|X| \equiv |Y| \pmod{p}$. □

Problem 51 (20A·2). Let G be a group of order $520 = 2^3 \cdot 5 \cdot 13$.

(a) For $p = 2, 5, 13$, let N_p denote the number of Sylow p-subgroups of G. According to the Sylow Theorems, what are the possibilities for N_2, N_5, and N_{13}?

(b) If $N_5 \neq 1$, how many elements are there of order 5 in G? If $N_{13} \neq 1$, how many elements are there of order 13 in G?

(c) Prove that G is not simple.

Proof. (a) By third Sylow's theorem, we see that $N_{13} = 13t + 1$ for some $t \in \mathbb{N}$ and $N_{13} \mid |G|$. Thus, $(13t + 1) \mid 40$. So, $t = 0$ or 3 and $N_{13} = 1$ or 40.

Similarly, $N_5 = 5t + 1$ for some $t \in \mathbb{N}$ and $N_5 \mid |G|$. Thus, $(5t + 1) \mid 2^3 \cdot 13$. So, $t = 0$ or 5 and $N_5 = 1$ or 26.

Moreover, $N_2 = 2t + 1$ for some $t \in \mathbb{N}$ and $N_2 \mid |G|$. Thus, $(2t + 1) \mid 5 \cdot 13$. So, $t = 0, 2, 6$ or 32 and $N_2 = 1, 5, 13$ or 65.

(b) If $N_5 \neq 1$, then there are 26 subgroups of order 5 in G. Each pair of distinct subgroups or order 5 has trivial intersection. Then, there are $26 \times (5 - 1) = 26 \times 4 = 104$ elements of order 5.

Similarly, if $N_{13} \neq 1$, then there are $40 \times (13 - 1) = 480$ elements of order 13 in G.

(c) We may assume that $N_5 \neq 1$ and $N_{13} \neq 1$, otherwise G has exactly one subgroup of order 5 or 13, which is normal in G by 2nd Sylow's theorem and G is then not simple. In this case, there are $104 + 480 = 584$ elements of order 5 or 13 in G. This is absurd as $|G| < 584$. Thus, $N_5 = 1$ or $N_{13} = 1$. Therefore, G is not simple. □

Problem 52 (21J·1). (a) Prove that an extension of a torsion group by a torsion group is torsion, i.e. if $G/N = H$ and H, N are torsion groups then G is torsion.

(b) Prove that an extension of a torsion-free group by a torsion-free group is torsion-free.

Proof. (a) Let $g \in G$, then gN is a torsion element as G/N is a torsion group, i.e. there exists an integer $n \in \mathbb{N}$ such that $g^n N = (gN)^n = N$. Thus, $g^n \in N$. Since N is a torsion subgroup, there exists an integer $m \in \mathbb{N}$ such that $(g^n)^m = 1$, i.e. $g^{mn} = 1$. Thus, g is a torsion element. Thus, G is a torsion group.

(b) Suppose $G/N = H$ and N, H are torsion-free. Argue by contradiction, we may assume that G is not torsion-free. So, there exists $g \in G$ such that $g^n = 1$ for some integer $n \in \mathbb{N}$. Then, $(gN)^n = g^n N = N$, which implies that $gN \in H$ is a torsion element. This is a contradiction as H is torsion-free. Thus, G is torsion-free. □

Problem 53 (21J·2). Let G be a group and G' be the commutator subgroup i.e. the subgroup generated by elements $[a, b] = aba^{-1}b^{-1}, a, b \in G$.

(a) Prove that G' is a normal subgroup in G.

(b) Prove that $G_{\text{ab}} = G/G'$ is abelian.

(c) Prove that if $N \lhd G$ and G/N is abelian then N contains G'.

Proof. (a) First, for any $g \in G$ and $a, b \in G$, we see that

$$g^{-1}[a, b]g = g^{-1}aba^{-1}b^{-1}g = g^{-1}agg^{-1}bgg^{-1}a^{-1}gg^{-1}b^{-1}g = [g^{-1}ag, g^{-1}bg].$$

Since G' is generated by commutators, for any $h \in G'$, $h = [a_1, b_1] \cdots [a_n, b_n]$ for some $a_i, b_i \in G$. Thus, for any $g \in G$, we have $g^{-1}hg = g^{-1}[a_1, b_1] \cdots [a_n, b_n]g = (g^{-1}[a_1, b_1]g) \cdots (g^{-1}[a_n, b_n]g) = [g^{-1}a_1 g, g^{-1}b_1 g] \cdots [g^{-1}a_n g, g^{-1}b_n g] \in G'$. Thus, $G' \lhd G$.

(b) For any $\overline{a}, \overline{b} \in G_{\text{ab}}$, we see that there exists $a, b \in G$ such that $\overline{a} = aG'$ and $\overline{b} = bG'$. So, $[\overline{a}, \overline{b}] = (aG')(bG')(aG')^{-1}(bG')^{-1} = (aba^{-1}b^{-1})G' = [a, b]G' = G'$. Thus, we see that $\overline{a}\overline{b} = \overline{b}\overline{a}$ for all $\overline{a}, \overline{b} \in G_{\text{ab}}$. Thus, G_{ab} is abelian.

(c) For any $g, h \in G$, we have $(gN)(hN)(gN)^{-1}(hN)^{-1} = N$ as G/N is abelian. Thus, $[g, h]N = (ghg^{-1}h^{-1})N = (gN)(hN)(gN)^{-1}(hN)^{-1} = N$. So, $[g, h] \in N$ for all $g, h \in G$. Thus, $G' \subseteq N$. □

Problem 54 (21J·3). Classify all groups of order 21.

Proof. Note that $21 = 3 \times 7$. Let G be a group of order 21. Let n_p be the number of Sylow p-subgroups of G, where p is a prime factor of $|G|$. By third Sylow's theorem, we see that $n_7 = 7t+1$ for some $t \in \mathbb{N}$ and $n_7 \mid |G|$. Thus, $(7t+1) \mid 3$. So, $t = 0$ and $n_7 = 1$. Thus, G has exactly one subgroup of order 7, say H. Then, by 2nd Sylow's theorem, $H \lhd G$. Similarly, $n_3 = 3t+1$ for some $t \in \mathbb{N}$ and $(3t+1) \mid 7$. Thus, $n_3 = 1$ or 7.

Let $a \in G$ be a generator of $H \cong \mathbb{Z}_7$ and $b \in G$ an element of order 3. Then, $b^{-1}ab \in H$ as $H \lhd G$. Thus, $b^{-1}ab = a^i$ is also a generator of H. Since $b^3 = 1$, we see that $a = b^{-3}ab^3 = a^{i^3}$, i.e. $a^{i^3-1} = 1$ in H. Thus, $7 \mid i^3 - 1$, and $i = 1, 2, 4$.

If $i = 1$, then $ab = ba$ and $G = \langle a, b \mid a^7 = b^3 = 1, ab = ba\rangle \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_7 \times \mathbb{Z}_3 \cong \mathbb{Z}_{21}$.

If $i = 2$, then $G = \langle a, b \mid a^7 = b^3 = 1, b^{-1}ab = a^2\rangle$.

If $i = 4$, then $G = \langle a, b \mid a^7 = b^3 = 1, b^{-1}ab = a^4\rangle$. □

2 Rings

Problem 55 (09J·3). Let $i = \sqrt{-1}$ in $\mathbb{C}$, and let x be an indeterminate.

(a) Show that the three additive groups $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{Z}[x]/(x^2)$ are all isomorphic to each other.

(b) Show that no two of the three rings $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{Z}[x]/(x^2)$ are isomorphic to each other.

Proof. (a) Consider $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}[i]$ by $(a, b) \mapsto a + bi$. Then $\varphi((a, b) + (c, d)) = \varphi(a + c, b + d) = (a + c) + (b + d)i = (a + bi) + (c + di) = \varphi(a, b) + \varphi(c, d)$. Thus, φ is an homomorphism. Clearly, φ is surjective. Note that $\varphi(a, b) = 0$ iff $a + bi = 0$ iff $a = b = 0$. Thus, φ is injective. Therefore, φ is an isomorphism.

Consider $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}[x]/(x^2)$ by $(a, b) \mapsto a + b\overline{x}$. Then $\phi((a, b) + (c, d)) = \phi(a + c, b + d) = (a + c) + (b + d)\overline{x} = (a + b\overline{x}) + (c + d\overline{x}) = \phi(a, b) + \phi(c, d)$. Thus, ϕ is an homomorphism. Clearly, ϕ is surjective. Note that $\phi(a, b) = 0$ iff $a + b\overline{x} = 0$ iff $a = b = 0$. Thus, ϕ is injective. Therefore, ϕ is an isomorphism.

Thus, the three additive groups $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{Z}[x]/(x^2)$ are all isomorphic to each other.

(b) Suppose $f : \mathbb{Z}[i] \to \mathbb{Z} \times \mathbb{Z}$ is an isomorphism. Let $(a, b) = f(i)$. Since $i^2 + 1 = 0$, we have $(a, b)^2 + (1, 1) = (0, 0)$, which is impossible as $a, b \in \mathbb{Z}$. Thus, $\mathbb{Z}[i]$ is not isomorphic to $\mathbb{Z} \times \mathbb{Z}$.

Suppose $g : \mathbb{Z}[i] \to \mathbb{Z}[x]/(x^2)$ is an isomorphism. Let $a + b\overline{x} = g(i)$. Since $i^2 + 1 = 0$, we have $(a + b\overline{x})^2 + 1 = 0$, i.e. $a^2 + 2ab\overline{x} + 1 = 0$. Thus $a^2 + 1 = 0$ and $ab = 0$, which is impossible as $a, b \in \mathbb{Z}$. Thus, $\mathbb{Z}[i]$ is not isomorphic to $\mathbb{Z}[x]/(x^2)$.

Suppose $h : \mathbb{Z}[x]/(x^2) \to \mathbb{Z} \times \mathbb{Z}$ is an isomorphism. Let $(a, b) = h(\overline{x})$. Since $\overline{x}^2 = 0$, we have $(a, b)^2 = 0$, i.e. $(a^2, b^2) = 0$. Thus $a^2 = b^2 = 0$ and thus $a = b = 0$, which implies that $\overline{x} \in \ker h$. This is a contradiction as $\overline{x} \neq 0$ and h is an isomorphism. Thus, $\mathbb{Z}[i]$ is not isomorphic to $\mathbb{Z}[x]/(x^2)$.

We conclude that no two of the three rings $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{Z}[x]/(x^2)$ are isomorphic to each other. □

Problem 56 (09J·4). Let R be a commutative ring with 1. Show that the sum of any two principal ideals of R is principal if and only if every finitely generated ideal of R is principal.

Proof. $\Rightarrow$: Trivial as $(a) + (b) = (a, b)$ is finitely generated.

$\Leftarrow$: Suppose $I = (a_1, \cdots, a_n)$. We will prove I is principal by induction on n. If $n = 1$, done. By induction hypothesis, $(a_1, \cdots, a_{n-1}) = (c)$ for some $c \in R$. Thus, $I = (a_1, \cdots, a_n) = (a_1, \cdots, a_{n-1}) + (a_n) = (c) + (a)$ is principal. Thus, every finitely generated ideal of R is principal. □

Problem 57 (09J·5). Let R be the subring of the polynomial ring $\mathbb{Z}[x]$ consisting of every polynomial in which the coefficients of x and x^2 are both 0. Prove that the field of fractions of R is precisely the field of rational functions $\mathbb{Q}(x)$ over $\mathbb{Q}$.

Proof. First, $\mathbb{Z} \subseteq R$, so $\mathbb{Q} \subseteq \mathrm{Frac}(R)$. Note that $x^3, x^4 \in R$, so $x = \frac{x^4}{x^3} \in \mathrm{Frac}(R)$. Thus, $\mathbb{Q}(x) \subseteq \mathrm{Frac}(R)$. Note that $\mathrm{Frac}(\mathbb{Z}[x]) = \mathbb{Q}(x)$ and $R \subseteq \mathbb{Z}[x]$, we see that $\mathrm{Frac}(R) \subseteq \mathbb{Q}(x)$. Thus, $\mathrm{Frac}(R) = \mathbb{Q}(x)$. □

Problem 58 (09A·4). (a) Describe all maximal ideals in $\mathbb{C}[x]$.

(b) Describe all maximal ideals in $\mathbb{R}[x]$.

(c) Describe (up to isomorphism) the fields that may be obtained as quotients $\mathbb{R}[x]/M$, where M is a maximal ideal of $\mathbb{R}[x]$.

Proof. (a) Since $\mathbb{C}[x]$ is a field, we know that $\mathbb{C}[x]$ is a PID. So, every maximal ideal of $\mathbb{C}[x]$ is of the form (f), where $f \in \mathbb{C}[x]$ is an irreducible polynomial. Note that $\mathbb{C}$ is algebraically closed, so we see that irreducible polynomials are precisely linear polynomials. So, maximal ideals of $\mathbb{C}[x]$ are of the form $(x - a)$ with some $a \in \mathbb{C}$. We conclude that all ideals of the form $(x - a)$ are maximal ideals of $\mathbb{C}[x]$.

(b) Since $\mathbb{R}[x]$ is a field, we know that $\mathbb{R}[x]$ is a PID. So, every maximal ideal of $\mathbb{R}[x]$ is of the form (f), where $f \in \mathbb{R}[x]$ is an irreducible polynomial. So, The maximal ideals of $\mathbb{R}[x]$ are of the form $(x - a)$ with $a \in R$ or $(x^2 + bx + c)$, with $b, c \in \mathbb{R}$ and $b^2 - 4c < 0$.

(c) If $M = (x - a)$ for some $a \in R$, then $\mathbb{R}[x]/M \cong \mathbb{R}$. If $M = (x^2 + bx + c)$ with $b^2 - 4c < 0$, then $\mathbb{R}[x]/(x^2 + bx + c) \cong \mathbb{R}(\frac{-b\pm\sqrt{b^2-4c}}{2}) = \mathbb{R}(\sqrt{b^2 - 4c})$. □

Problem 59 (09A·5). Let K be a field and let K^* be the non-zero elements in K. A discrete valuation on K is a function $\nu : K^* \to \mathbb{Z}$ such that

i. $\nu(ab) = \nu(a) + \nu(b)$ for all $a, b \in K^*$, i.e., ν is a homomorphism from the multiplicative group of the field to the integers.

ii. ν is surjective.

iii. $\nu(a + b) \geqslant \min\{\nu(a), \nu(b)\}$ for all $a, b \in K^*$ with $a + b \neq 0$.

The set $R = \{x \in K^* | \nu(x) \geqslant 0\} \cup \{0\}$ is call the valuation ring of ν.

(a) Prove that R is a subring of K which contains the identity.

(b) Prove that for each nonzero $x \in K$, either x or x^{-1} is in R.

Proof. (a) First, $\nu(1) = \nu(1 + 1) = \nu(1) + \nu(1)$ by i, so $\nu(1) = 0$. By definition, we see that $1 \in R$. We now show that R is a ring.

Again by i, $\nu(1) = \nu(-1) + \nu(-1) = 0$, thus, $\nu(-1) = 0$. So, $\nu(-a) = \nu(-1) + \nu(a) = \nu(a)$ for all $a \in K^*$. Thus for a non-zero $a \in R$, we have $\nu(a) \geqslant 0$, so $\nu(-a) = \nu(a) \geqslant 0$, i.e. $-a \in R$. Note that if $a, b \in R$, we have $\nu(a+b) \geqslant \min\{\nu(a), \nu(b)\} \geqslant 0$, i.e. $a + b \in R$. Thus, $(R, +)$ is an additive group. If $a, b \in R$, then $\nu(ab) = \nu(a) + \nu(b) \geqslant 0$, i.e. $ab \in R$. So, R is a ring with identity. Since $R \subseteq K$, we see that R is a subring of K containing the identity.

(b) Suppose $x \notin R$ and $x \neq 0$. Then, $\nu(x) \leqslant 0$. This implies that $\nu(x) + \nu(x^{-1}) = \nu(xx^{-1}) = \nu(1) = 0$, i.e. $\nu(x^{-1}) = -\nu(x) \geqslant 0$. Thus, we see that $x^{-1} \in R$. □

Problem 60 (10J·3). Let R be a principal ideal domain. Show that if $P \neq (0)$ is a prime ideal then P is maximal.

Proof. Let $P = (x)$ for some nonzero $x \in R$. Then, x is a prime element in R. Suppose $(x) \subsetneq (y)$. Then, $x = ay$ for some $a \in R$, i.e. $y|x$. Since x is prime, we see that $x|a$ or $x|y$. Suppose $x|y$, then

$(x) = (y)$, contradiction. Thus, $x|a$, say $a = xz$ for some $z \in R$. Thus, $x = xzy$, i.e. $x(1-zy) = 0$. Since R is an integral domain and $x \neq 0$, we see that $zy = 1$, i.e. y is a unit. Thus, $(y) = R$. So, we see that P is a maximal ideal. □

Problem 61 (10A·3). Let R be a ring with identity 1.

(*a*) Let M be a maximal ideal and $r \in R$ such that $1 - rx \in R^\times$ for all $x \in R$. Show that $r \in M$.

(*b*) (conversely) Suppose that $r \in M$ for every maximal ideal M. Show that $1 - rx \in R^\times$ for all $x \in R$. (Recall that every proper non-zero ideal is contained in some maximal ideal).

Proof. (*a*) Suppose, $r \notin M$, then $M \subsetneq M + (r) \subseteq (1)$. Thus, $M + (r) = (1)$ as M is maximal. So, $1 = rx + m$ for some $x \in R$, $m \in M$. Thus, $m = 1 - rx \in R^\times$. Then, $M = (1)$. Contradiction. So, $r \in M$.

(*b*) Argue by contradiction. Assume there exists $x \in R$ such that $1 - rx \notin R^\times$, then $1 - rx \in M$ for some maximal ideal M. Since $r \in M$, then $rx \in M$ and so $1 = (1-rx)+rx \in M$. Contradiction. Thus, $1 - rx \in R^\times$ for all $x \in R$. □

Problem 62 (11J·6). Show that the group of units in $\mathbb{Z}[(1+\sqrt{5})/2]$ is infinite.

Proof. Let $x = 9 + 4\sqrt{5}$, then x is a unit, as $(9+4\sqrt{5})(9-4\sqrt{5}) = 1$. Then, $1, x, x^2, \cdots, x^k, \cdots$ are distict units. Thus, the group of units in $\mathbb{Z}[(1+\sqrt{5})/2]$ is infinite. □

Problem 63 (11A·2). Decompose 35 into product of prime elements of $\mathbb{Z}[i]$ (and show this is indeed a prime decomposition).

Proof. Recall that $\mathbb{Z}[i]$ is an euclidean domain, thus a UFD. Note that $35 = 5\times 7 = 7(1+2i)(1-2i)$, we now show that this is indeed a prime decomposition. Consider the norm function $N : \mathbb{Z}[i] \to \mathbb{Z}$ given $\alpha \mapsto \alpha\overline{\alpha}$. Suppose $7 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Then, $N(\alpha)N(\beta) = N(7) = 49$. So, we may assume that $N(\alpha) = N(\beta) = 7$ or $N(\alpha) = 1$ and $N(\beta) = 49$. By solving the Diophantine equations $N(a + bi) = a^2 + b^2 = 7$, $a^2 + b^2 = 49$ and $a^2 + b^2 = 1$, we see that $\begin{cases} \alpha = i \\ \beta = -7i \end{cases}$ or $\begin{cases} \alpha = -i \\ \beta = 7i \end{cases}$. In either cases, α is a unit. Thus, we see that 7 is irreducible in $\mathbb{Z}[i]$, hence a prime elelment in $\mathbb{Z}[i]$.

Similarly, suppose $1 \pm 2i = \alpha\beta$, then we see that $N(\alpha)N(\beta) = N(1 \pm 2i) = 5$. So, we may assume that $N(\alpha) = 1$ and $N(\beta) = 5$. Then, $N(\alpha) = \alpha\overline{\alpha}$ implies that α is a unit. Thus, this implies that $1 \pm 2i$ are all irreducible elements in $\mathbb{Z}[i]$, hence prime elelments in $\mathbb{Z}[i]$. □

Problem 64 (11A·4). Find an inverse of $(1 + x)^3$ in $\mathbb{F}_2[[x]]$.

Proof. Note that $(1 + x)^3 = 1 + x + x^2 + x^3$. Let $f(x) = \sum_{i=0}^{\infty} b_i x^i \in \mathbb{F}_2[[x]]$, with $b_i \in \mathbb{F}_2$. By requiring $(1 + x)^3 f(x) = 1$, we see that

$$b_0 + (b_0 + b_1)x + (b_0 + b_1 + b_2)x^2 + \sum_{j=3}^{\infty}\left(\sum_{i=j-3}^{j} b_i\right)x^j = 1.$$

Thus, we obtain

$$\begin{cases} b_{4n} = 1 \\ b_{4n+1} = 1 \\ b_{4n+2} = 0 \\ b_{4n+3} = 0 \end{cases} \quad \text{with } n \in \mathbb{N}.$$

Thus, $f(x) = 1 + x + x^4 + x^5 + x^8 + x^9 + \cdots + x^{4n} + x^{4n+1} + \cdots = (1+x)(1 + x^4 + x^8 + \cdots)$, i.e. $(1+x)\sum_{n=0}^{\infty} x^{4n}$ is the inverse of $(1+x)^3$. □

Remark. Another way: Note that in $\mathbb{F}_2[[x]]$

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

and that

$$(1-x)\sum_{n=0}^{\infty} x^n = 1.$$

We see that

$$(1-x^4)\sum_{n=0}^{\infty} x^{4n} = 1.$$

So, we see that

$$(1+x)^3\left[(1+x)\sum_{n=0}^{\infty} x^{4n}\right] = \frac{1-x^4}{1+x}(1+x)\sum_{n=0}^{\infty} x^{4n} = (1-x^4)\sum_{n=0}^{\infty} x^{4n} = 1.$$

Problem 65 (12J·2). Let R be a commutative ring with 1_R, and let $X = \{f_i : i \in I\}$ be a subset of R such that the ideal generated by X is the unit ideal $\langle 1_R \rangle = R$.

a) Show that a finite number of elements of X generate the unit ideal.

b) Say $f_1, \cdots, f_k \in X$ generate the unit ideal. Show that $f_1^{n_1}, \cdots, f_k^{n_k}$ generate the unit ideal for $n_1, \cdots, n_k$ fixed positive integers.

c) Denote by R_ℓ the localization of R at the multiplicative set $S_\ell = \{1_R, f_\ell, f_\ell^2, f_\ell^3, \cdots\}$, i.e. $R_\ell = S_\ell^{-1}R$, and let $\varphi_\ell : R \to R_\ell$ be the canonical homomorphism. Consider two elements a and a' of R and suppose $\varphi_\ell(a) = \varphi_\ell(a')$ for $1 \leqslant \ell \leqslant k$. Show $a = a'$. (We are assuming as in *b*) that $f_1, \cdots, f_k$ generate the unit ideal.)

Proof. (*a*) Recall that

$$\langle X \rangle = \left\{ \sum_{i \in J} a_i f_i : \text{ for some finite subset } J \subseteq I \text{ with } a_i \in R \right\}.$$

Since $\langle X \rangle = R = \langle 1_R \rangle$, we have $1_R \in \langle X \rangle$. Thus, there exists some $a_1, \cdots, a_n \in R$ such that $1 = a_1 f_{i_1} + \cdots + a_n f_{i_n}$. Then, we see that $\langle f_{i_1}, \cdots, f_{i_n} \rangle = \langle 1_R \rangle = R$.

(*b*) For any ideal I in R, we define the set

$$\mathcal{V}(I) = \{\text{prime ideals } \mathfrak{p} \subseteq R : I \subseteq \mathfrak{p}\}.$$

We denote $\mathcal{V}(I)$ by $\mathcal{V}(f_1, \cdots, f_n)$ if $I = \langle f_1, \cdots, f_n \rangle$. We now show that $\mathcal{V}(I) \cap \mathcal{V}(J) = \mathcal{V}(I+J)$. Indeed, if $\mathfrak{p} \in \mathcal{V}(I) \cap \mathcal{V}(J)$, then $\mathfrak{p} \supset I$ and $\mathfrak{p} \supset J$, and so $\mathfrak{p} \supset I + J$, i.e. $\mathcal{V}(I) \cap \mathcal{V}(J) \subseteq \mathcal{V}(I+J)$. Conversely, if $\mathfrak{p} \in \mathcal{V}(I+J)$, then $\mathfrak{p} \supseteq I + J \supseteq I$ and $\mathfrak{p} \supseteq I + J \supseteq J$, i.e. $\mathfrak{p} \in \mathcal{V}(I) \cap \mathcal{V}(J)$.

Since $\langle f_1, \cdots, f_k \rangle = \langle 1_R \rangle$, we see that $\mathcal{V}(f_1, \cdots, f_k) = \mathcal{V}(\langle 1_R \rangle) = \varnothing$. By the above discussion and induction, we see that $\mathcal{V}(f_1, \cdots, f_k) = \mathcal{V}(\langle f_1 \rangle + \cdots + \langle f_k \rangle) = \bigcap_{i=1}^{k} \mathcal{V}(f_i)$. Note that for any prime ideal $\mathfrak{p}$, we have $f_i \in \mathfrak{p}$ if and only if $f_i^{n_i} \in \mathfrak{p}$, we conclude that $\mathcal{V}(f_i) = \mathcal{V}(f_i^{n_i})$. Thus,

$$\mathcal{V}(f_1^{n_1}, \cdots, f_k^{n_k}) = \bigcap_{i=1}^{k} \mathcal{V}(f_i^{n_i}) = \bigcap_{i=1}^{k} \mathcal{V}(f_i) = \mathcal{V}(f_1, \cdots, f_k) = \varnothing.$$

It follows that $\langle f_1^{n_1}, \cdots, f_k^{n_k} \rangle = \langle 1_R \rangle = R$ as any proper ideal must be contained in a maximal ideal, which is of course prime.

(c) Since $\varphi_\ell(a) = \varphi_\ell(a')$, we have $(a-a')f_\ell^{n_\ell} = 0$ for some $n_\ell \in \mathbb{N}$. By b), we see that $f_1^{n_1}, \cdots, f_k^{n_k}$ generate the unit ideal, so there exist $a_1, \cdots, a_k \in R$ such that $1 = a_1 f_1^{n_1} + \cdots + a_k f_k^{n_k}$. Thus, $a - a' = a_1(a-a')f_1^{n_1} + \cdots + a_k(a-a')f_k^{n_k} = 0$ as $(a-a')f_\ell^{n_\ell} = 0$ for $1 \leqslant \ell \leqslant k$. Thus, $a = a'$ as desired. □

Problem 66 (12J·8). Let R be a commutative ring with 1_R, and let $I \subsetneq R$ be a proper ideal. Show that there exists a minimal prime ideal P over I, i.e. a prime ideal P such that $I \subseteq P$ and such that there does not exist another prime ideal P' with $I \subseteq P' \subsetneq P$.

Proof. Let $S = \{\mathfrak{p} \subsetneq R : \mathfrak{p} \text{ is a prime ideal such that } I \subseteq \mathfrak{p}\}$. Define a partial order on S by $\mathfrak{p} \geqslant \mathfrak{q}$ if and only if $\mathfrak{p} \subseteq \mathfrak{q}$. Let $T = \{\mathfrak{q}_j : j \in J\}$ be a totally-ordered subset of S. Let $\mathfrak{q} = \bigcap_{j \in J} \mathfrak{q}_j$, then $\mathfrak{q}$ is an proper ideal of R. We now show that $\mathfrak{q}$ is also prime. Suppose $ab \in \mathfrak{q}$, and $a \notin \mathfrak{q}$, i.e. there exists $q_i \in T$ such that $a \notin \mathfrak{q}_i$. So $b \in \mathfrak{q}_i$. Then, for all $\mathfrak{q}_j \subseteq \mathfrak{q}_i$, we have $a \notin \mathfrak{q}_j$. So, $b \in \mathfrak{q}_j$ for all $\mathfrak{q}_j \subseteq \mathfrak{q}_i$. Thus, we have $b \in \bigcap_{j \in J} \mathfrak{q}_j = \mathfrak{q}$. Thus, $\mathfrak{q}$ is also a prime ideal. Since $I \subseteq \mathfrak{q}_j$ for all $j \in I$ by the hypothesis, we see that $I \subseteq \bigcap_{j \in J} \mathfrak{q}_j = \mathfrak{q}$. Thus, $\mathfrak{q} \in S$. Since $\mathfrak{q} \subseteq \mathfrak{q}_i$ for all i, we see that $\mathfrak{q} \geqslant \mathfrak{q}_i$ for all i. Thus, $\mathfrak{q}$ is a maximal element of T. By Zorn's lemma, there exists a minimal prime ideal P over I, i.e. a prime ideal P such that $I \subseteq P$ and such that there does not exist another prime ideal P' with $I \subseteq P' \subsetneq P$. □

Problem 67 (12A·8). Let D be a unique factorization domain and suppose $\pi \in D$ is irreducible.

a) Show $P = (\pi)$ is a prime ideal.

b) Let $S = D - P$. Note $1 \in S$ and S is closed under multiplication. Show the ring $S^{-1}D$ is a principal ideal domain.

Note: $D \subseteq S^{-1}D \subseteq K$, the field of fractions of the domain D.

Proof. (a) Suppose $ab \in P = (\pi)$, then $ab = \pi t$ for some $t \in D$. Since D is a UFD, we can factorize a, b and t into products of irreducible elements as $a = a_1 \cdots a_n$, $b = b_1 \cdots b_m$ and $t = t_1 \cdots t_l$with $a_i, b_j, t_k \in D$ are all irreducible elements. So $a_1 \cdots a_n b_1 \cdots b_m = \pi t_1 \cdots t_l$. Since D is a UFD, we see that $\pi = a_i$ or b_j by the uniqueness of factorization. Thus, $\pi | a$ or $\pi | b$, i.e. $a \in P$ or $b \in P$. Thus, P is a prime ideal.

(b) Let $R = S^{-1}D$.

We claim that for any non-trivial ideal $0 \subsetneq J \subsetneq R$, we have $J \subseteq R\pi$. Take $a/s \in J$, then $a/1 = s(a/s) \in J$. Factor $a = ua_1 \cdots a_n$ into irreducible elements in D with $u \in D$ a unit and $a_i \in D$ irreducible elements, then $a/1 = (a_1/1) \cdots (a_n/1)$. If $a_i \in S$ for all $i = 1, \cdots, n$, then $a_i/1$ is a unit in R as $(a_i/1)(1/a_i) = 1$. In this case, $a/1$ is a unit in J, which forces that $J = R$. Contradiction. Thus, there exists $a_i \notin S$, i.e. $a_i \in P = (\pi)$. Thus, $a/1 \in R\pi$ and $a/s = (1/s)(a/1) \in R\pi$. This means that $J \subseteq R\pi$. Let n be the largest integer such that $\pi^n | x$ for all $x \in J$. Then, we see that $J \subseteq R\pi^n$. Thus, there exists $y/t \in J$ with $y \in D$, $t \in S$ such that $\pi^{n+1} \nmid y$. Factor y into a product of irreducible elements, i.e. $y = up_1 \cdots p_k \pi^n$ for some unit $u \in D$ and irreducible elements $p_i \in D$ and $p_i \notin (\pi)$, i.e. p_i is a unit in R. So, $\pi^n = (1/u)(1/p_1) \cdots (1/p_k)t(y/t) \in J$. Thus, $J = R\pi^n$ is a principal ideal. We conclude that $S^{-1}D$ is a principal ideal domain. □

Problem 68 (13J·3). Give examples of the following objects. Be sure to verify that your examples satisfy the desired properties.

(a) An irreducible polynomial over $\mathbb{Q}$ that is irreducible by Eisenstein's criterion for $p = 5$.

(b) A unique factorization domain that is not a principal ideal domain.

(c) A finite extension of the rational function field $\mathbb{F}_p(x)$, for p a prime, that is normal but not separable.

Proof. (a) $f(x) = x^2 - 5$. Let $p = 5$, then $p|(-5)$, $p \nmid 1$, $p^2 \nmid (-5)$. By Eisenstein's criterion, we see that f is irreducible over $\mathbb{Q}$.

(b) $R = \mathbb{Z}[x]$ is a UFD by not a PID.

(c) Let $F = \mathbb{F}_p(x)$ and $R = \mathbb{F}_p[x]$, then $\mathrm{Frac}(R) = F$. Consider $f(t) = t^p - x \in R[t]$, since x is a prime element in R and $x|(-x)$, $x \nmid 1$, $x^2 \nmid (-1)$, by Eisenstein's criterion, we see that f is irreducible over $F[t]$. Since $f'(t) = pt^{p-1} = 0$ as $\mathrm{char}(F) = p$. We see that f is not separable over F. Let y be a root of f, i.e. $y^p - x = 0$. Then, $(t-y)^p = t^p - y^p = t^p - x = 0$, i.e. $y : \sqrt[p]{x}$ is the only root of $t^p - x$. Thus, the splitting field of f over F is $K := F(y) = \mathbb{F}_p(x, y) = \mathbb{F}_p(y)$ is normal and $[K : F] = p$. Thus, $K = \mathbb{F}_p(y) = \mathbb{F}_p(\sqrt[p]{x})$ is a finite extension of $\mathbb{F}_p(x)$ which is normal but not separable. □

Problem 69 (13A·1). Let R be a commutative ring with $1 \neq 0$, and suppose that for every $r \in R$ there is some $n > 1$ (depending on r) so that $r^n = r$. Prove that every prime ideal of R is maximal.

Proof. Let $\mathfrak{p}$ be a prime ideal of R. Denote by $\bar{r}$ the residue of r in $R/\mathfrak{p}$, i.e. $\bar{r} := r + \mathfrak{p}$. Suppose that $r \notin \mathfrak{p}$, i.e. $\bar{r} \neq 0$. Then, there exists some $n > 1$ such that $r^n = r$, so $\bar{r}^n = (r + \mathfrak{p})^n = r^n + \mathfrak{p} = r + \mathfrak{p} = \bar{r}$. Thus, $\bar{r}(\bar{r}^{n-1} - 1) = 0$. Since $R/\mathfrak{p}$ is a domain, we see that $\bar{r}^{n-1} - 1 = 0$, i.e. $\bar{r}^{n-1} = 1$ as $\bar{r} \neq 0$. Thus, $\bar{r}$ is a unit in $R/\mathfrak{p}$, which implies that $R/\mathfrak{p}$ is a field. Thus, $\mathfrak{p}$ is a maximal ideal in R. □

Problem 70 (13A·4). Let R be a unique factorization domain.

(a) Show that π is irreducible in R if and only if the ideal (π) in R is a prime ideal.

(b) Let $\pi \in R$ be irreducible, and suppose that $Q \subseteq (\pi)$ is a non-zero prime ideal. Show that $Q = (\pi)$. (Hint: Show that Q can be generated by irreducible elements.)

Proof. (a) $\Rightarrow$: Let $ab \in (\pi)$, then $ab = \pi t$ for some $t \in R$. Factor a, b, t into irreducible factors, i.e. $a = a_1 \cdots a_m$, $b = b_1 \cdots b_n$ and $t = t_1 \cdots t_k$. We have $a_1 \cdots a_m b_1 \cdots b_n = \pi t_1 \cdots t_k$. Since the factorization into irreducible elements is unique as R is a UFD, we see that $\pi = a_i$ or b_j. Thus, $a \in (\pi)$ or $b \in (\pi)$. Thus, (π) is a prime ideal of R.

$\Leftarrow$: Assume that $\pi \neq 0$. Suppose $\pi = ab$ with a, b non-zero non-units. Then, $ab \in (\pi)$. So, $a \in (\pi)$ or $b \in (\pi)$. We may assume that $a \in (\pi)$. Then, $a = \pi t$ for some $t \in R$. So, $\pi = ab = \pi t b$, i.e. $\pi(1 - tb) = 0$. Since R is a domain and $\pi \neq 0$, we have $1 - tb = 0$, i.e. b is a unit. Thus, π is irreducible.

(b) Argue by contradiction, we assume that $\pi \notin Q$. Take $a \in Q$, then $a \in (\pi)$. Thus, $a = \pi a_1$ for some $a_1 \in R$. So, $\pi a_1 = a_0 := a \in Q$. Since Q is a prime ideal and $\pi \notin Q$, we see that $a_1 \in Q$ and $a_1 | a_0$. Then, $a_1 = \pi a_2$ for some $a_2 \in R$ and $\pi a_2 \in Q$. So, $a_2 \in Q$ and $a_2 | a_1 | a_0$. Continue these steps, we obtain a sequence $a_0, a_1, \cdots, a_n, \cdots$ such that $a_n | a_{n-1}$ with each $a_i \in Q$. By our construction, we see that $a_n \neq a_{n+1}$ for all n. So, we see that a has infinitely many proper factors. Since R is a UFD, we can decompose $a = p_1 \cdots p_n$ as irreducible factors. This implies that a has only finitely many proper factors. Contradiction. Thus, $\pi \in Q$. □

Problem 71 (14J·3). Prove that a finite integral domain is a field. Prove that every prime ideal in a finite commutative ring is maximal.

Proof. Let $R = \{x_1, \cdots, x_n\}$ be a finite integral domain and take $y \in R - \{0\}$ arbitrarily. Consider $x_1y, \cdots, x_ny$, we see that $x_iy = x_jy \Leftrightarrow (x_i - x_j)y = 0 \Leftrightarrow x_i - x_j = 0 \Leftrightarrow x_i = x_j$. Thus, $x_1y, \cdots, x_ny$ is a permutation of $x_1, \cdots, x_n$. Thus, $R = \{x_1y, \cdots, x_ny\}$. So, $x_iy = 1$ for some i as $1 \in R$. Thus, $y \in R - \{0\}$ is a unit. Thus, R is a field.

Let R be a finite commutative ring and $\mathfrak{p}$ a prime ideal, then $R/\mathfrak{p}$ is a fintie integral domain, which is a field by the above argument. So, $\mathfrak{p}$ is a maximal ideal. □

Problem 72 (14A·8). Let R be a commutative ring that satisfies the descending chain condition on ideals (i.e. for any chain of ideals $\cdots \subset I_k \subset \cdots \subset I_1$ there is a t such that $I_j = I_t$ for all $j \geqslant t$). Show that every prime ideal in R is maximal. (Hint: consider R/P for a prime ideal).

Proof. Let $\mathfrak{p}$ be a prime ideal and $A := R/\mathfrak{p}$. We claim that A also satisfies the descending chain condition on ideals. Let $\widetilde{I_1} \supset \widetilde{I_2} \supset \cdots \supset \widetilde{I_k} \supset \cdots$ be a descending chain of ideals of A. Recall that there is a one-to-one correspondence between {ideals of R containing $\mathfrak{p}$} and {ideals of $R/\mathfrak{p}$}. So, we have a descending chain $I_1 \supset I_2 \supset \cdots \supset I_k \supset \cdots$ of ideals of R that contain $\mathfrak{p}$. Moreover, $\widetilde{I_k} = I_k/\mathfrak{p}$. Since R satisfies the descending chain condition on ideals, there exists a t such that $I_j = I_t$ for all $j \geqslant t$. Thus, $\widetilde{I_j} = I_j/\mathfrak{p} = I_t/\mathfrak{p} = \widetilde{I_t}$ for all $j \geqslant t$. Thus, $A = R/\mathfrak{p}$ also satisfies the descending chain condition on ideals.

Now take $x \in A$ such that $x \neq 0$. Consider the descending chain $(x) \supset (x^2) \supset \cdots \supseteq (x^k) \supset \cdots$, we must have $(x^n) = (x^{n+1})$ for large enough n. In particular, $x^n \in (x^{n+1})$, i.e. $x^n = x^{n+1}t$ for some $t \in A$. So, $x^n(xt - 1) = 0$. Since $x \neq 0$ and A is an integral domain, we see that $xt - 1 = 0$, i.e. $xt = 1$. So, $x \in A$ is a unit. Thus, A is a field and it follows that $\mathfrak{p}$ is a maximal ideal. □

Problem 73 (15J·3). Let R be an integral domain which is noetherian (every ideal is finitely generated). Prove that, if every pair of nonzero elements $a, b \in R$ has a common divisor that can be written as an R-linear combination $xa + yb$ of a and b, for some $x, y \in R$, then R is a principal ideal domain.

Proof. We first show that if $I = (a, b)$ is generated by two elements, then I is a principal ideal. Indeed, there exists $d \in R$ such that $d|a, d|b$ and $d = xa + yb$ for some $x, y \in R$. Thus, $d \in (a, b) = I$, i.e. $(d) \subseteq I$. Since $d|a$, we see that $a \in (d)$. Similarly, $b \in (d)$. Thus, $I = (d)$. Let J be an ideal of R. Since R is noetherian, J is finitely generated, i.e. $J = (x_1, \cdots, x_n)$ for some $x_i \in R$. Then, $(x_1, \cdots, x_n) = (x_1, \cdots, x_{n-2}) + (x_{n-1}, x_n) = (x_1, \cdots, x_{n-2}) + (d_1) = (x_1, \cdots, x_{n-3}) + (d_1, x_{n-2}) = (x_1, \cdots, x_{n-3}) + (d_2) = \cdots = (x_1, d_{n-2}) = (d_{n-1})$ is principal. □

Problem 74 (15J·4). Prove that the polynomial $x^4 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$.

Proof. Let $f(x) = x^4 + x^2 + x + 1 = \frac{x^5-1}{x-1}$. Let $g(x) = f(x+1) = \frac{(x+1)^5-1}{(x+1)-1} = x^4 + \binom{5}{4}x^3 + \cdots + \binom{5}{1}$. Take $p = 5$ to be a prime in $\mathbb{Z}$. Then, we see that $p|\binom{5}{i}$ for all $1 \leqslant i \leqslant 5$, $p \nmid 1$ and $p^2 \nmid \binom{5}{1}^2$. We conclude that $g(x)$ is an irreducible polynomial over $\mathbb{Q}$ by Eisenstein's criterion. If f is reducible over $\mathbb{Q}$, then $f = pq$ for some proper factors $p, q \in \mathbb{Q}[x]$. Then $g(x) = f(x+1) = p(x+1)q(x+1)$ is a product of proper factors. Contradiction. Thus, f is irreducible over $\mathbb{Q}$. □

Problem 75 (15J·8). Let R be a commutative ring with identity, I a prime ideal of R, and S the complement of I in R. Prove that the quotient ring $S^{-1}R$ is local.

Proof. Recall that there is a bijective map

$$\{\text{prime ideals } \mathfrak{p} \text{ of } R \text{ such that } \mathfrak{p} \cap S = \varnothing\} \to \{\text{prime ideals of } S^{-1}R\}$$

given by

$$\mathfrak{p} \mapsto S^{-1}\mathfrak{p}.$$

So, for any maximal ideal J of $S^{-1}R$, we have $J = S^{-1}\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of R such that $\mathfrak{p} \cap S = \varnothing$, i.e. $\mathfrak{p} \subseteq I$. So, $J = S^{-1}\mathfrak{p} \subseteq S^{-1}I$. Thus, $S^{-1}I = J$ is a maximal ideal and it is the unique maximal ideal of $S^{-1}R$. Thus, $S^{-1}R$ is a local ring. □

Problem 76 (16J·5).
(*a*) Is $\mathbb{Z}[x]$ a UFD? Is it a PID? Is it a Euclidean domain?
(*b*) The same questions for the ring $\mathbb{Z}[x, y]$. Justify your answers.

Proof. (*a*) $\mathbb{Z}[x]$ is a UFD as $\mathbb{Z}$ is. It is not a PID as $(x, 2)$ is not principal. Indeed, if $(x, 2) = (f)$, then $x = af, 2 = bf$ for some $a, b \in \mathbb{Z}[x]$. So, f must be a non-zero unit. Thus, $(x, 2) = (f) = (1)$. However, $\mathbb{Z}[x]/(x, 2) \cong \mathbb{Z}/2\mathbb{Z}$ means that $(x, 2)$ is a maximal ideal. Contradiction.

It is not a Euclidean domain as it is not a PID.

(*b*) It is a UFD as $\mathbb{Z}[x]$ is. It is not a PID as (x, y) is not principal. Indeed, if $(x, y) = (f)$, then $x = af, y = bf$ for some $a, b \in \mathbb{Z}[x, y]$. So, f must be a non-zero unit. Thus, $(x, y) = (f) = (1)$. However, $\mathbb{Z}[x, y]/(x, y) \cong \mathbb{Z}$ means that (x, y) is a prime ideal. Contradiction. Thus, (x, y) is not a prime ideal.

It is not a Euclidean domain as it is not a PID. □

Problem 77 (16A·2). Let $f : R \to S$ be a homomorphism of commutative rings. Let P be a prime ideal of S and M a maximal ideal of S.
(*a*) Prove that $f^{-1}(P)$ is a prime ideal of R.
(*b*) If R is a subring of S, and f is the inclusion homomorphism, use (*a*) to prove that $P \cap R$ is a prime ideal of R.
(*c*) Prove that, if f is surjective, then $f^{-1}(M)$ is a maximal ideal of R.

Proof. (*a*) We first prove that $f^{-1}(P)$ is an ideal. Indeed, take $a, b \in f^{-1}(P)$, then $f(a - b) = f(a) - f(b) \in P$, i.e. $a - b \in f^{-1}(P)$. Since $f(0) = 0 \in P$, we see that $0 \in f^{-1}(P)$. Thus, $f^{-1}(P)$ is an abelian group. Let $a \in f^{-1}(P)$ and $r \in R$, then $f(ar) = f(a)f(r) \in P$ as $f(a) \in P$ and P is an ideal. Thus, $ar \in f^{-1}(P)$. So, we see that $f^{-1}(P)$ is an ideal. Suppose $ab \in f^{-1}(P)$, then $f(a)f(b) = f(ab) \in P$. Thus, $f(a) \in P$ or $f(b) \in P$, i.e. $a \in f^{-1}(P)$ or $b \in f^{-1}(P)$. Thus, $f^{-1}(P)$ is a prime ideal.

(*b*) It suffices to prove that $P \cap R = f^{-1}(P)$. Let $a \in P \cap R$, then $f(a) = a \in P \cap R \subseteq P$, i.e. $a \in f^{-1}(P)$. Let $a \in f^{-1}(P)$, then $a = f(a) \in P$. So, $a \in R \cap P$ because $f^{-1}(P) \subseteq R$.

(*c*) From (*a*) we have seen that $f^{-1}(M)$ is an ideal of R. Consider the map $g : R \to S/M$ obtained by $g = p \circ f$, where $p : S \to S/M$ is the natural quotient map. Then, g is surjective as p and f are. Since $\ker g = \{x \in R : p(f(x)) = 0\} = \{x \in R : f(x) \in M\} = f^{-1}(M)$. Thus, by the first isomorphism theorem $R/f^{-1}(M) \cong S/M$ is a field. Thus, $f^{-1}(M)$ is a maximal ideal. □

Problem 78 (16A·3). Let R be a commutative ring. Let I be an ideal of R, and let J be the ideal of $R[x]$ generated by I.
(*a*) Prove that $R[x]/J \cong (R/I)[x]$.
(*b*) Prove that if I is a prime ideal of R, then J is a prime ideal of $R[x]$.

Proof. (a) Consider the map $\pi : R[x] \to (R/I)[x]$ by

$$a_0 + a_1x + \cdots + a_nx^n \mapsto \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n,$$

where $\overline{a_i}$ is the natural image of a_i in R/I. This map is clearly sujective as $R \to R/I$ is surjective. Note that $\ker \pi = \{f \in R[x] : \text{ all coefficients of } f \text{ are in } I\} = J$. Thus, $R[x]/J \cong (R/I)[x]$.

(b) If I is a prime ideal of R, then R/I is an integral domain. Let $f, g \in (R/I)[x]$ be two non-zero elements, say $f(x) = a_nx^n + \cdots + a_1x + a_0$ and $g(x) = b_mx^m + \cdots + b_1x + b_0$. Then $a_n \neq 0$ and $b_m \neq 0$. Thus, $a_nb_m \neq 0$ in R/I as R/I is an integral domain. Thus, $fg \neq 0$ as $fg = a_nb_mx^{m+n} + \cdots + a_0b_0$. So, we see that $(R/I)[x]$ is an integral domain. So, by (a), $R[x]/J$ is an integral domain. Thus, J is a prime ideal of $R[x]$. □

Problem 79 (17J·4). Prove that every two-sided ideal of the ring $M_n(\mathbb{Z})$ of $n \times n$ matrices is of the form $M_n(k\mathbb{Z})$ for some $k \in \mathbb{N}$.

Proof. Suppose $A = (a_{ij}) \in M_n(\mathbb{Z})$ is an $n \times n$ matrix, we define $\gcd(A) = \gcd(a_{ij})$. Let I be a two-sided ideal of the ring $M_n(\mathbb{Z})$. Let J be an ideal of $\mathbb{Z}$ genrated by all $\gcd(A)$, where $A \in I$. Then, $J = k\mathbb{Z}$ for some $k \in \mathbb{N}$. Thus, we see that $k \mid \gcd(A)$, i.e. $k \mid a_{ij}$ for all i, j. So, $A \in M_n(k\mathbb{Z})$ and $I \subseteq M_n(k\mathbb{Z})$. To show the equality holds, we only need to show that $kI_n \in I$. Since $J = k\mathbb{Z}$, we can find a matrix $A \in I$ such that at least one entry of A is $\pm k$, say $a_{ij} = \pm k$. Let $E_{ij} \in M_n(\mathbb{Z})$ be the matrix with $e_{ij} = 1$ and other entries zero. Then, $E_{ii}AE_{jj} = \pm kE_{ij} \in I$. So, we see that $kE_{ij} \in I$ as $(-kE_{ij})(-I) = kE_{ij}$. Thus, for each $1 \leqslant \ell \leqslant n$, $P^{\ell,i}(kE_{ij})P_{\ell,j} = kE_{\ell\ell} \in I$, where $P^{\ell,i}$ is is the elementary matrix obtained from I_n by exchange row ℓ and row i and $P_{\ell,j}$ is the elementary matrix obtained from I_n by exchange column ℓ and column j. So, we see that $kI_n = \sum_{i=1}^{n} kE_{ii} \in I$. It follows that $M_n(k\mathbb{Z}) \subseteq I$. Therefore, we see that $I = M_n(k\mathbb{Z})$ for some $k \in \mathbb{N}$. □

Problem 80 (17J·5). Are the quotient rings $\mathbb{Z}[x]/(x^2 - 2)$ and $\mathbb{Z}[x]/(x^2 - 3)$ isomorphic?

Proof. No. Suppose there is a ring isomorphism $f : \mathbb{Z}[x]/(x^2 - 2) \to \mathbb{Z}[x]/(x^2 - 3)$. Then $f(\overline{x}) = \overline{a + bx}$ for some $a, b \in \mathbb{Z}$. Thus, $f(\overline{x^2 - 2}) = f(\overline{x})^2 - \overline{2} = (\overline{a + bx})^2 - \overline{2} = 2ab\overline{x} + (a^2 + 3b^2 - 2) = 0$. Thus, $ab = 0$ and $a^2 + 3b^2 - 2 = 0$. Thus, either $\begin{cases} a = 0 \\ 3b^2 - 2 = 0 \end{cases}$ or $\begin{cases} b = 0 \\ a^2 - 2 = 0 \end{cases}$. Both are impossible. Thus, $\mathbb{Z}[x]/(x^2 - 2)$ and $\mathbb{Z}[x]/(x^2 - 3)$ are not isomorphic as rings. □

Problem 81 (17A·3). Let K be a field. Prove that the polynomial ring $K[x]$ has infinitely many maximal ideals.

Proof. Let $p_1, \cdots, p_n \in K[x]$ be a finite collection of irreducible polynomials. Consider $f = p_1 \cdots p_n + 1$. Let p be an irreducible factor of f. Then p cannot be any of $p_1, \cdots, p_n$ because otherwise p would divide 1. Hence, no finite collection of prime polynomials exhausts the set of irreducible polynomials and so the set of irreducible polynomials is infinite. Thus, $K[x]$ has infinitely many maximal ideals. □

Problem 82 (18J·5). Determine all homomorphisms from $\mathbb{Q}$ to $\mathbb{Z}$, and all homomorphisms from $\mathbb{Z}$ to $\mathbb{Q}$.

Proof. Let $f : \mathbb{Q} \to \mathbb{Z}$ be a ring homomorphism, then $f = 0$. Otherwise, suppose $f(1) = 1$, then $1 = f(1) = f(\frac{p}{p}) = f(p)f(\frac{1}{p}) = pf(\frac{1}{p})$. So, $f(\frac{1}{p}) = \frac{1}{p} \notin \mathbb{Z}$. This is impossible.

Let $g : \mathbb{Z} \to \mathbb{Q}$ be a non-trivial ring homomorphism, then $g(1) = 1$ and so $g(n) = n$ for all $n \in \mathbb{Z}$. Thus, the trivial homomorphism and imbedding are all homomorphisms from $\mathbb{Z}$ to $\mathbb{Q}$. □

Problem 83 (18J·6). Give the definition for an element of a commutative ring R to be prime and the definition for an element of a commutative ring R to be irreducible. Prove that in a principal ideal domain every irreducible element is prime.

Proof. A non-zero non-unit element $p \in R$ is said to be prime if, whenever $p \mid ab$, then $p \mid a$ or $p \mid b$. A non-zero non-unit element $p \in R$ is said to be irreducible if, whenever $p = ab$, then a is a unit or b is a unit.

Let p be an irreducible element in a PID R. Suppose $p|ab$ with $a, b \in R$. Then, $ab = pt$ for some $t \in R$. Since R is a PID, so a UFD. We may write a, b, t as products of irreducible elements, i.e. $a = a_1 \cdots a_n$, $b = b_1 \cdots b_m$ and $t = t_1 \cdots t_r$. By the uniqueness of decomposition, we see that $p = a_i$ or b_j. Thus, $p|a$ or $p|b$. So, p is prime. □

Problem 84 (18A·3). Let $R = \mathbb{C}[x, y]/(x^3, y^3)$.

(a) Find all prime ideals of R.

(b) Show that R has a unique maximal ideal.

(c) Find all units of R.

Proof. (a) Let $\mathfrak{p}$ be a prime ideal of $\mathbb{C}[x, y]$ containing (x^3, y^3). Then $x^3 \in \mathfrak{p}$ and so $x \in \mathfrak{p}$. Similarly, $y \in \mathfrak{p}$. Thus, $\mathfrak{p} \supseteq (x, y)$. Since (x, y) is a maximal ideal of $\mathbb{C}[x, y]$, we see that $\mathfrak{p} = (x, y)$. Thus, R has exactly one prime ideal $\mathfrak{m} = \mathfrak{p}/(x^3, y^3) = (x, y)/(x^3, y^3) = (\overline{x}, \overline{y})$.

(b) This follows from (a).

(c) $R^\times = R - \mathfrak{m}$, where $\mathfrak{m}$ is the unique maximal ideal of R. □

Problem 85 (18A·4). Show that the ideal $I = (3, x^6 + 1)$ is not a prime ideal of $\mathbb{Z}[x]$. Find prime ideals $A \neq 0$ and B such that $A \subset I \subset B \subset \mathbb{Z}[x]$.

Proof. Since $\mathbb{Z}[x]/I \cong \mathbb{Z}_3[x]/(x^6 + 1)$ and $x^6 + 1 = (x^2 + 1)^3$ is not irreducible in $\mathbb{Z}_3[x]$, we see that $x^6 + 1$ is not prime in $\mathbb{Z}_3[x]$ as $\mathbb{Z}_3[x]$ is a PID. Thus, $\mathbb{Z}_3[x]/(x^6 + 1)$ is not an integral domain. Thus, I is not a prime ideal of $\mathbb{Z}[x]$.

We may take $A = (3)$, clearly A is a prime ideal of $\mathbb{Z}[x]$. Take $B = (3, x^2 + 1)$, then $I \subseteq B$ as $x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$. Note that $\mathbb{Z}[x]/B \cong \mathbb{Z}_3[x]/(x^2 + 1)$ and $x^2 + 1$ has no root in $\mathbb{Z}_3[x]$. Thus we see that $x^2 + 1$ is irreducible over $\mathbb{Z}_3$ and thus $\mathbb{Z}_3[x]/(x^2 + 1)$ is an integral domain. Thus, B is prime. □

Problem 86 (19J·4). Let R be a commutative ring with $1 \neq 0$, and let S be a nonempty subset of R such that $0 \notin S$ and $ab \in S$ whenever $a, b \in S$.

(a) Prove that there exists an ideal J of R that is maximal with respect to having empty intersection with S.

(b) Prove that J is a prime ideal.

Proof. (a) Let $X = \{J \text{ ideal of } R : J \cap S = \varnothing\}$ be a set endowed with a partial order given by $J \leqslant I \Leftrightarrow J \subseteq I$. Note that X is non-empty as $(0) \in X$. Let $\{J_i\}_{i \in I}$ be a totally-ordered subset of X. Let $J = \bigcup_{i \in I} J_i$. Then, for any $a, b \in J$, $a, b \in J_i$ for some i. Thus, $a - b \in J_i \subseteq J$. For any $r \in R$, $ra \in J_i \subseteq J$. Thus, J is an ideal. Suppose $J \cap S \neq \varnothing$. Let $a \in J \cap S$. Then, $a \in J_i$ for some $i \in I$. Thus, $a \in J_i \cap S$, which is a contradiction. Thus, $J \cap S = \varnothing$. So, $J \in X$. By Zorn's lemma, we see that X has a maximal element J.

(b) Let $ab \in J$. If $a \notin J$ and $b \notin J$, then we have $(J + Ra) \cap S \neq \varnothing$ and $(J + Rb) \cap S \neq \varnothing$. Thus, there exist $i, j \in J$ and $r, s \in R$ such that $j + ra \in S$ and $i + sb \in S$. Thus, $(j + ra)(i + sb) = ij + rai + sbj + rsab \in S$. Note that $ij \in J$, $rai \in J$, $sbj \in J$ and $rsab \in J$, we see that $J \cap S \neq \varnothing$. Contradiction. Thus, $a \in J$ or $b \in J$. Thus, J is a prime ideal. □

Problem 87 (19A·3). Let R be a ring. Let N be the subset of R consisting of all nilpotent elements. (An element $r \in R$ is nilpotent if $r^n = 0$ for some positive integer n.)

(a) Prove that if R is commutative, then N is an ideal.

(b) If R is not commutative, must N be an ideal? Prove or give a counterexample.

Proof. (a) Let $a, b \in N$, then $a^m = 0$ and $b^n = 0$ for some positive integers m, n. Then, $(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i} = 0$ since if $i < m$, then $m + n - i > n$. Since $(-b)^n = (-1)^n b^n = 0$, and $(ra)^m = r^m a^m = 0$, we see that $a - b \in N$ and $ra \in N$ for all $r \in R$. Thus, N is an ideal.

(b) No. Suppose $R = M_2(\mathbb{Z})$. Let $x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then $x^2 = 0$ and $y^2 = 0$. But, $x + y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $(x + y)^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which implies that $x + y \notin N$. Thus, N is not an ideal. □

Problem 88 (19A·4). Let R be a finite ring. Prove that if R has no zero divisors, then R is a division ring (that is, each nonzero element of R is invertible).

Proof. Let $R = \{a_1, \cdots, a_n\}$ and $x \in R - \{0\}$. Then, $\{a_1 x, \cdots, a_n x\} \subseteq R$. Note that $a_i x = a_j x \Leftrightarrow (a_i - a_j)x = 0 \Leftrightarrow a_i - a_j = 0 \Leftrightarrow a_i = a_j$. Thus, $R = \{a_1 x, \cdots, a_n x\}$. Since $1 \in R$, we see that $a_i x = 1$ for some $i = 1, 2, \cdots, n$. Thus, x has a left inverse. Similarly, x has a right inverse. So, x is invertible. □

Problem 89 (20J·2). Recall that by definition, a commutative ring R is local if R has a unique maximal ideal. Prove that a commutative ring R is local if and only if for all $r, r' \in R$, if $r + r' = 1_R$ then r or r' is a unit.

Proof. $\Rightarrow$: Suppose R is local with the maximal ideal $\mathfrak{m}$. Suppose $r + r' = 1_R$. If r and r' are both not units. Then, $(r) \subseteq \mathfrak{m}$ and $(r') \subseteq \mathfrak{m}$, i.e. $r, r' \in \mathfrak{m}$. So, we see that $1_R = r + r' \in \mathfrak{m}$. Contradiction. Thus, r or r' is a unit.

$\Leftarrow$: Suppose for all $r, r' \in R$, if $r + r' = 1_R$ then r or r' is a unit. Let $\mathfrak{m}$ be a maximal ideal. If $r \notin \mathfrak{m}$, then $\mathfrak{m} + (r) = (1_R)$. So, there exists $r' \in \mathfrak{m}, a \in R$ such that $r' + ar = 1_R$. So, ar is a unit, i.e. $bar = 1$ for some $b \in R$. So, we see that r is a unit. □

Problem 90 (20A·3). Let R be a commutative ring, and let $M \subseteq R$ be an ideal of R. We let M^2 be the ideal of R generated by the set $\{ab : a, b \in M\}$.

(a) Prove the following statement. If M is both maximal and principal, then for any ideal $I \subseteq R$ with $M^2 \subseteq I \subseteq M$, it must be the case that $I = M$ or $I = M^2$. (Hint: define and make use of an R-module homomorphism $\phi : R/M \to M/M^2$.)

(b) Give examples that show that neither of the conditions on M in part (a) can be removed.

Proof. (a) Since M is a maximal ideal, we see that R/M is a field. First we show that M/M^2 is an R/M-vector space. Indeed, we can define $(r+M) \cdot (m+M^2) := (rm+M^2)$. Then, if $r+M = s+M$ and $m + M^2 = n + M^2$, then $r - s \in M$ and $m - n \in M^2$. So, $rm - sn = rm - sm + sm - sn = (r - s)m + s(m - n) \in M^2$, i.e. $rm + M^2 = sn + M^2$. Thus, the above action is well-defined. So, M/M^2 is indeed an R/M-vector space. Since M is principal, say $M = (a)$ for some $a \in R$, then $\overline{a} := a + M^2$ is a basis for M/M^2 as an R/M-vector space. Thus, $\dim_{R/M}(M/M^2) = 1$. Similarly, we see that I/M^2 is a R/M-subspace of M/M^2. Thus, $\dim_{R/M}(I/M^2) = 0$ or 1, i.e. $I/M^2 = 0$ or M/M^2. So, we see that $I = M^2$ or M.

(b) Let $R = \mathbb{R}[x, y]$. Counterexample 1: $M = (x, y)$ is maximal but not principal. Then, $M^2 = (x^2, y^2, xy)$ and we can take $I = (x, y^2)$.

Counterexample 2: $M = (xy)$ is principal but not maximal. Then, $M^2 = (x^2y^2)$ and we can take $I = (xy^2)$. □

Problem 91 (20A·4). Let R be a unique factorization domain. Prove the following.

(a) Every non-zero element of R is contained in only finitely many principal ideals of R.

(b) For any infinite chain of principal ideals in R,

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots \subseteq (a_n) \subseteq \cdots \subseteq R,$$

there exists a positive integer s so that for all $t \geqslant s$, we have $(a_t) = (a_s)$.

Proof. (a) Let $a \in R$ be a non-zero element. Since R is a unique factorization domain, we may decompose a as

$$a = up_1 \cdots p_n$$

for some unit $u \in R$ and irreducible elements $p_1, \cdots, p_n$. Suppose $a \in (x)$ for some $x \in R$, then $a = rx$ for some $r \in R$, i.e. $up_1 \cdots p_n = rx$. So, $x = vp_{i_1} \cdots p_{i_k}$ for some $i_1, \cdots, i_k \in \{1, 2, \cdots, n\}$. Thus, $(x) = (p_{i_1} \cdots p_{i_k})$. There are only finitely many principal ideals of the form $(p_{i_1} \cdots p_{i_k})$. So, we see that every non-zero element of R is contained in only finitely many principal ideals of R.

(b) By (a), there are only finitely many principal ideals containing (a_1). Let $(a_{i_1}), \cdots, (a_{i_k})$ be all distinct principal ideals containing (a_1). Let $s = \max_{j=1}^{k} i_j$. Then, for all $t \geqslant s$, we have $(a_t) = (a_s)$. □

Problem 92 (21J·5). Let $R = \mathbb{Z}[\sqrt{-5}]$ be the ring of complex numbers of the form $a + bi\sqrt{5}$, $a, b \in \mathbb{Z}$, $i = \sqrt{-1}$. Which of the following statements are true for R?

(a) R is an integral domain.

(b) R is a Euclidian domain.

(c) R is a unique factorization domain. Justify your answers.

Proof. (a) True. Consider a norm $N : R \to \mathbb{Z}$ given by $x \mapsto x\overline{x}$, where $\overline{x} = a - b\sqrt{-5}$ if $x = a + b\sqrt{-5}$. By direct computaton, we see that N is multiplicative, i.e. $N(xy) = N(x)N(y)$ for all $x, y \in R$. So, if $xy = 0$, then $N(xy) = N(x)N(y) = 0$. Without lose of generality, we may assume that $N(x) = 0$. Let $x = a + b\sqrt{5}$, then $N(x) = a^2 - (-5b^2) = a^2 + 5b^2 = 0$. Thus, $a = b = 0$, i.e. $x = 0$. Thus, R has no zero divisors. Clearly, R is commutative with multiplicative identity 1. Thus, R is an integral domain.

(b) False. We will prove that R is not a unique factorization domain in (c). Then, R is not a Euclidian domain as Euclidian domains are all PIDs, and hence are all UFDs.

(c) False. First note that $6 = 2 \times 3$ and $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. It suffices to show that $2, 3, 1 \pm \sqrt{-5}$ are irreducible elements in R.

Suppose $2 = xy$, then $N(x)N(y) = N(xy) = N(2) = 4$. Thus, we may assume that $N(x) = 1, N(y) = 4$ or $N(x) = N(y) = 2$. If $N(x) = 1, N(y) = 4$, we see that $x = 1, -1$ and correspondingly $y = 2, -2$. If $N(x) = N(y) = 2$, then $a^2 + 5b^2 = 2$, impossible. Thus, 2 is irreducible in R. Similarly, 3 is irreducible in R.

Suppose $1 + \sqrt{-5} = xy$, then $N(x)N(y) = N(xy) = N(1 + \sqrt{-5}) = 6$. Thus, we may assume that $N(x) = 1, N(y) = 6$ or $N(x) = 2, N(y) = 3$. If $N(x) = 1, N(y) = 6$, then $x = \pm 1$ is a unit. If $N(x) = 2, N(y) = 3$, then $a^2 + 5b^2 = 2$ for some $a, b \in \mathbb{Z}$ and $c^2 + 5d^2 = 3$ for some $c, d \in \mathbb{Z}$, impossible. Thus, $1 + \sqrt{5}$ is irreducible in R. Similarly, $1 - \sqrt{-5}$ is irreducible in R.

Thus, we see that R is not a UFD. □

Problem 93 (21J·7). Prove that every nonzero nonunit in a principal ideal domain is the product of finitely many irreducible elements.

Proof. Let R be a PID. Let $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots$ be a ascending chain of principal ideals of R. Then, $I := \bigcup_{i=1}^{\infty}(a_i)$ is an ideal of R. Thus, $I = (b)$ for some $b \in R$.. So, $b \in (a_s)$ for some $s \in \mathbb{N}$, i.e. $(b) \subseteq (a_s)$. Since $(a_s) \subseteq I = (b)$, we see that $(a_s) = (b)$. Thus, for all $t \geqslant s$, we have $(a_t) = (a_s) = (b)$.

Argue by contradiction, we assume $a \in R$ is an non-zero element that cannot be written as a product of finitely many irreducible elements. In particular, a is not irreducible, i.e. there exist $a_1, b_1 \in R$ such that $a = a_1 b_1$ with $(a) \subsetneq (a_1)$ and $(a) \subseteq (b_1)$. If both a_1 and b_1 can be factored as a product of finitely many irreducible elements, then a is a product of finitely many irreducible elements. Thus, we may assume that a_1 cannot be written as a product of finitely many irreducible elements. Therefore, we have

$$(a) \subsetneq (a_1)$$

and a_1 cannot be factored as a product of finitely many irreducible elements.

Iterating this argument constructs an infinitely increasing chain

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$$

This is a contradiction. Thus, every non-zero element is a product of finitely many irreducible elements. □

3 Modules

Problem 94 (09J·7). Let R be a ring with 1. Consider R to be a left R-module via multiplication. Prove that R is a division ring if and only if R is simple as an R-module.

Proof. $\Leftarrow$: Let M be a non-zero left R-submodule of R. Then there exists $x \in M \subseteq R$ such that $x \neq 0$. Since R is a division ring, there exists $y \in R$ such that $yx = 1$. So, $1 = yx \in M$ as M is left R-module. Thus, $M = R$. We conclude that R is simple as an R-module.

$\Rightarrow$: For any non-zero element $x \in R$, Rx is left R-submodule of R. Since R is simple, we see that $Rx = R$ as $Rx \neq 0$. Thus, there exists $y \in R$ such that $yx = 1$. Thus, x is invertible in R. Therefore, R is a division ring. □

Problem 95 (09A·6). Let R be a ring with $1 \neq 0$ and M an R-module. Let

$$T(M) = \{m \in M | rm = 0 \text{ for some nonzero } r \in R\},$$

$$A(M) = \{r \in R | rm = 0 \text{ for all } m \in M\}.$$

(a) Prove that $A(M)$ is a left ideal of R.

(b) If R is commutative, prove that $T(M)$ is an R-submodule of M.

(c) Give an example, with explanation, of a ring R and an R-module M such that $T(M)$ is not an R-submodule of M. (Hint: consider the R-module R, under left multiplication.)

Proof. (a) To show that $A(M)$ is a left ideal of R, we first show that $A(M)$ is an additive group. In fact, the addition is clearly associative and $0 \in A(M)$ as $0 \cdot m = 0$ for all $m \in M$; let $r, s \in A(M)$, i.e. $rm = sm = 0$ for all $m \in M$. Then, $(r + s)m = rm + sm = 0$ for all $m \in M$. Thus, $A(M)$

is closed under the addition; if $r \in A(M)$, then $(-r)m = -rm = 0$ for all $m \in M$. So, $(A(M), +)$ is an abelian group. Let $a \in A(M)$, then $am = 0$ for all $m \in M$. Thus, for any $r \in R$, we have $(ra)m = r(am) = r \cdot 0 = 0$ for all $m \in M$. Thus, $ra \in A(M)$. Thus, $A(M)$ is a left ideal of R.

(b) In fact, we require R to be an integral domain, otherwise we have a counterexample: $R = M = \mathbb{Z}/6\mathbb{Z}$, $2, 3 \in T(M)$ but $5 = 2+3 \notin T(M)$. We first show that $T(M)$ is a abelian subgroup of M. Indeed, the addition is clearly associative and $0 \in T(M)$ by definition; if $m_1, m_2 \in T(M)$, then there exist non-zero $r_1, r_2 \in R$ such that $r_1m_1 = 0$ and $r_2m_2 = 0$. So, $r_1r_2(m_1 \pm m_2) = r_2r_1m_1 \pm r_1r_2m_2 = 0$, where $r_1r_2 \neq 0$ as R is an integral domain. So, $m_1 \pm m_2 \in T(M)$. So, $(T(M), +)$ is an abelian group. Suppose $m \in T(M)$, then there exists some non-zero $s \in R$ with $sm = 0$. So, $s(rm) = r(sm) = 0$ for all $r \in R$. Thus, $rm \in T(M)$, which implies that $T(M)$ is an R-submodule of M.

(c) Let $R = M = \mathbb{Z}/6\mathbb{Z}$, then M is an R-module under left multiplication. We have $2, 3 \in T(M)$ as $2 \cdot 3 = 6 = 0$ in $\mathbb{Z}/6\mathbb{Z}$. Then, $5 = 2 + 3 \notin T(M)$ as in $\mathbb{Z}/6\mathbb{Z}$, we have $5 \cdot 5 = 25 = 1$, which implies that if there exists $r \in R$ with $r \cdot 5 = 5r = 0$, we have $r = 5 \cdot (5r) = 0$. □

Problem 96 (10J·4). An R-module M is indecomposable if there are no R-submodules $A \neq 0$ and $B \neq 0$ of M such that $M = A \oplus B$. Show that if R is a principal ideal domain then if M is indecomposable and finitely generated then either $M \cong R$ or $M \cong R/(p^n)$ for some prime element p of R.

Proof. By the classification theorem of finitely generated module over a PID, we see that

$$M \cong R^{\oplus r} \oplus R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_m^{n_m})$$

for some prime elements $p_i \in R$, $r \geqslant 0$ and $m \geqslant 0$. Since M is indecomposable, we see that either $r = 0, m = 1$ or $r = 1, m = 0$. Equivalently, $M \cong R$ or $M \cong R/(p^n)$ for some prime element p of R. □

Problem 97 (10A·2). Let M, N be modules over a ring R and $\mathrm{Hom}(M, N)$ the set of R-module homomorphisms from M to N. For any $S \subseteq M$ define:

$$A(S) = \{\phi \in \mathrm{Hom}(M, N) : \phi(S) = \{0\}\}.$$

One of the following is always true for submodules M_1, M_2 of M:
(i) $A(M_1 \cap M_2) = A(M_1) + A(M_2)$
(ii) $A(M_1 + M_2) = A(M_1) \cap A(M_2)$
Prove the true statement.

Proof. (ii) is the true statement. Let $\phi \in A(M_1+M_2)$, then $\phi(M_1+M_2) = 0$. So, $\phi(M_1) = \phi(M_2) = 0$. Thus, $\phi \in A(M_1) \cap A(M_2)$. Conversely, if $\phi \in A(M_1) \cap A(M_2)$, then $\phi(M_1) = \phi(M_2) = 0$. Let $m_1 \in M_1$ and $m_2 \in M_2$, then $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2) = 0$, so $\phi(M_1 + M_2) = 0$, i.e. $\phi \in A(M_1 + M_2)$. □

Problem 98 (10A·7). Let p be prime, $R = \mathbb{Z}_{p^n}$ the ring of integers modulo p^n, and A, B and C finitely-generated R-modules. Show that if $A \oplus B \cong A \oplus C$, then $B \cong C$.

Proof. Since R is a PID, then the result follows from the classification theorem of finitely generated modules over a PID by comparing the elementary divisors. □

Problem 99 (11J·7). An R-module M is called faithful if $rM = 0$ for $r \in R$ implies $r = 0$. Let M be a finitely generated faithful R-module and let I be an ideal of R such that $IM = M$. Prove $I = R$.

Proof. Let $x_1, \cdots, x_r \in M$ be a set of generators. Then, $x_i \in M = IM$. So,

$$x_i = \sum_{j=1}^{s} a_{ij} x_j,$$

where $a_{ij} \in I$. Equivalently,

$$\sum_{j=1}^{s} (\delta_{ij} - a_{ij}) y_j = 0$$

for all $i = 1, \cdots, s$, where $\delta_{ij} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$. Let $X = (x_1, \cdots, x_r)^T$ and $M = (a_{ij})$. Then, $(I_r - M)X = 0$. Let M' be the adjugate matrix of $I_r - M$, by Cramer's rule, we have $\det(I_r - M) = M'(I_r - A)$. Thus, we see that $\det(I_r - M)x_i = 0$ for all i. So, $\det(I_r - M) \cdot M = 0$. Since M is faithful, we see that $\det(I_r - M) = 0$. However, $\det(I_r - M) \equiv 1 \pmod{I}$. This implies that $1 \in I$. Thus, $I = R$. □

Problem 100 (11A·5). Let M be a module over a ring R,N and P submodules in M. Define $(N : P) = \{r \in R | rP < N\}$. Show that $(N : P)$ is an ideal of R. Show also that $(N : P) = \operatorname{Ann}((N + P)/N)$, where if L is an R module then $\operatorname{Ann}(L) = \{r \in R | rL = 0\}$.

Proof. Let $r, s \in (N : P)$, then $(r - s)P = rP - sP < N$. Clearly, $0 \in (N : P)$, we see that $(N : P)$ is an abelian group. Let $a \in R$ and $r \in (N : P)$, then $arP < aN < N$ as N is an R-module. Thus, $ar \in (N : P)$. So, $(N : P)$ is an ideal of R.

Let $r \in (N : P)$, $r(N + P) = rN + rP < N$, so $r \cdot \Big((N + P)/N\Big)$. Thus, we see that $r \in \operatorname{Ann}((N + P)/N)$, i.e. $(N : P) \subseteq \operatorname{Ann}((N + P)/N)$. Conversely, let $r \in \operatorname{Ann}((N + P)/N)$, then $rP \subseteq r(N + P) \subseteq N$. So, $r \in (N : P)$. Thus, $\operatorname{Ann}((N + P)/N) \subseteq (N : P)$.

Therefore, we conclude that $\operatorname{Ann}((N + P)/N) = (N : P)$. □

Problem 101 (11A·6). Let R be a commutative ring with identity, and let P and Q be projective R-modules. Prove that $P \otimes_R Q$ is a projective R-module.

Proof. Recall that P is a projective R-module if and only if P is a direct summand of some free R-module.

Suppose $P \oplus A = R^{(I)}$ and $Q \oplus B = R^{(J)}$ for some R-modules A, B and index sets I, J. Then $R^{(I \times J)} \cong R^{(I)} \otimes R^{(J)} = (P \oplus A) \otimes_R (Q \oplus B) \cong (P \otimes_R Q) \oplus (A \otimes_R Q) \oplus (P \otimes_R B) \oplus (A \otimes_R B)$. We see that $P \otimes_R Q$ is a direct summand of the free module $R^{(I \times J)}$, thus it is a projective R-module. □

Problem 102 (12J·5). Let R be a ring with identity 1_R (not necessarily commutative). Show that the following conditions on a unitary (left) R module M are equivalent.

i) M is injective.

ii) every short exact sequence $0 \to M \to B \to C \to 0$ (of unitary left R-modules) is split exact, i.e. $B \cong M \oplus C$.

Proof. $(i) \Rightarrow (ii)$: Consider the following diagram

$$\begin{tikzcd}
 & M & & & \\
0 \arrow[r] & M \arrow[u, "\mathrm{id}_M"] \arrow[r, "f"] & B \arrow[r, "g"] \arrow[ul, dotted, "h"'] & C \arrow[r] & 0
\end{tikzcd}$$

Since $f : M \to B$ is injective, the injectivity of M implies that $\mathrm{id}_M : M \to M$ can be extended to a map $h : B \to M$ such that $hf = \mathrm{id}_M$. Thus, the above short exact sequence is split exact.

$(ii) \Rightarrow (i)$: We first claim that if M is a submodule of an R-module B, then M is a direct summand of B. Indeed, consider the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "f"] & B \arrow[r, "g"] & B/M \arrow[r] & 0 \end{tikzcd}$$

By our hypothesis, there exists a section $h : B/M \to B$ with $gh = \mathrm{id}_{B/M}$. Thus, $B = M + h(B/M)$ as $\forall b$, $b = (b - hg(b)) + h(g(b))$, where $b - hg(b) \in M$. Indeed, $g(b - hg(b)) = g(b) - ghg(b) = 0$, so $b - hg(b) \in \ker g = \mathrm{Im}\ f = M$. Take $c \in M \cap h(B/M)$, then $c = h(d) \in M = \mathrm{Im}\ f = \ker g$ for some d. So, $d = gh(d) = 0$ and so $c = h(d) = 0$. Thus, $B = M \oplus h(B/M)$ as desired.

Now, recall that every R-module can be embeded into an injective R-module. So, we can embed M into an injective R-module J, then M is injective as M is a direct summand of an injective R-module. □

Problem 103 (12A·3). Let R be a commutative ring with $1_R \neq 0_R$ and let $M \neq 0$ be a simple R-module, i.e. M has no non-zero proper submodules.

a) Show that M is isomorphic as R-module to R/m for some maximal ideal $m \subseteq R$.

b) Show that if M_1, M_2 are both simple R-modules and $\varphi : M_1 \to M_2$ is an R-module homomorphism then φ is either the zero map or an isomorphism.

Proof. (a) Consider a homomorphism $\varphi : R \to M$ given by $1 \mapsto x$, where $x \neq 0$. Then, $\varphi(r) = r\varphi(1) = rx$. Since Rx is a non-zero submodule of M and M is simple, we see that $Rx = M$. Thus, φ is surjective. By the first isomorphism theorem, we see that $R/\ker\varphi \cong M$ is simple. If $\ker\varphi$ is not a maximal ideal of R, then $\ker\varphi$ is contained in some maximal ideal of R, say $\mathfrak{m}$. Then, $\mathfrak{m}/\ker\varphi$ is a proper submodule of $R/\ker\varphi$, which contradicts that $R/\ker\varphi$ is simple. Thus, $\ker\varphi$ is a maximal ideal.

(b) Consider the $\ker\varphi \subseteq M_1$, it must be 0 or M_1 as M_1 is simple.

Case I: $\ker\varphi = M_1$, then φ is the zero map.

Case II: $\ker\varphi = 0$, then φ is injective. Consider $\mathrm{Im}\ \varphi \subseteq M_2$, then $\mathrm{Im}\ \varphi = 0$ or M_2 as M_2 is simple. Since φ is injective, $\mathrm{Im}\ \varphi$ cannot be zero. So, $\mathrm{Im}\ \varphi = M_2$. Thus, φ is surjective. In this case, φ is an isomorphism. □

Problem 104 (12A·4). Let R be a commutative ring with $1_R \neq 0_R$ and $0 \to M \overset{f}{\to} N$ an exact sequence of R-modules, i.e. f is injective. Let P be a projective R-module. Show that $M \otimes_R P \overset{f\otimes 1}{\to} N \otimes_R P$ is also injective. (You may use the fact that tensor product commutes with direct sum, that is,

$$\left(\bigoplus_{i\in I} A_i\right) \otimes_R B \cong \bigoplus_{i\in I} (A_i \otimes_R B)$$

in the obvious way.)

Proof. We first prove that for any family $\{0 \to L_i \overset{f_i}{\to} M_i\}_{i\in I}$ of complexes of R-modules, we have $\forall i \in I$,

$$\begin{tikzcd} 0 \arrow[r] & L_i \arrow[r, "f_i"] & M_i \end{tikzcd}$$

is exact if and only if

$$\begin{tikzcd} 0 \arrow[r] & \bigoplus_{i\in I} L_i \arrow[r, "\bigoplus_{i\in I} f_i"] & \bigoplus_{i\in I} M_i \end{tikzcd}$$

is exact. First, suppose $\forall i \in I$,

$$\begin{tikzcd} 0 \arrow[r] & L_i \arrow[r, "f_i"] & M_i \end{tikzcd}$$

is exact. Let $(\ell_i)_{i\in I} \in \ker(\bigoplus_{i\in I} f_i)$, then $(\bigoplus_{i\in I} f_i)\big((\ell_i)_{i\in I}\big) = (f_i(\ell_i))_{i\in I} = 0$. So, $f_i(\ell_i) = 0$ for all $i \in I$, i.e. $\ell_i = 0$ for all $i \in I$ as f_i is injective for all $i \in I$. Thus, $\bigoplus_{i\in I} f_i$ is injective. Conversely, if

$$\begin{tikzcd} 0 \arrow[r] & \bigoplus_{i\in I} L_i \arrow[r, "\bigoplus_{i\in I} f_i"] & \bigoplus_{i\in I} M_i \end{tikzcd}$$

is exact, for each $i \in I$, take $\ell_i \in \ker f_i$, then $(\bigoplus_{i\in I} f_i)((\ell_i)_{i\in I}) = (f_i(\ell_i))_{i\in I} = 0$. Thus, $(\ell_i)_{i\in I} \in \ker(\bigoplus_{i\in I} f_i)$, hence $(\ell_i)_{i\in I} = 0$ as $\bigoplus_{i\in I} f_i$ is injective. We see that $\ell_i = 0$ for all $i \in I$.

We say an R-module T is **flat** if for any exact sequence $0 \to M \xrightarrow{f} N$ of R-modules, i.e. f is injective, $0 \to M \otimes_R P \xrightarrow{f\otimes 1} N \otimes_R P$ is also exact.

Note that R is flat the fact that tensor product commutes with direct sum, that is,

$$\left(\bigoplus_{i\in I} A_i\right) \otimes_R B \cong \bigoplus_{i\in I} (A_i \otimes_R B)\,.$$

We see that any free R-module is flat. Since P is a projective R-module, there exists an R-module Q such that $P \oplus Q$ is a free R-module, hence flat. Thus, we have a commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & M \otimes_R (P \oplus Q) \arrow[r, "f\otimes(1_P\oplus 1_Q)"] \arrow[d, "\cong"] & N \otimes_R (P \oplus Q) \arrow[d, "\cong"] \\ 0 \arrow[r] & (M \otimes_R P) \oplus (M \otimes_R Q) \arrow[r, "f\otimes 1_P \oplus f\otimes 1_Q"] & (N \otimes_R P) \oplus N \otimes_R Q) \end{tikzcd}$$

Thus,

$$\begin{tikzcd} 0 \arrow[r] & M \otimes_R P \arrow[r, "f\otimes 1_P"] & N \otimes_R P \end{tikzcd}$$

is exact by the discussion above. □

Problem 105 (13J·4). Let R be a commutative ring with $1 \neq 0$. Let M and N be left R-modules such that M is finitely generated and N is noetherian. Show that $M \otimes_R N$ is noetherian.

Proof. We first prove that $N^{\oplus n}$ is noetherian for all $n \in \mathbb{N}^*$ by induction on n. If $n = 1$, N is northerian by the hypothesis. Suppose for $n \leqslant k-1$, $N^{\oplus n}$ is noetherian. Consider the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & N^{\oplus k} \arrow[r] & N^{\oplus(k-1)} \arrow[r] & 0, \end{tikzcd}$$

we see that $N^{\oplus k}$ is noetherian as N and $N^{\oplus(k-1)}$ is noetherian. Thus, $N^{\oplus n}$ is noetherian for all $n \in \mathbb{N}^*$.

Since M is a finitely generated R-module, then $M \cong R^{\oplus n}/I$ for some $n \in \mathbb{N}^*$ and ideal I of R. Consider an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] & R^{\oplus n} \arrow[r] & M \arrow[r] & 0. \end{tikzcd}$$

By tensoring N, we obtain a right exact sequence

$$\begin{tikzcd}
I \otimes_R N \arrow[r] \arrow[d, equal] & R^{\oplus n} \otimes_R N \arrow[r, "\varphi"] \arrow[d, "\cong"] & M \otimes_R N \arrow[r] \arrow[d, equal] & 0 \\
I \otimes_R N \arrow[r] & N^{\oplus n} \arrow[r, "\varphi"] & M \otimes_R N \arrow[r] & 0
\end{tikzcd}$$

So, we have a exact sequence by replacing $I \otimes_R N$ with $\ker \varphi$, i.e.

$$\begin{tikzcd}
0 \arrow[r] & \ker \varphi \arrow[r] & N^{\oplus n} \arrow[r, "\varphi"] & M \otimes_R N \arrow[r] & 0
\end{tikzcd}$$

Since, $N^{\oplus n}$ is noetherian, we see that $M \otimes_R N$ is noetherian. □

Problem 106 (13J·5). Let R be a commutative ring with $1 \neq 0$, and let N be a left R-module. For a prime ideal $\mathfrak{p} \subseteq R$, let $R_\mathfrak{p}$ and $N_\mathfrak{p}$ denote their localizations at $\mathfrak{p}$. That is, $R_\mathfrak{p} = S^{-1}R$ and $N_\mathfrak{p} = S^{-1}N$, where $S = R - \mathfrak{p}$. Show that the following are equivalent:

(i) $N = \{0\}$,

(ii) $N_\mathfrak{p} = \{0\}$ for all prime ideals $\mathfrak{p} \subseteq R$,

(iii) $N_\mathfrak{m} = \{0\}$ for all maximal ideals $\mathfrak{m} \subseteq R$.

(Hint: First show that if $x \neq 0$ is an element of a module M over a commutative ring R with 1, then the set $A(x) := \{r \in R : r \cdot x = 0\}$ is an ideal of R.)

Proof. $(i) \Rightarrow (ii)$: Trivial.

$(ii) \Rightarrow (iii)$: Trivial, as maximal ideals are prime.

$(iii) \Rightarrow (i)$: Let $x \in N$ be an element of N. Consider $I := \operatorname{ann}(x) := \{r \in R : r \cdot x = 0\}$. We first show that I is an ideal of R. First, $0 \in \operatorname{ann}(x)$. Take $r, s \in \operatorname{ann}(x)$, then $(r - s)x = rx - sx = 0$, so $(r - s) \in I$. So, I is a abelian group. Let $s \in I$ and $r \in R$, we see that $(rs)x = r(sx) = r \cdot 0 = 0$, thus $rs \in I$, which means that I is an ideal. Note that

$$\begin{aligned}
x/1 = 0 \text{ in } N_\mathfrak{m} &\Leftrightarrow \exists r \in R - \mathfrak{m}, \text{ such that } rx = 0 \\
&\Leftrightarrow \exists r \in R - \mathfrak{m}, \text{ such that } r \in \operatorname{ann}(x) \\
&\Leftrightarrow \exists r \in \operatorname{ann}(x), \text{ such that } r \notin \mathfrak{m} \\
&\Leftrightarrow \operatorname{ann}(x) \nsubseteq \mathfrak{m}.
\end{aligned}$$

Thus, we see that $\operatorname{ann}(x) \subseteq \mathfrak{m}$ for all maximal ideals $\mathfrak{m} \subseteq R$. It follows that $\operatorname{ann}(x) = R$. In particular, $1 \in \operatorname{ann}(x)$, i.e. $x = 1 \cdot x = 0$. Thus, $N = \{0\}$. □

Problem 107 (13J·8). Let R be a ring with $1 \neq 0$, and let M be a finitely generated left R-module.

(a) Suppose that M is projective as a left R-module. Then prove there exist elements $m_1, \cdots, m_k \in M$ and R-module homomorphisms $f_i : M \to R, 1 \leqslant i \leqslant k$, such that for all $m \in M$,

$$m = \sum_{i=1}^{k} f_i(m) m_i.$$

(b) Prove that the converse of (a) is true.

Proof. Suppose $m_1, \cdots, m_k$ is a set of generators of M as a left R-module. Let $e_1, \cdots, e_k$ be a basis of $R^{\oplus k}$ as a left free R-module. Consider the R-linear map

$$\varphi : R^{\oplus k} \to M$$

given by

$$e_i \mapsto m_i,$$

we obtain a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker\varphi \arrow[r] & R^{\oplus k} \arrow[r, "\varphi"] & M \arrow[r] & 0. \end{tikzcd}$$

Since M is projective, there exists a map $\phi : M \to R^{\oplus}$ such that the following commutative diagram is commutative

$$\begin{tikzcd} & & & M \arrow[dl, dotted, "\phi"'] \arrow[d, "\mathrm{id}"] & \\ 0 \arrow[r] & \ker\varphi \arrow[r] & R^{\oplus k} \arrow[r, "\varphi"] & M \arrow[r] & 0. \end{tikzcd}$$

Let $f_i : M \to R$ be the composite map of the projection map p_i and ϕ, i.e. $f_i = p_i \circ \phi$. Since $\phi(m) \in R^{\oplus k}$, we see that $\phi(m) = \sum_{j=1}^{k} a_j e_j$ for some $a_j \in R$. So, $m = \varphi \circ \phi(m) = \varphi(\sum_{j=1}^{k} a_j e_j) = \sum_{j=1}^{k} a_j \varphi(e_j) = \sum_{j=1}^{k} a_j m_j$ and $f_i(m) = p_i(\phi(m)) = p_i(\sum_{j=1}^{k} a_j e_j) = a_i$. Thus, we see that $m = \sum_{j=1}^{k} f_j(m) m_j$ for all $m \in M$.

(*b*) Let $e_1, \cdots, e_k$ be a basis of $R^{\oplus k}$ as a left free R-module. Consider the R-linear map

$$\varphi : R^{\oplus k} \to M$$

given by

$$e_i \mapsto m_i,$$

we obtain a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker\varphi \arrow[r] & R^{\oplus k} \arrow[r, "\varphi"] & M \arrow[r] & 0. \end{tikzcd}$$

Define a map $\phi : M \to R^{\oplus k}$ by $m \mapsto \sum_{j=1}^{k} f_j(m) e_j$. Then, we see that $\varphi \circ \phi(m) = \varphi\left(\sum_{j=1}^{k} f_j(m) e_j\right) = \sum_{j=1}^{k} f_j(m) \varphi(e_j) = \sum_{j=1}^{k} f_j(m) m_j = m$ for all $m \in M$. Thus, the following commutative diagram is commutative

$$\begin{tikzcd} & & & M \arrow[dl, "\phi"'] \arrow[d, "\mathrm{id}"] & \\ 0 \arrow[r] & \ker\varphi \arrow[r] & R^{\oplus k} \arrow[r, "\varphi"] & M \arrow[r] & 0. \end{tikzcd}$$

This means that the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker\varphi \arrow[r] & R^{\oplus k} \arrow[r, "\varphi"] & M \arrow[r] & 0 \end{tikzcd}$$

is split, i.e. $R^{\oplus k} \cong M \oplus \ker\varphi$. Thus, M is a direct summand of a free R-module. So, M is projective as a left R-module. □

Problem 108 (13A·5). Let R be a commutative ring with $1 \neq 0$, and let I and J be ideals of R. Show that there is an R-module isomorphism $\phi : R/I \otimes_R R/J \to R/(I+J)$ with $\phi(\overline{x} \otimes \overline{y}) = \overline{xy}$.

(Here $\overline{x}$ denotes the coset $x + I \in R/I$, and similarly $\overline{y} = y + J \in R/J$ and $\overline{xy} = xy + (I + J) \in R/(I + J)$.)

Proof. Consider a map $\varphi : R/I \times R/J \to R/(I + J)$ by $(\overline{x}, \overline{y}) \mapsto \overline{xy}$. Let $(\overline{x}, \overline{y}) = (\overline{a}, \overline{b})$, then $x - a \in I$ and $y - b \in J$. So, $xy - ab = (x - a)(y - b) + ay + xb \in IJ \subseteq I + J$. Thus, $\overline{xy} = \overline{ab}$ in $R/(I + J)$. So, φ is well-defined. Note that

$$\varphi(r\overline{x}, \overline{y}) = r\overline{xy} = r\varphi(\overline{x}, \overline{y})$$

$$\varphi(\overline{x}, r\overline{y}) = r\overline{xy} = r\varphi(\overline{x}, \overline{y})$$

$$\varphi(\overline{a} + \overline{b}, \overline{y}) = (\overline{a} + \overline{b})\overline{y} = \overline{ay} + \overline{by} = \varphi(\overline{a}, \overline{y}) + \varphi(\overline{b}, \overline{y})$$

$$\varphi(\overline{x}, \overline{a} + \overline{b}) = \overline{x}(\overline{a} + \overline{b}) = \overline{xa} + \overline{xb} = \varphi(\overline{x}, \overline{a}) + \varphi(\overline{x}, \overline{b})$$

So, φ is R-bilinear. Thus, by the universal property of tensor product, there is an R-module homomorphism

$$\phi : R/I \otimes_R R/J \to R/(I + J)$$

given by

$$\overline{x} \otimes \overline{y} \mapsto \overline{xy}.$$

Note that for all $x \in R$, we have $\phi(\overline{x} \otimes \overline{1}) = \overline{x}$, so ϕ is surjective.

Consider a map $\psi : R/(I + J) \to R/I \otimes_R R/J$ given by $\overline{x} \mapsto \overline{x} \otimes \overline{1}$. Let $\overline{x} = \overline{y}$ in $R/(I + J)$, i.e. $x - y \in I + J$. Thus, $x - y = i + j$ for some $i \in I, j \in J$. Thus, $\overline{x - y} \otimes \overline{1} = \overline{i + j} \otimes \overline{1} = \overline{i} \otimes \overline{1} + \overline{1} \otimes \overline{j} = 0$. Thus, $\overline{x} \otimes \overline{1} = \overline{y} \otimes \overline{1}$. Thus, ψ is well-defined. Thus, $\psi \circ \phi(\overline{x} \otimes \overline{y}) = \overline{xy} \otimes \overline{1} = \overline{x} \otimes \overline{y}$. Thus, $\psi \circ \phi = \text{id}$. This implies that ϕ is injective. Thus, ϕ is an R-module isomorphism as desired. □

Problem 109 (13A·7). Let R be a ring with identity $1 \neq 0$. Let M be a left R-module. You may assume that all R-modules under consideration are unitary (i.e., that $1 \cdot m = m$ for all $m \in M$).

(a) Complete the following sentence to define a projective module: "M is a projective left R-module if and only if given a _________ R-module homomorphism $g : L \to N$ and any R-module homomorphism $f : M \to N$, we have ____________________."

(b) The definition in (a) is equivalent to a number of other statements about M. Provide one of them.

(c) Show that if $M_i, i \in I$, are projective left R-modules, then the direct sum $\bigoplus_{i \in I} M_i$ is a projective left R-module.

Proof. (a) surjective

an R-module homomorphism $h : M \to L$ such that $f = g \circ h$

(b) M is a projective left R-module if and only if M is a direct summand of a free left R-module.

(c) Given a surjective R-module homomorphism $g : L \to N$ and any R-module homomorphism $f : \bigoplus_{i \in I} M_i \to N$. Let $\ell_i : M_i \to \bigoplus_{i \in I} M_i$ be the include map. Let $f_i := f \circ \ell_i$. Since M_i is projective, there exists an R-module homomorphism $h_i : M_i \to L$ for each $i \in I$ such that the following diagram is commutative:

$$\begin{tikzcd}
 & & L \arrow[d, "g"] \ , \\
M_i \arrow[r, "\ell_i"] \arrow[rru, dotted, "h_i"] & \bigoplus_{i \in I} M_i \arrow[r, "f"] & N
\end{tikzcd}$$

i.e. $g \circ h_i = f_i = f \circ \ell_i$ for each $i \in I$. Then, by the universal property of direct sum, there exists a R-module homomorphism $h : \bigoplus_{i\in I} M_i \to L$ such that $h \circ \ell_i = h_i$. Thus, $g \circ h \circ \ell_i = f \circ \ell_i$ for all $i \in I$. Thus, $g \circ h = f$ by the property of direct sum. Thus, we see that $\bigoplus_{i\in I} M_i$ is projective. □

Problem 110 (14J·4). Let R be a commutative ring. Observe that for any two R-modules M, N, the collection $\mathrm{Hom}(M, N)$ of R-module homomorphisms $\varphi : M \to N$ is naturally an R-module. Suppose that

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "e"] & M \arrow[r, "f"] & N \arrow[r, "g"] & P \arrow[r] & 0 \end{tikzcd}$$

is an exact sequence of R-modules (so that g is a surjection whose kernel is equal to the image $f(M)$ of M under f, and e is an injection whose image is the kernel of f). Let A be an R-module. Prove that the induced sequence

$$0 \longrightarrow \mathrm{Hom}(A, L) \xrightarrow{e_*} \mathrm{Hom}(A, M) \xrightarrow{f_*} \mathrm{Hom}(A, N)$$

is exact in that e_* is injective and its image is the kernel of the map f_*. Also prove that the induced sequence

$$\mathrm{Hom}(M, A) \xleftarrow{f^*} \mathrm{Hom}(N, A) \xleftarrow{g^*} \mathrm{Hom}(P, A) \longleftarrow 0$$

is exact in that g^* is injective and its image is the kernel of the map f^*.

Proof. (1) Note that $e_*(\varphi) = e \circ \varphi$. Let $e_*(\varphi) = e_*(\psi)$, i.e. $e \circ \varphi = e \circ \psi$. Then for any $a \in A$, we have $e(\varphi(a)) = e(\psi(a))$ for all $a \in A$. Since e is injective, we see that $\varphi(a) = \psi(a)$. Thus, $\varphi = \psi$, i.e. e_* is injective.

Note that $f_* \circ e_*(\varphi) = f_*(e \circ \varphi) = f \circ e \circ \varphi = 0$ for all $\varphi \in \mathrm{Hom}(A, L)$ as $\mathrm{Im}\ e = \ker f$. We see that $\mathrm{Im}\ e_* \subseteq \ker f_*$. Let $\varphi \in \ker f_* \subseteq \mathrm{Hom}(A, M)$, we see that $f \circ \varphi = 0$. Thus, $f(\varphi(a)) = 0$ for all $a \in A$. Then, $\varphi(a) \in \ker f = \mathrm{Im}\ e$. Thus, for any $a \in A$, $\varphi(a) = e(\psi(a))$ for some $\psi(a) \in L$. So, we see that we have a map $\psi : A \to L$ given by $a \mapsto \psi(a)$. Since $e(\psi(a + b)) = \varphi(a + b) = \varphi(a) + \varphi(b) = e(\psi(a)) + e(\psi(b)) = e(\psi(a) + \psi(b))$ and e is injective, we see that $\psi(a + b) = \psi(a) + \psi(b)$ for all $a, b \in A$. Similarly, $\psi(ra) = r\psi(a)$ for all $r \in R$ and $a \in A$. We see that $\psi \in \mathrm{Hom}(A, L)$. Thus, $\varphi = e \circ \psi = e_*(\psi)$ for some $\psi \in \mathrm{Hom}(A, L)$. So, $\ker f_* \subseteq \mathrm{Im}\ e_*$. Therefore, $\mathrm{Im}\ e_* = \ker f_*$ and the induced sequence

$$0 \longrightarrow \mathrm{Hom}(A, L) \xrightarrow{e_*} \mathrm{Hom}(A, M) \xrightarrow{f_*} \mathrm{Hom}(A, N)$$

is exact.

(2) Let $g^*(\varphi) = 0$ for $\varphi \in \mathrm{Hom}(P, A)$, i.e. $\varphi \circ g = 0$. So, $\varphi(g(a)) = 0$ for all $a \in N$. Since $g : N \to P$ is surjective, we see that $\varphi(p) = 0$ for all $p \in P$. Thus, $\varphi = 0$, i.e. g^* is injective.

Note that $f^* \circ g^*(\varphi) = \varphi \circ g \circ f = 0$ for all $\varphi \in \mathrm{Hom}(P, A)$ as $\mathrm{Im}\ f = \ker g$. We see that $f^* \circ g^* = 0$, i.e. $\mathrm{Im}\ g^* \subseteq \ker f^*$.

Let $\varphi \in \ker f^* \subseteq \mathrm{Hom}(N, A)$, i.e. $f^*(\varphi) = \varphi \circ f = 0$. So, $\ker g = \mathrm{Im}\ f \subseteq \ker \varphi$. Since $g : N \to P$ is surjective, for any $p \in P$, $p = g(n)$ for some $n \in N$. Define $\psi : P \to A$ by $p \mapsto \varphi(n)$. We first show that it is well-defined. Suppose $p = g(n_1) = g(n_2)$ for some $n_1, n_2 \in N$, then $g(n_1 - n_2) = 0$, i.e. $n_1 - n_2 \in \ker g \subseteq \ker \varphi$, so $\varphi(n_1) = \varphi(n_1)$. Let $p_1 = g(n_1)$, $p_2 = g(n_2)$, then $p_1 + p_2 = g(n_1 + n_2)$ and $\psi(p_1 + p_2) = \varphi(n_1 + n_2) = \varphi(n_1) + \varphi(n_2) = \psi(p_1) + \psi(p_2)$. Similarly, $\psi(rp) = r\psi(p)$ for all $r \in R$ and $p \in P$. Thus, $\psi \in \mathrm{Hom}(P, A)$. Note that $\psi(g(n)) = \varphi(n)$ for all $n \in N$, we see that $\psi \circ g = \varphi$, i.e. $\varphi = g^*(\psi) \in \mathrm{Im}\ g^*$. So, $\ker f^* \subseteq \mathrm{Im}\ g^*$.

We conclude that $\ker f^* = \text{Im } g^*$ and it follows that the induced sequence

$$\text{Hom}(M, A) \xleftarrow{f^*} \text{Hom}(N, A) \xleftarrow{g^*} \text{Hom}(P, A) \longleftarrow 0$$

is exact. □

Problem 111 (14A·5). Give an example of each of the following (no justification necessary)

(a) A polynomial $f \in \mathbb{F}[x]$ with Galois group over $\mathbb{F}$ isomorphic to $\mathbb{Z}_5$ (you may choose $\mathbb{F}$).

(b) A torsion-free $\mathbb{Z}$-module that is not free.

(c) A projective module that is not free.

(d) A torsion injective $\mathbb{Z}$-module.

Solution. (a) Take $\mathbb{F} = \mathbb{F}_2$ and $f(x) = x^5 + x^2 + 1$. Note that $f(0) = 1$, $f(1) = 1$, so we see that f has no zeros in $\mathbb{F}$. So, f is reducible if and only if f is divisible by some quadratic polynomial over $\mathbb{Z}_2$. Note that x^2, $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$ are all quadratic polynomials in $\mathbb{F}_2[x]$. One can verify that these polynomials do not divide f. Thus, f is irreducible over $\mathbb{F}$.

Let $\mathbb{E}$ be the splitting field of f up to isomorphism and α be a root of f. We claim that $\mathbb{E} = \mathbb{F}(\alpha)$. Take a root β of f such that $\beta \neq \alpha$. Then, $\mathbb{F}(\alpha) \subseteq \mathbb{F}(\alpha, \beta)$ and $\mathbb{F}(\beta) \subseteq \mathbb{F}(\alpha, \beta)$. Since $|\mathbb{F}(\alpha)| = 2^5$, we see that for any $a \in \mathbb{F}(\alpha)^\times$, $a^{2^5-1} = 1$ as $\mathbb{F}(\alpha)^\times$ is a cyclic group of order $2^5 - 1$. Thus, $a^{2^5} - a = 0$ for all $a \in \mathbb{F}(\alpha)$. Since $x^{2^5} - x$ has at most 2^5 roots over $\mathbb{F}(\alpha, \beta)$, we see that $\mathbb{F}(\alpha)$ is the set of all roots of $x^{2^5} - x$ in $\mathbb{F}(\alpha, \beta)$. Similarly, $\mathbb{F}(\beta)$ is also the set of all roots of $x^{2^5} - x$ in $\mathbb{F}(\alpha, \beta)$. Thus,

$$\mathbb{F}(\alpha) = \{a \in \mathbb{F}(\alpha, \beta) : a \text{ is a root of } x^{2^5} - x\} = \mathbb{F}(\beta).$$

Thus, we see that $\mathbb{E} = \mathbb{F}(\alpha)$. Thus, $|\text{Gal}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}] = 5$. Thus, $\text{Gal}(\mathbb{E}/\mathbb{F}) \cong \mathbb{Z}_5$.

(b) Let $M = \mathbb{Q}$ be a $\mathbb{Z}$-module. Then M is torsion-free. Assume $\mathbb{Q}$ is free over $\mathbb{Z}$, then there exists a $\mathbb{Z}$-basis $(e_i)_{i \in I}$ for $\mathbb{Q}$. Suppose $e_i = \frac{a}{b}$ and $e_j = \frac{c}{d}$, we see that $ade_j - bce_i = 0$. Thus, $(e_i)_{i \in I}$ is not $\mathbb{Z}$-linearly independent, contradiction. So, $\mathbb{Q}$ is not free over $\mathbb{Z}$.

(c) Since $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$, we see that $\mathbb{Z}_2$ is $\mathbb{Z}_6$-projective. Since $2a = 0$ for all $a \in \mathbb{Z}_2$, it is not torsion-free as a $\mathbb{Z}_6$-module. Thus, $\mathbb{Z}_2$ is not free as a $\mathbb{Z}_6$-module.

(d) Let $M = \mathbb{Q}/\mathbb{Z}$, then $\mathbb{Q}/\mathbb{Z}$ is divisible abelian group, hence an injective $\mathbb{Z}$-module. Let $\frac{a}{b} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, then $b(\frac{a}{b} + \mathbb{Z}) = a + \mathbb{Z} = \mathbb{Z}$. Thus, $\mathbb{Q}/\mathbb{Z}$ is a torsion $\mathbb{Z}$-module. □

Problem 112 (15J·7). Let A, B and C be left modules over the commutative ring R (with identity) and let

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "i"] & B \arrow[r, "p"] & C \arrow[r] & 0 \end{tikzcd}$$

be a short exact sequence (in other words i is injective R-module homomorphism, p is surjective R-module homomorphism, and $\ker(p) = \text{Im }(i)$).

Prove that there exists an R-module homomorphism $j : C \to B$ such that $pj = 1_C$ if and only if there exists an R-module homomorphism $q : B \to A$ such that $qi = 1_A$.

Proof. $\Rightarrow$: Suppose there exists an R-module homomorphism $j : C \to B$ such that $pj = 1_C$.

Let $b \in B$, then $p(b) = 1_C(p(b)) = pj(p(b))$. Thus, $jp(b) - b \in \ker p = \text{Im } i$. So, $jp(b) - b = i(a)$ for some $a \in A$. Define a map $q : B \to A$ by $b \mapsto -a$. It is well-defined because if $i(a_1) = i(a_2)$, then $a_1 = a_2$ as i is injective. Moreover, q is a homomorphism of R-modules by $jp(b) - b = i(a)$. Take $x \in A$, then $jp(i(x)) - i(x) = i(-x)$. Thus, $qi(x) = -(-x) = x$. Thus, $qi = 1_A$. Thus, there exists an R-module homomorphism $q : B \to A$ such that $qi = 1_A$.

$\Leftarrow$: Suppose there exists an R-module homomorphism $q : B \to A$ such that $qi = 1_A$.

Let $c \in C$. Since p is surjective, then there exists $b \in B$ such that $p(b) = c$. Define a map $j : C \to B$ by $c \mapsto b - iq(b)$. Then j is well-defined. Indeed, if $p(b_1) = p(b_2) = c$, then $b_1 - b_2 \in \ker p = \text{Im } i$. Thus, $b_1 - b_2 = i(a)$ for some $a \in A$. Thus, $[b_1 - iq(b_1)] - [b_2 - iq(b_2)] = (b_1 - b_2) - iq(b_1 - b_2) = i(a) - iqi(a) = 0$ as $qi = 1_A$. By definition, it is routine to check that j is a homomorphism of R-modules. Since for all $c \in C$, $pj(c) = p(b - b - iq(b)) = p(b) - piq(b) = p(b) = c$, we see that $pj = 1_C$. □

Problem 113 (15A·4). Given any ring R, and R-modules A, A', B, B', C, C', and R-module homomorphisms $f, f', g, g', \alpha, \beta, \gamma$ such that α and γ are monomorphisms and the diagram

(1)
$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0
\end{tikzcd}$$

commutes and (1) has exact top and bottom rows, please prove that β is a monomorphism.

Proof. Let $x \in \ker \beta$. Then, $\gamma(g(x)) = g'(\beta(x)) = 0$. Since γ is a monomorphism, we see that $g(x) = 0$, i.e. $x \in \ker g = \text{Im } f$. Thus, $\exists a \in A$ such that $x = f(a)$. Then, $f'(\alpha(a)) = \beta(f(a)) = \beta(x) = 0$. Thus, $\alpha(a) = 0$ as f' is injective. So, $a = 0$ as α is a monomorphism. So, $x = f(a) = 0$. So, $\ker \beta = 0$ and β is a monomorphism. □

Problem 114 (15A·7). Suppose M is a faithful R-module with the property that, if $m_1, m_2 \in M$, then either $Rm_1 = Rm_2$ or $Rm_1 \cap Rm_2 = \{0\}$. Please prove that either (i) M is irreducible or (ii) R is a field.

Proof. We will prove a stronger result that (ii) always holds. Recall that M is faithful means that $\text{ann}(M) = 0$.

We first show that for any non-zero $m \in M$, Rm is non-zero irreducible. Take a non-zero submodule $N \subseteq Rm$, and non-zero element $n \in N$. Since $Rn \cap Rm = Rn \neq 0$, we have $Rn = Rm$. Thus, $N = Rm$, i.e. Rm is irreducible. Consider a surjective map $\varphi : R \to Rm$, $r \mapsto rm$. We see that $\ker \varphi = \text{ann}(m)$, so $R/\text{ann}(m) \cong Rm$ is an irreducible R-module. So, $\text{ann}(m)$ is a maximal R-submodule of R, i.e. $\text{ann}(m)$ is a maximal ideal of R if $m \neq 0$.

We now show that for all $m, n \in M$ with $m, n \neq 0$, we have $\text{ann}(m) = \text{ann}(n)$.

Case 1: $n \in Rm$, i.e. $n = rm$ for some $r \in R$, then $\text{ann}(m) \subseteq \text{ann}(rm)$. By the maximality of $\text{ann}(m)$, we see that $\text{ann}(m) = \text{ann}(rm) = \text{ann}(n)$.

Case 2: $n \notin Rm$, then $n + m \neq 0$, otherwise $n = -m \in Rm$. Take $r \in \text{ann}(n)$, we may assume that $r \notin \text{ann}(m)$, otherwise we are done. Then $rn = 0$, and $rm = rm + rn = r(m + n) \neq 0$. Since $Rm \cap Rrm = Rrm \neq 0$, we see that $Rm = Rrm$. Similarly, $Rr(m + n) = R(m + n)$. So, $Rm = Rrm = Rr(m + n) = R(m + n)$. So, $m + n \in Rm$, i.e. there exists $s \in R$ such that $m + n = sm$. So, $n = sm - m \in Rm$. Contradiction.

So we see that for all non-zero $m, n \in M$, we have $\text{ann}(m) = \text{ann}(n)$. Thus, for any $r \in \text{ann}(m)$, we have $rn = 0$ for all non-zero $n \in M$. Clearly, $r \cdot 0 = 0$, Thus, $r \in \text{ann}(M) = 0$. So, $\text{ann}(m) = 0$. Thus, 0 is a maximal ideal of R. So, R is a field.

□

Problem 115 (16J·6). Let A be a finitely generated abelian group.

(a) If A is finite, prove that $A \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

(b) If A is infinite, prove that, for some positive integer r, $A \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathbb{Q}^r$ are isomorphic as $\mathbb{Z}$-modules.

Proof. (a) By the classification theorem of finitely generated abelian groups and the additivity of $-\otimes_{\mathbb{Z}}\mathbb{Q}$, we may assume that $A=\mathbb{Z}/n\mathbb{Z}$ for some positive integer $n\geqslant 2$.

Consider the short exact sequence

$$\begin{tikzcd}0 \arrow[r] & n\mathbb{Z} \arrow[r, "\iota"] & \mathbb{Z} \arrow[r, "p"] & A \arrow[r] & 0\end{tikzcd}$$

Tensoring with $-\otimes_{\mathbb{Z}}\mathbb{Q}$, we have a right exact sequence

$$\begin{tikzcd}n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q} \arrow[r, "\iota\otimes\mathrm{id}"] & \mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q} \arrow[r, "p\otimes\mathrm{id}"] & A\otimes_{\mathbb{Z}}\mathbb{Q} \arrow[r] & 0\end{tikzcd}$$

Since $\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q}\cong\mathbb{Q}$ and correspondingly $n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q}$ has image $n\mathbb{Q}$ in $\mathbb{Q}$, we see that $A\otimes_{\mathbb{Z}}\mathbb{Q}\cong\mathbb{Q}/n\mathbb{Q}=0$ as any $r\in\mathbb{Q}$, $r=n\cdot\frac{r}{n}\in n\mathbb{Q}$.

(b) By the classification theorem of finitely generated abelian groups, the result of (a) and the additivity of $-\otimes_{\mathbb{Z}}\mathbb{Q}$, we may assume that A is a finitely generated free abelian group. So, $A\cong\mathbb{Z}^r$ for some r as $\mathbb{Z}$-modules. Thus, $A\otimes_{\mathbb{Z}}\mathbb{Q}\cong(\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q})^r\cong\mathbb{Q}^r$. □

Problem 116 (16A·7). Show that $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module.

Proof. Suppose $\mathbb{Q}$ is a projective $\mathbb{Z}$-module. We first show that $\mathrm{Hom}(\mathbb{Q},\mathbb{Z})=0$. Indeed, take $f\in\mathrm{Hom}(\mathbb{Q},\mathbb{Z})$, then $f(1)=f(\frac{p}{p})=pf(\frac{1}{p})\in p\mathbb{Z}$ for all p. Thus, $f(1)=0$ and $f=0$.

Let I be a set of generator of $\mathbb{Q}$ as a $\mathbb{Z}$-module. Let $M=\bigoplus_{i\in I}\mathbb{Z}$. Then, we have a surjective map $M\to\mathbb{Q}$ given by $e_i\mapsto i$. Then, the induced map $\mathrm{Hom}(\mathbb{Q},M)\to\mathrm{Hom}(\mathbb{Q},\mathbb{Q})$ is sujective. Then, we see that $\mathrm{Hom}(\mathbb{Q},M)=\mathrm{Hom}(\mathbb{Q},\bigoplus_{i\in I}\mathbb{Z})\cong\bigoplus_{i\in I}\mathrm{Hom}(\mathbb{Q},\mathbb{Z})=0$. Thus, $\mathrm{Hom}(\mathbb{Q},\mathbb{Q})=0$ as the induced map $\mathrm{Hom}(\mathbb{Q},M)\to\mathrm{Hom}(\mathbb{Q},\mathbb{Q})$ is sujective. This is absurd as $\mathrm{id}_{\mathbb{Q}}\in\mathrm{Hom}(\mathbb{Q},\mathbb{Q})$.

Thus, $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module. □

Problem 117 (16A·8). Let $R=\mathbb{Z}[x]$, and consider the sequence of R-module homomorphisms

$$\begin{tikzcd}0 \arrow[r] & R \arrow[r, "f"] & R \arrow[r, "g"] & \mathbb{Z} \arrow[r] & 0\end{tikzcd}$$

where, for $P=P(x)\in R$, we define $f(P)=xP(x)$ and $g(P)=P(0)$.

Here $\mathbb{Z}$ is an R-module for the action of x on $1\in\mathbb{Z}$ given by $x\cdot 1=0$.

(a) Show that the above sequence of R-modules is exact.

(b) Does it split as an exact sequence of R-modules?

(c) Does it split as an exact sequence of abelian groups?

Proof. (a) First f is injective as $xP(x)=0$ implies that $P=0$. g is clearly surjective. Sicne $gf(P)=g(xP(x))=0$, we have $\mathrm{Im}\ f\subseteq\ker g$. We only need to show that $\ker g\subseteq\mathrm{Im}\ f$. Let $P\in\ker g$, i.e. $P(0)=0$, so $P(x)=xQ(x)$ for some $Q\in R$. Thus, $P\in\mathrm{Im}\ f$. So, the above sequence of R-modules is exact.

(b) Consider the natural imbedding $i:\mathbb{Z}\to R$, we have $g\circ i=\mathrm{id}_{\mathbb{Z}}$. Thus, the above short exact sequence admits a section $i:\mathbb{Z}\to R$. So it splits.

(c) Yes, as $\mathbb{Z}$ is a free $\mathbb{Z}$-module, and hence projective. □

Problem 118 (17J·6). Let R be a ring, and let M be a Noetherian left R-module. Suppose $\phi:M\to M$ is a surjective R-module homomorphism. Show that ϕ is an isomorphism. (Hint: Consider iterations $\phi,\phi^2=\phi\circ\phi,\phi^3=\phi\circ\phi\circ\phi$, etc..)

Proof. Since ϕ is surjective, we see that all iterations $\phi^n : M \to M$ are surjective. Thus, $\ker \phi^n$ is an R-submodule of M. Note that $\ker \phi^n \subseteq \ker \phi^{n+1}$ for all $n \geqslant 1$. We obtain a ascending chain of R-submodules of M

$$\ker \phi \subseteq \ker \phi^2 \subseteq \cdots \subseteq \ker \phi^n \subseteq \cdots$$

Since M is Noetherian, we see that there exists $N \in \mathbb{N}^*$ such that $\ker \phi^N = \ker \phi^{N+1} = \cdots$ Let $x \in \ker \phi^n$, then $x = \phi^n(y)$ for some $y \in M$ as ϕ^n is surjective. Thus, $\phi^{2n}(y) = \phi^n(x) = 0$. Thus, $y \in \ker \phi^n = \ker \phi^n$, i.e. $x = \phi^n(y) = 0$. So, $\ker \phi^n = 0$ and we see that $\ker \phi = 0$. □

Problem 119 (17J·7). Let R be an integral domain. Show that R is a field if and only if every R-module is projective. (Hint: for one direction, find an ideal I of R that is not prime and then consider R/I as an R-module.)

Proof. $\Rightarrow$: If R is a field, then every R-module is an R-vector space, which is free over R and hence it is projective.

$\Leftarrow$: Let I be a non-zero ideal of R. Then, R/I is projective. So, the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, "i"] & R \arrow[r, "\pi"] & R/I \arrow[r] & 0 \end{tikzcd}$$

splits. Thus, there exists a section $h : R/I \to R$ such that $\pi \circ h = \mathrm{id}_{R/I}$. So, we see that $\pi h(\overline{1}) = \overline{1}$, i.e. $h(\overline{1}) + I = 1 + I$. Thus, there exists $j \in I$ such that $h(\overline{1}) = 1 + j$. So, for all $r \in R$, we have $h(\overline{r}) = rh(\overline{1}) = r(1+j)$. Take $r \in I$ with $r \neq 0$, then $\overline{r} = 0$ in R/I, so $h(\overline{r}) = 0$, i.e. $r(1+j) = 0$ in R. Since R is an integral domain and $r \neq 0$, we see that $1 + j = 0$ and $j = -1$. So, $1 \in I$ and $I = R$. So, R is a field as (0) is the maximal ideal of R. □

Problem 120 (17A·5). Let R be a commutative ring, and let $I, J \subseteq R$ be ideals. Let $\varphi : R \to R/I \otimes_R R/J$ be the function defined by

$$\varphi(r) = r(\overline{1} \otimes \overline{1}), \forall r \in R.$$

(Here we are letting $\overline{1}$ denote either the coset $1 + I$ or $1 + J$, depending on the context.)

(a) Prove that φ is a surjective R-module homomorphism.

(b) Prove that the kernel of φ is $I + J$. (Hint: First show there is an R-module map $\psi : R/I \otimes_R R/J \to R/(I+J)$ such that $\psi(\overline{x} \otimes \overline{y}) = \overline{xy}$. Here as above, $\overline{x} = x + I$, $\overline{y} = y + J$, and $\overline{xy} = xy + (I+J)$.)

Proof. (a) First, φ is clearly an R-module homomorphism. An element in $R/I \otimes_R R/J$ is of the form $\sum_{i=1}^n \overline{r_i} \otimes \overline{s_i}$. Since $\sum_{i=1}^n \overline{r_i} \otimes \overline{s_i} = \sum_{i=1}^n r_i s_i(\overline{1} \otimes \overline{1}) = (\sum_{i=1}^n r_i s_i)(\overline{1} \otimes \overline{1}) = \varphi(\sum_{i=1}^n r_i s_i)$, we see that φ is sujective.

(b) Consider a map $\eta : R/I \times R/J \to R/(I+J)$ by $(\overline{x}, \overline{y}) \mapsto \overline{xy}$. Let $(\overline{x}, \overline{y}) = (\overline{a}, \overline{b})$, then $x - a \in I$ and $y - b \in J$. So, $xy - ab = (x-a)(y-b) + ay + xb \in IJ \subseteq I + J$. Thus, $\overline{xy} = \overline{ab}$ in $R/(I+J)$. So, η is well-defined. Note that

$$\eta(r\overline{x}, \overline{y}) = r\overline{xy} = r\eta(\overline{x}, \overline{y})$$

$$\eta(\overline{x}, r\overline{y}) = r\overline{xy} = r\eta(\overline{x}, \overline{y})$$

$$\eta(\overline{a} + \overline{b}, \overline{y}) = (\overline{a} + \overline{b})\overline{y} = \overline{ay} + \overline{by} = \eta(\overline{a}, \overline{y}) + \eta(\overline{b}, \overline{y})$$

$$\eta(\overline{x}, \overline{a} + \overline{b}) = \overline{x}(\overline{a} + \overline{b}) = \overline{xa} + \overline{xb} = \eta(\overline{x}, \overline{a}) + \eta(\overline{x}, \overline{b})$$

So, η is R-bilinear. Thus, by the universal property of tensor product, there is an R-module homomorphism

$$\phi : R/I \otimes_R R/J \to R/(I+J)$$

given by

$$\overline{x} \otimes \overline{y} \mapsto \overline{xy}.$$

Note that for all $x \in R$, we have $\phi(\overline{x} \otimes \overline{1}) = \overline{x}$, so ϕ is surjective.

Consider a map $\psi : R/(I+J) \to R/I \otimes_R R/J$ given by $\overline{x} \mapsto \overline{x} \otimes \overline{1}$. Let $\overline{x} = \overline{y}$ in $R/(I+J)$, i.e. $x-y \in I+J$. Thus, $x-y = i+j$ for some $i \in I, j \in J$. Thus, $\overline{x-y} \otimes \overline{1} = \overline{i+j} \otimes \overline{1} = \overline{i} \otimes \overline{1} + \overline{1} \otimes \overline{j} = 0$. Thus, $\overline{x} \otimes \overline{1} = \overline{y} \otimes \overline{1}$. Thus, ψ is well-defined. Thus, $\psi \circ \phi(\overline{x} \otimes \overline{y}) = \overline{xy} \otimes \overline{1} = \overline{x} \otimes \overline{y}$. Thus, $\psi \circ \phi = \text{id}$. This implies that ϕ is injective. Thus, $\ker \varphi = \ker(\phi \circ \varphi)$. Note that $\phi \circ \varphi : R \to R/(I+J)$ is given by $r \mapsto r + (I+J)$, we see that $\ker \varphi = \ker(\phi \circ \varphi) = I + J$. □

Problem 121 (17A·6). Let R be a commutative ring, let P and F be left R-modules, and let

$$\text{Hom}_R(P, F) = \{f : P \to F | f \text{ is an } R\text{-module homomorphism}\}.$$

(a) For $r \in R$ and $f \in \text{Hom}_R(P, F)$, show that the function $rf : P \to F$ defined by $(rf)(x) := f(rx)$, for $x \in P$, is an R-module homomorphism. Show that this makes $\text{Hom}_R(P, F)$ into a well-defined left R-module.

(b) Assume further that both P and F are finitely generated as R-modules, that P is a projective R-module, and that F is a free R-module. Prove that $\text{Hom}_R(P, F)$ is a projective R-module.

Proof. (a) Let $f, g \in \text{Hom}_R(P, F)$, define $(f+g)(x) := f(x) + g(x)$. Then, $(f+g)(x+y) = f(x+y) + g(x+y) = f(x) + f(y) + g(x) + g(y) = (f+g)(x) + (f+g)(y)$ for all $x, y \in P$ and $(f+g)(sx) = f(sx) + g(sx) = sf(x) + sg(x) = s(f+g)(x)$ for all $s \in R$. So, $f + g \in \text{Hom}_R(P, F)$. For all $x, y \in P$, $(rf)(x+y) = f(rx+ry) = f(rx) + f(ry) = (rf)(x) + (rf)(y) = (rf)(x+y)$. For all $s \in R$, we have $(rf)(sx) = f(rsx) = rsf(x) = srf(x)$, i.e. $rf \in \text{Hom}_R(P, F)$. Thus, this makes $\text{Hom}_R(P, F)$ into a well-defined left R-module.

(b) Since P is a finitely generated projective R-module and F is finitely generated free R-module, then there exists an R-module Q such that $P \oplus Q \cong R^{\oplus m}$ and $F \cong R^{\oplus n}$. So,

$$\begin{aligned}
\text{Hom}_R(P, F) \oplus \text{Hom}_R(Q, F) &\cong \text{Hom}_R(P \oplus Q, F) \\
&\cong \text{Hom}_R(R^{\oplus m}, R^{\oplus n}) \\
&\cong \text{Hom}_R(R, R^{\oplus n})^{\oplus m} \\
&\cong \text{Hom}_R(R, R)^{\oplus mn} \\
&\cong R^{\oplus mn}
\end{aligned}$$

Thus, $\text{Hom}_R(P, F)$ is a projective R-module. □

Problem 122 (18J·1). Consider an attempt to define an $\mathbb{R}$-linear map

$$f : \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \to \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \qquad \text{or} \qquad \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C},$$

in either direction given by the formula

$$f(x \otimes y) = x \otimes y.$$

In which direction is this map well-defined? Is it then surjective? Is it injective?

Proof. Note that $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \cong \mathbb{C}$. We see that $f : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ given by the formula $f(x \otimes y) = x \otimes y$ is well-defined. Indeed, we have a map $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ given by $(x, y) \mapsto xy$, which is $\mathbb{R}$-bilinear. Thus, this map induced the map $f : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ given by $f(x \otimes y) = x \otimes y$ according to the universal property of tensor product. Since every element of $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ is of the form $x \otimes 1$, we see that $f(x \otimes 1) = x \otimes 1$. Thus, f is surjective. Note that $f(i \otimes i + 1 \otimes 1) = 0$, we see that f is not injective. □

Problem 123 (18J·2). Let R be an integral domain with field of fractions K, and let $\overline{K}$ be an algebraic closure of K. Fix $\alpha \in \overline{K}$. Suppose that $M \subseteq \overline{K}$ is a finitely generated R-submodule such that

$$\alpha M \subseteq M.$$

Prove that there is a monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$. (Hint: If M is generated over R by $m_1, \cdots, m_n$, then consider the characteristic polynomial of an $n \times n$ matrix over R that relates the two vectors

$$\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \alpha m_1 \\ \vdots \\ \alpha m_n \end{pmatrix}$$

in $\overline{K}^n$.)

Proof. Let $m_1, \cdots, m_n$ be a set of generators of M. Then, for each $1 \leqslant i \leqslant n$, we have $\alpha m_i \in M$ and

$$\alpha m_i = a_{i1} m_1 + \cdots + a_{in} m_n.$$

Let $A = (a_{ij}) \in M_n(R)$, then

$$(\alpha I - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

Multiplying the adjugate matrix of $(\alpha I - A)$ from both sides, we obtain

$$\det(\alpha I - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

That is, for each $1 \leqslant i \leqslant n$, we have $\det(\alpha I - A) m_i = 0$ in $\overline{K}$. Thus, $\det(\alpha I - A) = 0$. Note that $f(x) = \det(xI - A)$ is a monic polynomial over R and $f(\alpha) = 0$, we are done. □

Problem 124 (18J·7). Let R be a commutative ring, and let M be a noetherian R-module. Set

$$I := \{r \in R \mid \forall m \in M, rm = 0\}$$

so that I is the annihilator of M. Prove that R/I is a noetherian ring.

Proof. Since M is noetherian, it is finitely generated, say by $m_1, \cdots, m_s$. Consider an R-homomorphism $R \to M^{\oplus s}$ given by $r \mapsto (rm_1, rm_2, \cdots, rm_s)$. Then, $r \in \ker \varphi \Leftrightarrow rm_i = 0$ for all $1 \leqslant i \leqslant s \Leftrightarrow r \in I$. So, we have an injective homomorphism $\varphi : R/I \hookrightarrow M^{\oplus s}$ and R/I is isomorphic to a submodule of $M^{\oplus s}$. Since M is noetherian, then $M^{\oplus s}$ is also noetherian, and hence R/I is noetherian. □

Problem 125 (18A·5). Let R be a domain and F be its field of fractions. Prove that F is an injective R-module.

Proof. Let I be a non-zero ideal of R and $f : I \to F$ be an R-module homomorphism. Let $a = f(1) \in F$. We see that $f(x) = xf(1) = xa$. Define an R-module homomorphism $g : R \to F$ by $r \mapsto ra$. Then, we see that $g|_I = f$. Thus, f can be extended to R as an R-module homomorphism. Thus, by Baer's criterion, we see that F is an injective R-module. □

Problem 126 (18A·6). (a) Prove that every element of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ can be written in the form $x \otimes 1$ for $x \in \mathbb{Q}$.

(b) Prove that the map $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}$ generated by $a \otimes b \to ab$ is an isomorphism of additive groups.

Proof. (a) Note that $\frac{p}{q} \otimes \frac{a}{b} = \frac{pb}{qb} \otimes \frac{a}{b} = \frac{pa}{qb} \otimes \frac{b}{b} = \frac{pa}{qb} \otimes 1$. We are done.

(b) Denote the map by f. Then, $f(x \otimes 1) = x$. And if $x \otimes 1 \in \ker f$, then $x = f(x \otimes 1) = 0$. Thus, $x \otimes 1 = 0$. This means that f is injective. For any $x \in \mathbb{Q}$, we have $f(x \otimes 1) = x$. Thus, f is surjective. Thus, f is an isomorphism of additive groups. □

Problem 127 (18A·7). Let A, B, C be R-modules, where R is commutative with 1. Suppose that there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0 \end{tikzcd}.$$

(a) Show that if A and C are free R-modules, then B is a free R-module.

(b) Prove that if an ideal I of R is a free R-module, then I is principal.

(c) Suppose that R is not a PID. Show that there is an exact sequence as in part (a) where B is free but neither A nor C is free.

Proof. (a) If C is free, then it is projective. Thus, the short exact sequence splits, i.e. $B \cong A \oplus C$ is also free.

(b) Let $\{e_\lambda : \lambda \in \Lambda\}$ be a basis for I. Then $ce_\lambda = 0 \Rightarrow c = 0$ as any finite subseteq $\{e_1, \cdots, e_n\}$ is linearly independent. This means that e_λ is not a zero divisor for all $\lambda \in \Lambda$. Since $\{e_\lambda : \lambda \in \Lambda\}$ is a basis, we see that $Re_\lambda \cap Re_\mu = 0$. Thus, $e_\lambda e_\mu = 0$ as $e_\lambda e_\mu \in Re_\lambda \cap Re_\mu$. However, $e_\lambda \neq 0$ for all $\lambda \in \Lambda$, which implies that e_λ is a zero divisor. Contradiction.

(c) Take $R = \mathbb{Z}_6$, $A = \mathbb{Z}_2$, $B = \mathbb{Z}_6$ and $C = \mathbb{Z}_3$. □

Problem 128 (19J·5). Let R be a commutative ring with $1 \neq 0$, let M be an R-module, and let I be an ideal of R. Prove that $(R/I) \otimes_R M$ and M/IM are isomorphic as R-modules.

(IM denotes the R-submodule of M consisting of all finite sums of elements of the form im where $i \in I$ and $m \in M$.)

Proof. Consider the right exact sequence

$$\begin{tikzcd} I \arrow[r, "i"] & R \arrow[r, "\pi"] & R/I \arrow[r] & 0, \end{tikzcd}$$

where i is the inclusion and π the natural projection, tensor it with M and we get a right exact sequence

$$\begin{tikzcd} I \otimes_R M \arrow[r, "i\otimes 1"] & R \otimes_R M \arrow[r, "\pi\otimes 1"] & (R/I) \otimes_R M \arrow[r] & 0, \end{tikzcd}$$

Since $R \otimes_R M \cong M$ and correspondingly $I \otimes_R M$ has image IM in M, we see that $(R/I) \otimes_R M \cong M/IM$. □

Problem 129 (19J·6). Let R be a commutative ring with $1 \neq 0$.

(a) Suppose that we have the following commutative diagram of R-modules:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[d, "\gamma"] \\
A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C'
\end{tikzcd}$$

Assume that the top row is exact, and that f' is injective. Prove that the sequence

$$\ker(\alpha) \xrightarrow{f|_{\ker(\alpha)}} \ker(\beta) \xrightarrow{g|_{\ker(\beta)}} \ker(\gamma)$$

is exact.

(b) Suppose that we have the following commutative diagram of R-modules:

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[d, "\alpha_1"] & A_2 \arrow[r] \arrow[d, "\alpha_2"] & A_3 \arrow[r] \arrow[d, "\alpha_3"] & A_4 \arrow[r] \arrow[d, "\alpha_4"] & A_5 \arrow[d, "\alpha_5"] \\
B_1 \arrow[r] & B_2 \arrow[r] & B_3 \arrow[r] & B_4 \arrow[r] & B_5
\end{tikzcd}$$

Assume that both rows are exact. Which of the following statements are true, and which ones are false? (You do not need to justify your response.)

(i) If α_1 is surjective, and both α_2 and α_4 are injective, then α_3 is injective.

(ii) If α_1 is surjective, and both α_2 and α_4 are injective, then α_3 is surjective.

(iii) If α_5 is injective, and both α_2 and α_4 are surjective, then α_3 is injective.

(iv) If α_5 is injective, and both α_2 and α_4 are surjective, then α_3 is surjective.

Proof. (a) Since $g|_{\ker(\beta)} \circ f|_{\ker(\alpha)} = g \circ f = 0$ as the top row is exact, we have $\text{Im } f|_{\ker(\alpha)} \subseteq \ker g|_{\ker(\beta)}$. Take $b \in \ker g|_{\ker(\beta)}$, then we see that $b \in \ker \beta \cap \ker g$. So, $b \in \text{Im } f$, i.e. $f(a) = b$ for some $a \in A$. Then, $f'(\alpha(a)) = \beta f(a) = \beta(b) = 0$. Thus, $\alpha(a) \in \ker f' = 0$, i.e. $\alpha(a) = 0$, or $a \in \ker \alpha$. Thus, $b = f(a) \in \text{Im } f|_{\ker(\alpha)}$. We are done.

(b) (i) True.

(ii) False.

(iii) False.

(iv) True. □

Problem 130 (19A·6). Let R be a ring, and let M be an R-module. Prove that the following conditions are equivalent:

(i) Every R-submodule N of M is finitely generated.

(ii) M satisfies the ascending chain condition, that is for every sequence of R-submodules

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

of M, there is a positive integer t such that $M_s = M_t$ for all $s \geqslant t$.

Proof. (i) ⇒ (ii): Let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

be a sequence of R-submodules of M. Let $N = \bigcup_{i=1}^{\infty}$. Then N is a submodule of M and N is finitely generated. Suppose $N = (x_1, \cdots, x_r)$ for some $x_i \in N$. So, we see that $x_i \in M_{j_i}$ for some positive integer j_i. Let $j = \max_{i=1}^{r}\{j_i\}$, then $x_i \in M_j$ for all $i = 1, \cdots, r$. Thus, $M_j = N$. Thus, $M_j = M_{j+1} = \cdots$.

$(ii) \Rightarrow (i)$: Suppose M has a submodule N which is not finitely generated, say $N = (x_1, x_2, \cdots, x_n, \cdots)$ with $x_n \neq (x_1, \cdots, x_{n-1})$ for all $n \geqslant 0$. Then, we have a sequence

$$(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \cdots, x_n) \subsetneq \cdots$$

It contradicts (ii). Thus, every R-submodule N of M is finitely generated. □

Problem 131 (19A·7).

(a) Prove that $\mathbb{Q} \otimes_{\mathbb{Z}} G = 0$ for all finite abelian groups G.

(b) Find $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$. Justify your answer.

Proof. (a) Since G is a finite abelian group, every element of G has finite order. Take $r \otimes g \in \mathbb{Q} \otimes_{\mathbb{Z}} G$ where $r \in \mathbb{Q}$, $g \in G$ and the order of g is n. Then, $r \otimes g = \frac{rn}{n} \otimes g = \frac{r}{n} \otimes ng = \frac{r}{n} \otimes 0 = 0$. Since every element of $\mathbb{Q} \otimes_{\mathbb{Z}} G$ is of the form $\sum_{i=1}^{m} r_i \otimes g_i = \sum_{i=1}^{m} 0 = 0$. So, $\mathbb{Q} \otimes_{\mathbb{Z}} G = 0$.

(b) Take $\frac{a}{b} \otimes \frac{c}{d} \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$, we see that $\frac{a}{b} \otimes \frac{c}{d} = \frac{ad}{bd} \otimes \frac{c}{d} = \frac{a}{bd} \otimes \frac{cd}{d} = \frac{a}{bd} \otimes c = \frac{ac}{bd} \otimes 1$. Thus, $\sum_{i=1}^{n} r_i \otimes s_i = \sum_{i=1}^{n} r_i s_i \otimes 1 = (\sum_{i=1}^{n} r_i s_i) \otimes 1$. This implies that every element of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ has the form $r \otimes 1$. Define a map

$$\varphi : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}$$

by

$$r \otimes 1 \mapsto r.$$

We see that φ is surjective. If $\varphi(r \otimes 1) = 0$, then $r = 0$ and $r \otimes 1 = 0$. Thus, φ is injective. Thus, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$. □

Problem 132 (20J·3). Let $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ be an exact sequence of R-modules. Let $\mathrm{id}_A, \mathrm{id}_C$ denote the identity maps on A, C, respectively. Consider the following statements:

(i) There is an R-module homomorphism $\phi : C \to B$ such that $\beta \circ \phi = \mathrm{id}_C$.

(ii) There is an R-module homomorphism $\psi : B \to A$ such that $\psi \circ \alpha = \mathrm{id}_A$.

Prove that (i) implies (ii). (Note it is also true that (ii) implies (i).)

Proof. Define $\psi : B \to A$ by $b \mapsto b - \phi \circ \beta(b)$. Then, for all $b_1, b_2 \in B$, we have $\psi(b_1 + b_2) = b_1 + b_2 - \phi \circ \beta(b_1 + b_2) = b_1 + b_2 - \phi \circ \beta(b_1) - \phi \circ \beta(b_2) = \psi(b_1) + \psi(b_2)$. For any $r \in R$, $b \in B$, we have $\psi(rb) = rb - \phi \circ \beta(rb) = rb - \phi(r\beta(b)) = rb - r\phi(\beta(b)) = r(b - \phi \circ \beta(b)) = r\psi(b)$. Thus, ψ is a homomorphism of R-modules. Note that $\psi(\alpha(a)) = \alpha(a) - \phi(\beta(\alpha(a))) = \alpha(a)$ for all $a \in A$. We see that $\psi \circ \alpha = \mathrm{id}_A$. □

Problem 133 (20J·4). Let R be a commutative ring and let M be an R-module. Let $T(M)$ be the set of torsion elements of M, that is,

$$T(M) = \{m \in M \mid r \cdot m = 0 \text{ for some nonzero } r \in R\}.$$

(a) Prove that if R is an integral domain, then $T(M)$ is an R-submodule of M.

(b) Give an example of a ring R and an R-module M for which $T(M)$ is not an R-submodule of M.

(c) Let M, N be R-modules, and let $f : M \to N$ be an R-module homomorphism. Prove that $f(T(M)) \subseteq T(N)$.

Proof. (a) Let $m, n \in T(M)$, then $r \cdot m = 0$, $s \cdot n = 0$ for some non-zero $r, s \in R$. Since R is an integral domain, $rs = sr \neq 0$. So, $rs \cdot (m - n) = srm - rsn = 0$. Thus, $m - n \in T(M)$. For any $r' \in R$, we see that $r \cdot (r'm) = r'rm = 0$. Thus, $r'm \in T(M)$. So, $T(M)$ is an R-submodule of M.

(b) Let $R = M = \mathbb{Z}_6$. Since $3 \cdot 2 = 0$ and $2 \cdot 3 = 0$, we see that $2, 3 \in T(M)$. But $1 = 3 + (-2) \notin T(M)$. So, $T(M)$ is not an R-submodule of M.

(c) Let $n \in f(T(M))$, then $n = f(m)$ for some $m \in T(M)$. So, there exists non-zero $r \in R$ such that $r \cdot m = 0$. So, $r \cdot n = r \cdot f(m) = f(r \cdot m) = f(0) = 0$. Thus, $n \in T(N)$. Thus, $f(T(M)) \subseteq T(N)$. □

Problem 134 (20J·5). Let R be a commutative ring and let I, J be ideals of R. Prove that there is an R-module isomorphism $(R/I) \otimes_R (R/J) \cong R/(I + J)$.

Proof. Consider a map $\varphi : R/I \times R/J \to R/(I + J)$ by $(\overline{x}, \overline{y}) \mapsto \overline{xy}$. Let $(\overline{x}, \overline{y}) = (\overline{a}, \overline{b})$, then $x - a \in I$ and $y - b \in J$. So, $xy - ab = (x - a)(y - b) + ay + xb \in IJ \subseteq I + J$. Thus, $\overline{xy} = \overline{ab}$ in $R/(I + J)$. So, φ is well-defined. Note that

$$\varphi(r\overline{x}, \overline{y}) = r\overline{xy} = r\varphi(\overline{x}, \overline{y})$$

$$\varphi(\overline{x}, r\overline{y}) = r\overline{xy} = r\varphi(\overline{x}, \overline{y})$$

$$\varphi(\overline{a} + \overline{b}, \overline{y}) = (\overline{a} + \overline{b})\overline{y} = \overline{ay} + \overline{by} = \varphi(\overline{a}, \overline{y}) + \varphi(\overline{b}, \overline{y})$$

$$\varphi(\overline{x}, \overline{a} + \overline{b}) = \overline{x}(\overline{a} + \overline{b}) = \overline{xa} + \overline{xb} = \varphi(\overline{x}, \overline{a}) + \varphi(\overline{x}, \overline{b})$$

So, φ is R-bilinear. Thus, by the universal property of tensor product, there is an R-module homomorphism

$$\phi : R/I \otimes_R R/J \to R/(I + J)$$

given by

$$\overline{x} \otimes \overline{y} \mapsto \overline{xy}.$$

Note that for all $x \in R$, we have $\phi(\overline{x} \otimes \overline{1}) = \overline{x}$, so ϕ is surjective.

Consider a map $\psi : R/(I + J) \to R/I \otimes_R R/J$ given by $\overline{x} \mapsto \overline{x} \otimes \overline{1}$. Let $\overline{x} = \overline{y}$ in $R/(I + J)$, i.e. $x - y \in I + J$. Thus, $x - y = i + j$ for some $i \in I, j \in J$. Thus, $\overline{x - y} \otimes \overline{1} = \overline{i + j} \otimes \overline{1} = \overline{i} \otimes \overline{1} + \overline{1} \otimes \overline{j} = 0$. Thus, $\overline{x} \otimes \overline{1} = \overline{y} \otimes \overline{1}$. Thus, ψ is well-defined. Thus, $\psi \circ \phi(\overline{x} \otimes \overline{y}) = \overline{xy} \otimes \overline{1} = \overline{x} \otimes \overline{y}$. Thus, $\psi \circ \phi = \mathrm{id}$. This implies that ϕ is injective. Thus, ϕ is an R-module isomorphism as desired. □

Problem 135 (20A·6). Let R be a commutative ring, and let P and M be R-modules.

(a) Define

$$\mathrm{Hom}_R(P, R) \times M \to \mathrm{Hom}_R(P, M)$$

by $h(f, m)(p) = f(p)m$ for $f \in \mathrm{Hom}_R(P, R)$, $m \in M$, and $p \in P$. Show that h is R-bilinear.

(b) Let

$$\phi : \mathrm{Hom}_R(P, R) \otimes_R M \to \mathrm{Hom}_R(P, M)$$

be the function induced by the R-bilinear map h in part (a). Prove that if P is finitely generated and projective as an R-module, then ϕ is an R-module isomorphism. (Hint: first do the case when P is free.)

Proof. (a) (i) $h(f + g, m)(p) = (f + g)(p)m = f(p)m + g(p)m = h(f, m)(p) + h(g, m)(p)$ for all $p \in P$. Thus, $h(f + g, m) = h(f, m) + h(g, m)$ for all $f, g \in \mathrm{Hom}_R(P, R)$ and $m \in M$.

(ii) $h(f, m + n)(p) = f(p)(m + n) = f(p)m + f(p)n = h(f, m)(p) + h(f, n)(p)$ for all $p \in P$. Thus, $h(f, m + n) = h(f, m) + h(f, n)$ for all $f \in \mathrm{Hom}_R(P, R)$ and $m, n \in M$.

(iii) $rh(f,m)(p) = rf(p)m = (rf)(p)m = h(rf,m)(p)$ for all $p \in P$. Thus, $rh(f,m) = h(rf,m)$ for all $r \in R, f \in \mathrm{Hom}_R(P,R)$ and $m \in M$. Also, $rh(f,m)(p) = rf(p)m = f(p)(rm) = h(f,rm)(p)$ for all $p \in P$. Thus, $rh(f,m) = h(f,rm)$ for all $r \in R, f \in \mathrm{Hom}_R(P,R)$ and $m \in M$.

Thus, h is R-bilinear.

(b) Suppose first P is free, then there exists a R-basis $e_1,\cdots,e_n$ as P is finitely generated. Then, for any $x \in P$, there exist $a_1,\cdots,a_n$ such that $x = a_1e_1+\cdots+a_ne_n$. Define

$$f_i : P \to R$$

by $x \mapsto a_i$. We see that $f_i \in \mathrm{Hom}_R(P,R)$. For any $g \in \mathrm{Hom}_R(P,M)$, let $m_i = g(e_i)$, then $\phi(\sum_{i=1}^n f_i \otimes m_i)(x) = \sum_{i=1}^n h(f_i,m_i)(x) = \sum_{i=1}^n f_i(x)m_i = \sum_{i=1}^n a_i g(e_i) = g(\sum_{i=1}^n a_ie_i) = g(x)$ for all $x \in P$. Thus, $\phi(\sum_{i=1}^n f_i \otimes m_i) = g$. We see that ϕ is surjective.

We may define a map

$$\psi : \mathrm{Hom}_R(P,M) \to \mathrm{Hom}_R(P,R) \otimes_R M$$

by

$$g \mapsto \sum_{i=1}^n f_i \otimes g(e_i).$$

Then, we see that $\psi(\phi(f \otimes m)) = \psi(h(f,m)) = \sum_{i=1}^n f_i \otimes h(f,m)(e_i) = \sum_{i=1}^n f_i \otimes f(e_i)m = (\sum_{i=1}^n f(e_i)f_i) \otimes m = f \otimes m$ for all $f \in \mathrm{Hom}_R(P,R)$ and $m \in M$. Thus, $\psi \circ \phi = \mathrm{id}$. So, we see that ϕ is injective. Thus, ϕ is an R-module isomorphism.

For the general case, there exists a finitely generated projective R-module Q and a finitely generated free R-module F such that $P \oplus Q = F$.

For any projective R-module P, We denote by ϕ_P the map

$$\phi_P : \mathrm{Hom}_R(P,R) \otimes_R M \to \mathrm{Hom}_R(P,M)$$

induced by the R-bilinear map $h_P : \mathrm{Hom}_R(P,R) \times M \to \mathrm{Hom}_R(P,M)$, which is given by $h(f,m)(p) = f(p)m$ for $f \in \mathrm{Hom}_R(P,R)$, $m \in M$, and $p \in P$.

We then consider the following commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_R(P,R) \otimes_R M \oplus \mathrm{Hom}_R(Q,R) \otimes_R M \arrow[r, "\phi_P \oplus \phi_Q"] \arrow[d, "\cong"] & \mathrm{Hom}_R(P,M) \oplus \mathrm{Hom}_R(Q,M) \arrow[d, "\cong"] \\
\mathrm{Hom}_R(F,R) \otimes_R M \arrow[r, "\phi_F"] & \mathrm{Hom}_R(F,M)
\end{tikzcd}$$

We see that $\phi_P \oplus \phi_Q : (a,b) \mapsto (\phi_P(a), \phi_Q(b))$ is an isomorphism. Thus $\phi_P = \phi$ is also an isomorphism. □

Problem 136 (21J·6). A group G is divisible if for any $g \in G$ and positive integer n there is an $x \in G$ such that $x^n = g$ (if G is abelian group then in additive notations this means that $nx = g$).

(a) Give one example of divisible abelian groups.

(b) Prove that the direct product of divisible groups is a divisible group.

(c) Give the definition of injective R-module where R is a ring.

(d) Prove that every injective $\mathbb{Z}$-module is a divisible abelian group.

Proof. (a) $(\mathbb{Q},+)$.

(b) Let A, B be two divisible groups and $G = A \times B$. Given $(a, b) \in G$ and n a positive integer, we see that there exist $x \in A$ and $y \in B$ such that $x^n = g$ and $y^n = b$ as A and B are divisible. Thus, $(x, y)^n = (x^n, y^n) = (g, h)$. Thus, G is also divisible.

(c) An R-module J is called injective if for any given injective R-module homomorphism $g : A \to B$ and R-module homomorphism $f : A \to J$, there exists an R-module homomorphism $h : B \to J$ such that $f = h \circ g$.

(d) Let G be an injective $\mathbb{Z}$-module. For any $g \in G$ and positive integer n, we may consider an $\mathbb{Z}$-module homomorphism $f : n\mathbb{Z} \to G$ given by $n \mapsto g$ and $i : n\mathbb{Z} \hookrightarrow \mathbb{Z}$. Then, there exists an R-module homomorphism $h : \mathbb{Z} \to G$ such that $h \circ i = f$. Thus, $nh(1) = h(n) = h \circ i(n) = f(n) = g$. Thus, if we take $x = h(1)$, we have $nx = g$. Thus, G is a divisible abelian group. □

4 Advanced Linear Algebra

Problem 137 (09J·6). Let V be a finite dimensional vector space over an algebraically closed field F, and let S and T be two linear transformations from V to V. Assume that $ST = TS$ and that the characteristic polynomial of S has distinct roots.

(a) Show that every eigenvector of S is an eigenvector of T.

(b) If T is nilpotent, show that $T = 0$.

Proof. (a) Let $p(x) \in F[x]$ be the characteristic polynomial of S. Since p has distinct roots, we may assume that $p(x) = (x - \lambda_1) \cdots (x - \lambda_n)$, where $n = \dim V$ and $\lambda_1, \cdots, \lambda_n$ are pairwisely distinct. Denote $E(\lambda_i, S)$ the eigenspace of S corresponding to λ_i. Let v_i be an eigenvector of S corresponding to λ_i, i.e. $Sv_i = \lambda_i v_i$. Recall that $v_1, \cdots, v_n$ is linearly independent as they corresponds to dinstinct eigenvalues. By counting dimension, we see that $V = Fv_1 \oplus \cdots \oplus Fv_n$. Since $V = E(\lambda_1, S) \oplus \cdots \oplus E(\lambda_n, S)$ and $Fv_i \subseteq E(\lambda_i, S)$, we have $E(\lambda_i, S) = Fv_i$. Note that $S(Tv_i) = TSv_i = T(\lambda_i v_i) = \lambda_i(Tv_i)$, we see that Tv_i is an eigenvector of S corresponding to λ_i, which implies that $Tv_i \in E(\lambda_i, S) = Fv_i$. Thus, $Tv_i = \mu_i v_i$ for some $\mu_i \in F$. So, v_i is an eigenvector of T for all $i = 1, \cdots, n$.

(b) By (a), we see that $v_1, \cdots, v_n$ are eigenvectors corresponding to $\mu_1, \cdots, \mu_n$ (not necessarily distinct), i.e. $Tv_i = \mu_i v_i$ for all $i = 1, \cdots, n$. Since T is nilpotent, there exists $k \in \mathbb{N}^*$ such that $T^k = 0$. Note that $T^k v_i = T^{k-1}(Tv_i) = T^{k-1}(\mu_i v_i) = \mu_i T^{k-1} v_i = \cdots = \mu_i^k v_i$. So, we see that T^k has $\mu_1^k, \cdots, \mu_n^k$ as its eigenvalues. Since $T^k = 0$, we see that $\mu_1^k = \cdots = \mu_n^k = 0$, i.e. $\mu_1 = \cdots = \mu_n = 0$. Thus, $Tv_i = \mu_i v_i = 0$ for all i. Notice that $v_1, \cdots, v_n$ is a basis for V, we conclude that $T = 0$. □

Problem 138 (09A·3). Find the Jordan Canonical Form J and matrix P such that $PAP^{-1} = J$ where

$$A = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 0 & 2 & 1 & 3 \end{pmatrix}$$

Proof. First, $xI - A = \begin{pmatrix} x-3 & 0 & 0 & 0 \\ -1 & x-3 & 0 & 0 \\ -1 & 0 & x-3 & 0 \\ 0 & -2 & -1 & x-3 \end{pmatrix}$. By performing elementary row and column operation, we see that $\begin{pmatrix} x-3 & 0 & 0 & 0 \\ -1 & x-3 & 0 & 0 \\ -1 & 0 & x-3 & 0 \\ 0 & -2 & -1 & x-3 \end{pmatrix} \to \begin{pmatrix} x-3 & 0 & 0 & 0 \\ 0 & x-3 & 3-x & 0 \\ -1 & 0 & x-3 & 0 \\ 0 & -2 & -1 & x-3 \end{pmatrix} \to$

$$\begin{pmatrix} 1 & 0 & 3-x & 0 \\ 0 & x-3 & 3-x & 0 \\ x-3 & 0 & 0 & 0 \\ 0 & -2 & -1 & x-3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x-3 & 3-x & 0 \\ x-3 & 0 & (x-3)^2 & 0 \\ 0 & -2 & -1 & x-3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x-3 & 3-x & 0 \\ 0 & 0 & (x-3)^2 & 0 \\ 0 & -2 & -1 & x-3 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3-x & x-3 & 0 \\ 0 & (x-3)^2 & 0 & 0 \\ 0 & -1 & -2 & x-3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -2 & x-3 \\ 0 & (x-3)^2 & 0 & 0 \\ 0 & 3-x & x-3 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & x-3 \\ 0 & -(x-3)^2 & 0 & 0 \\ 0 & x-3 & 3-x & 0 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -(x-3)^2 & 2(x-3)^2 & (x-3)^3 \\ 0 & x-3 & -3(x-3) & -(x-3)^2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2(x-3)^2 & (x-3)^3 \\ 0 & 0 & -3(x-3) & -(x-3)^2 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x-3 & \frac{1}{3}(x-3)^2 \\ 0 & 0 & 2(x-3)^2 & (x-3)^3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x-3 & 0 \\ 0 & 0 & 0 & (x-3)^3 \end{pmatrix}$$

So, we see that the invariant factors of A are $x-3$ and $(x-3)^3$ and the minimal polynomial is $(x-3)^3$. So, the elementary divisors of A are $x-3$ and $(x-3)^3$. So, the Jordan canonical form

$$J = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

To find P, let $P^{-1} = \begin{pmatrix} \xi & \eta_1 & \eta_2 & \eta_3 \end{pmatrix}$. Then,

$$A \begin{pmatrix} \xi & \eta_1 & \eta_2 & \eta_3 \end{pmatrix} = AP^{-1} = P^{-1}J = \begin{pmatrix} \xi & \eta_1 & \eta_2 & \eta_3 \end{pmatrix} \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

So, $\begin{pmatrix} A\xi & A\eta_1 & A\eta_2 & A\eta_3 \end{pmatrix} = \begin{pmatrix} 3\xi & 3\eta_1 & \eta_1 + 3\eta_2 & \eta_2 + 3\eta_3 \end{pmatrix}$. We see that

$$\begin{cases} (A-3I)\xi = 0 \\ (A-3I)\eta_1 = 0 \\ (A-3I)\eta_2 = \eta_1 \\ (A-3I)\eta_3 = \eta_2 \end{cases}$$

Thus, we can take

$$\begin{cases} \xi = \begin{pmatrix} 0 & 1 & -2 & 0 \end{pmatrix}^T \\ \eta_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^T \\ \eta_2 = \begin{pmatrix} 0 & 1/3 & 1/3 & 0 \end{pmatrix}^T \\ \eta_3 = \begin{pmatrix} 1/3 & 0 & 0 & 0 \end{pmatrix}^T \end{cases}$$

So, we may take $P^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1/3 \\ 1 & 0 & 1/3 & 0 \\ -2 & 0 & 1/3 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$. Thus, $P = \begin{pmatrix} 0 & 1/3 & -1/3 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 3 & 0 & 0 & 0 \end{pmatrix}$. □

Problem 139 (10J·2). Let $T \in \mathrm{End}(V)$ be a linear operator on a vector space V with $\dim(V) = n$ such that $\min_T(x) = \mathrm{char}_T(x)$, i.e. the minimal and characteristic polynomials of T coincide.

(a) Show that there exists an $\alpha \in V$ such that $\{\alpha, T(\alpha), \cdots, T^{n-1}(\alpha)\}$ is a basis for V.

(b) Show that if $U \in \mathrm{End}(V)$ satisfies $UT = TU$ then U is a polynomial in T.

Proof. (a) Consider V as a $k[x]$-module by $f \cdot v = f(T)v$ for all $v \in V$ and $f \in k[x]$. Then, by the classification theorem of finitely generated module over a PID, there exists an $k[x]$-module isomorphism

$$\varphi : V \cong k[x]^{\oplus r} \oplus \frac{k[x]}{(f_1)} \oplus \cdots \oplus \frac{k[x]}{(f_m)},$$

where $f_1|\cdots|f_m$ are invariant factors. Clearly, φ is a isomorphism of k-vector spaces, so by counting the dimension, we see that $r = 0$, i.e.

$$\varphi : V \cong \frac{k[x]}{(f_1)} \oplus \cdots \oplus \frac{k[x]}{(f_m)}.$$

Recall that f_m is the minimal polynomial of T and $f_1 \cdots f_m$ is the characteristic polynomial of T. Thus, $f_1 = \cdots = f_{m-1} = 1$, i.e. there exists a $k[x]$-module isomorphism

$$\varphi : V \cong k[x]/(f),$$

where $f(x) = \min_T(x) = \mathrm{char}_T(x)$. We may assume that $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$. As a k-vector space, $k[x]/(f)$ has a basis $\{1, x, x^2, \cdots, x^{n-1}\}$. Let $\alpha = \varphi^{-1}(1)$, then we see that $\varphi^{-1}(x^i) = x^i\varphi^{-1}(1) = x^i \cdot \alpha = T^i\alpha$. Since φ is also an isomorphism of k-vector spaces, we see that $\{\alpha, T\alpha, \cdots, T^{n-1}\alpha\}$ is a basis of V.

(b) By (a) there exists an $\alpha \in V$ such that $\{\alpha, T(\alpha), \cdots, T^{n-1}(\alpha)\}$ is a basis for V. So, there exists $b_0, \cdots, b_{n-1}$ such that $U\alpha = b_0\alpha + b_1T\alpha + \cdots + b_{n-1}T^{n-1}\alpha$. Let $g(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in k[x]$. Then, we see that $U\alpha = g(T)\alpha$. By induction, we can easily prove that $UT^i = T^iU$. So, $U(T^i\alpha) = UT^i\alpha = T^iU\alpha = T^ig(T)\alpha = g(T)T^i\alpha$ for all i. Since $\{\alpha, T(\alpha), \cdots, T^{n-1}(\alpha)\}$ is a basis for V, it follows that $U = g(T)$. □

Problem 140 (10A·5). Let $\mathrm{GL}(n, F)$ denote the group of invertible $n \times n$ matrices with entries in F.

(a) Show that if $A \in \mathrm{GL}(n, \mathbb{C})$ has finite order, then A is diagonalizable over $\mathbb{C}$ (that is, there is a basis for $\mathbb{C}^n$ with respect to which A is a diagonal matrix).

(*b*) Let p be a prime satisfying $p > n+1$ (so p is odd). Show that if $A \in \mathrm{GL}(n, \mathbb{Q})$ satisfies $A^p = I$, then $A = I$ (here I denotes the $n \times n$ identity matrix).

Proof. (*a*) Suppose A has order m, then $A^m = I$. Let p be the minimal polynomial of A over $\mathbb{C}$, we see that $p(x)|x^m - 1$. Thus, $p(x)$ has no repeated roots over $\mathbb{C}$ as $x^m - 1$ has no repeated roots over $\mathbb{C}$. It follows that elementary divisors of A are all linear factors, so the associated Jordan blocks are all 1×1, i.e. A is diagonalizable.

(*b*) Let $m(x)$ be the minimal polynomial of A over $\mathbb{Q}$, then $m(x)|x^p - 1$. Note that $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$ and $f(x) := x^{p-1} + \cdots + x + 1$ is irreducible. Indeed, let $g(x) = f(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \dbinom{p}{p-1} x^{p-2} + \cdots + \dbinom{p}{2} x + \dbinom{p}{1}$. Since $p|\binom{p}{i}$ for all $1 \leqslant i \leqslant p-1$, $p \nmid 1$ and $p^2 \nmid \binom{p}{1}$, by Eisenstein's criterion, we see that $g(x)$ is irreducible. Thus, $f(x)$ is irreducible. Since $\deg m(x) \leqslant n < p-1$, we see that $m(x) = x - 1$. Thus, $m(A) = A - I = 0$, i.e. $A = I$. □

Problem 141 (11J·4). Suppose T is a linear operator on an n-dimensional vector space V over a field F such that for any non-zero v in V the set $\{T^i(v) : i = 0, \cdots, n-1\}$ is linearly independent. Show that the characteristic polynomial of T is irreducible over F.

Proof. Let f be the minimal polynomial of T over F. Then, $\deg f = n$ and f is exactly the characteristic polynomial of T. Indeed, if $\deg f \leqslant n-1$, suppose $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ with $m \leqslant n-1$. Then, for any non-zero $v \in V$, $f(T)v = a_0 v + \cdots + a_m T^m v = 0$, which contradicts that $\{T^i(v) : i = 0, \cdots, n-1\}$ is linearly independent.

We now show that V has no proper invariant subspaces. Indeed, assume $W \subseteq V$ is a proper invariant subspace. Take $v \in V$, then $\{T^i(v) : i = 0, \cdots, n-1\} \subseteq W$. Contradiction.

Suppose $f = gh$ with g, h proper factors. Let $W = \ker g(T)$. For any $w \in W$, we have $g(T)w = 0$. So $g(T)(Tw) = Tg(T)w = 0$. Thus, W is a invariant subspace. So, $W = 0$ or V. If $W = V$, then $g(T) = 0$, contradiction. So, $W = 0$, i.e. $g(T)$ is injective. Since $f(T) = 0$, then $g(T)h(T)v = 0$ for all $v \in V$. Thus, $h(T)v = 0$ for all $v \in V$ as $g(T)$ is injective. But this implies that $h(T) = 0$, contradction. Thus, we see that f must be irreducible. □

Problem 142 (11A·7). Let $A \subseteq \mathrm{End}(V)$ be a subring of linear operators on an N-dimensional $\mathbb{C}$-vector space V and define $\mathrm{tr} : A \to \mathbb{C}$ by $\mathrm{tr}(a) = \sum_{i=1}^N \lambda_i$, where $\lambda_1, \cdots, \lambda_N$ are the roots of the characteristic polynomial of a (i.e. the eigenvalues with multiplicities).

(*a*) Show that $\mathrm{Ann}(\mathrm{tr}) := \{s \in A |\, \mathrm{tr}(sb) = 0, \text{ for all } b \in A\}$ is a 2-sided ideal in A.

(*b*) Use the fact that if $\mathrm{tr}(s^k) = 0$ for all $k \geqslant 1$ then s is nilpotent to prove that every element of Ann(tr) is nilpotent. Conclude that Ann(tr) is contained in every maximal left ideal of A.

Proof. (*a*) Take $s, r \in \mathrm{Ann}(\mathrm{tr})$, we see that $\mathrm{tr}((s-r)b) = \mathrm{tr}(sb - rb) = \mathrm{tr}(sb) - \mathrm{tr}(rb) = 0$. Thus, $s - r \in \mathrm{Ann}(\mathrm{tr})$. Clearly, $0 \in \mathrm{Ann}(\mathrm{tr})$, we see that Ann(tr) is an abelian group. Let $s \in \mathrm{Ann}(\mathrm{tr})$ and $a \in A$, we see that $\mathrm{tr}((sa)b) = \mathrm{tr}(s(ab)) = 0$ for all $b \in A$. Recall that $\mathrm{tr}(ab) = \mathrm{tr}(ba)$ for all $a, b \in A$, we have $\mathrm{tr}((as)b) = \mathrm{tr}(asb) = \mathrm{tr}(sba) = 0$ for all $b \in A$. Thus, we see that Ann(tr) is a two-sided ideal of A.

(*b*) Let $s \in \mathrm{Ann}(\mathrm{tr})$, we must have $\mathrm{tr}(s) = \mathrm{tr}(s \cdot 1) = 0$, where $1 \in A$ is the identity operator. Moreover, $\mathrm{tr}(s^k) = \mathrm{tr}(s \cdot s^{k-1}) = 0$ for all $k \geqslant 2$. Thus, we have $\mathrm{tr}(s^k) = 0$ for all $k \geqslant 1$. By the fact that if $\mathrm{tr}(s^k) = 0$ for all $k \geqslant 1$ then s is nilpotent, we see that s is a nilpotent. Let $\mathfrak{m}$ be a maximal left ideal of A. Suppose, $\mathrm{Ann}(\mathrm{tr}) \nsubseteq \mathfrak{m}$, then there exists $s \in \mathrm{Ann}(\mathrm{tr})$ such that $s \notin \mathfrak{m}$. Consider $As + \mathfrak{m}$, it is a left ideal strictly containing $\mathfrak{m}$, so we see that $As + \mathfrak{m} = A$. Thus, there exist $a \in A$ and $m \in \mathfrak{m}$ such that $as - m = 1$. Thus, $as = 1 + m \in \mathrm{Ann}(\mathrm{tr})$. So, we see that $1 + m$ is a nilpotent, i.e. $\exists k \geqslant 1$ such that $(1+m)^k = 0$. Note that $(1+m)^k = 1 + \binom{k}{1} m + \cdots + \binom{k}{k-1} m^{k-1} + m^k = 0$. Thus, $1 = -\binom{k}{1} m - \cdots - \binom{k}{k-1} m^{k-1} - m^k \in \mathfrak{m}$. Contradiction. Thus, $\mathrm{Ann}(\mathrm{tr}) \subseteq \mathfrak{m}$. □

Problem 143 (12J·7). Let V be a two dimensional vector space over the field F_p with p elements (p an odd prime). Let $L : V \to V$ be a linear transformation on V such that $L^{p-1} = I$, the identity map. Prove that L is diagonalizable, that is prove that there is a basis $\mathcal{B}$ for V such that $[L]_{\mathcal{B}}$, the matrix of L with respect to $\mathcal{B}$, is a diagonal matrix.

Proof. Let f be the minimal polynomial of L over F_p, then f divides $x^{p-1} - 1$. Note that for any $a \in F_p^{\times}$, we have $a^{p-1} = 1$. We see that the elements of $F_p^{\times}$ must be roots of $x^{p-1}-1$. Since $x^{p-1}-1$ has at most $p-1$ roots, we see that the roots of $x^{p-1}-1$ are precisely $F_p^{\times}$. Thus, f splits to linear factors and has no repeated roots. If L has 2 distinct eigenvalues λ_1, $\lambda_2 \in F_p$, then $Lv_1 = \lambda_1 v_1$ and $Lv_2 = \lambda_2 v_2$. Take $\mathcal{B} = \{v_1, v_2\}$, we see that $[L]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ Thus, L is diagonalizable in this case. If L has repeated eigenvalues λ, then the characteristic polynomial of L is $(x-\lambda)^2$. So, the minimal polynomial $f(x) = x - \lambda$ in this case. Thus, $L = \lambda I$ is diagonalizable.

To conclude, L is diagonalizable, that is prove that there is a basis $\mathcal{B}$ for V such that $[L]_{\mathcal{B}}$, the matrix of L with respect to $\mathcal{B}$, is a diagonal matrix. □

Remark. Since the minimal polynomial f splits to linear factors and has no repeated roots. We see that the elementary divisors of L are all linear factors. The associated Jordan blocks of elementary divisors are all 1×1. Thus, its Jordan form is diagonal, i.e. by taking $\mathcal{B}$ to be Jordan basis, $[L]_{\mathcal{B}}$ is a diagonal matrix.

Problem 144 (12A·6). Let $\langle , \rangle : V \times V \to \mathbb{R}$ be a symmetric bilinear form on a finite dimensional real vector space V. Thus for $v_1, v_2, v, w \in V$ and $\alpha \in \mathbb{R}$, we have

$$\langle v_1 + v_2, v \rangle = \langle v_1, v \rangle + \langle v_2, v \rangle$$

$$\langle \alpha v, w \rangle = \alpha \langle v, w \rangle$$

$$\langle v, w \rangle = \langle w, v \rangle.$$

Show there exists an orthogonal basis $\{v_1, \cdots, v_n\}$ for V, i.e. $\langle v_i, v_j \rangle = 0$ for $i \neq j$, with $\langle v_i, v_i \rangle = 1, -1$,or 0 for every i.

Proof. Suppose $\{v_1, \cdots, v_n\}$ is an orthogonal basis for V, then by setting

$$u_i = \begin{cases} v_i, & \text{if } \langle v_i, v_i \rangle = 0, \\ \frac{v_i}{\sqrt{|\langle v_i, v_i \rangle|}}, & \text{if } \langle v_i, v_i \rangle \neq 0, \end{cases}$$

we see that

$$\langle u_i, u_i \rangle = \begin{cases} 0, & \text{if } \langle v_i, v_i \rangle = 0, \\ \frac{\langle v_i, v_i \rangle}{|\langle v_i, v_i \rangle|} = \pm 1, & \text{if } \langle v_i, v_i \rangle \neq 0, \end{cases}$$

and $\langle u_i, u_j \rangle$ is a multiple of $\langle v_i, v_j \rangle$ hence $\langle u_i, u_j \rangle = 0$ for $i \neq j$.

Thus it remains to show that there exists an orthogonal basis $\{v_1, \cdots, v_n\}$ for V, i.e. $\langle v_i, v_j \rangle = 0$ for $i \neq j$.

Let $A = \{u \in V : \langle u, v \rangle = 0 \text{ for all } v \in V\}$ and B be a subspace of V such that $V = A \oplus B$. Let $\{v_1, \cdots, v_m\}$ and $\{u_1, \cdots, u_n\}$ be bases for A and B respectively, then we have $\langle v_i, v_j \rangle = \langle v_i, u_k \rangle = 0$ for all $j = 1, \cdots, m$ and $k = 1, \cdots n$. So, it suffices to show that there exists an orthogonal basis for B. Note that if $\langle u, v \rangle = 0$ for all $v \in B$, then $\langle u, v \rangle = 0$ for all $v \in V$. So, $u \in A \cap B = \{0\}$, i.e. $u = 0$. So, $\langle \cdot, \cdot \rangle|_B$ is non-degenerate.

So, it remains to prove that if $\langle\cdot,\cdot\rangle$ is non-degenerate symmetric bilinear form on V, then there exists an orthogonal basis $\{v_1, \cdots, v_n\}$ for V. We prove this statement by induction on $n := \dim V$. Suppose the statement holds for all vector spaces of dimension $\leqslant n-1$.

We claim that there exists $u \in V$ such that $\langle u,u\rangle \neq 0$, otherwise by $2\langle u,v\rangle = \langle u+v, u+v\rangle - \langle u,u\rangle - \langle v,v\rangle$, we see that for any $u, v \in V$, we have $\langle u,v\rangle = 0$, which contradicts that $\langle\cdot,\cdot\rangle$ is non-degenerate. Let $L = \langle u\rangle$ be a subspace generated by u. Let $L^\perp = \{v \in V : \langle v,u\rangle = 0\}$. Take $x \in V$, we see that $x - \frac{\langle x,u\rangle}{\langle u,u\rangle}u \in L^\perp$ as $\langle x - \frac{\langle x,u\rangle}{\langle u,u\rangle}u, u\rangle = \langle x,u\rangle - \frac{\langle x,u\rangle}{\langle u,u\rangle}\langle u,u\rangle = 0$. So, $x = u + (x - \frac{\langle x,u\rangle}{\langle u,u\rangle}u) \in L + L^\perp$. Let $v \in L \cap L^\perp$, then $v = \lambda u$ for some $\lambda \in \mathbb{R}$ and $\lambda\langle u,u\rangle = \langle \lambda u, u\rangle = \langle v,u\rangle = 0$. Since $\langle u,u\rangle \neq 0$, we see that $\lambda = 0$ and $v = 0$. Thus, $V = L \oplus L^\perp$. It follows that $\dim L^\perp = n-1$. By induction hypothesis, there exists an orthogonal basis $\{v_2, \cdots, v_n\}$ for $L^\perp$. Let $v_1 = u$, we see that $\{v_1, \cdots, v_n\}$ is an orthogonal basis for V. □

Problem 145 (14J·5). Let M be an invertible $n \times n$ matrix with real number entries and positive determinant. Show that M can be written as RK where R is in $SO(n)$ (R is orthogonal with determinant 1) and K is an upper triangular matrix with positive entries on the diagonal. Hint: Orthogonal matrices have orthonormal column vectors.

Proof. Clearly, $RK \subseteq M$. It suffices to show that $M \subseteq RK$. Let $M = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \end{bmatrix}$ with $v_1, v_2, \cdots, v_n$ column vectors of M. Take $A \in M$, since A is invertible, we see that $v_1, v_2, \cdots, v_n$ is a basis for $\mathbb{R}^n$. We then can obtain an orthonormal basis $e_1, e_2, \cdots, e_n$ by Gram-Schmidt process. More precisely,

$$\begin{aligned}
e_1 &= \frac{v_1}{\|v_1\|},\\
e_2 &= \frac{v_2 - \langle e_1, v_2\rangle e_1}{\|v_2 - \langle e_1, v_2\rangle e_1\|},\\
e_3 &= \frac{v_3 - \langle e_1, v_3\rangle e_1 - \langle e_2, v_3\rangle e_2}{\|v_3 - \langle e_1, v_3\rangle e_1 - \langle e_2, v_3\rangle e_2\|},\\
&\cdots,\\
e_n &= \frac{v_n - \langle e_1, v_n\rangle e_1 - \cdots - \langle e_{n-1}, v_n\rangle e_{n-1}}{\|v_n - \langle e_1, v_n\rangle e_1 - \cdots - \langle e_{n-1}, v_n\rangle e_{n-1}\|}.
\end{aligned}$$

Then,

$$\begin{aligned}
v_1 &= \|v_1\| e_1,\\
v_2 &= \langle e_1, v_2\rangle e_1 + \|v_2 - \langle e_1, v_2\rangle e_1\| e_2,\\
v_3 &= \langle e_1, v_3\rangle e_1 + \langle e_2, v_3\rangle e_2 + \|v_3 - \langle e_1, v_3\rangle e_1 - \langle e_2, v_3\rangle e_2\| e_3,\\
&\cdots,\\
v_n &= \langle e_1, v_n\rangle e_1 + \cdots + \langle e_{n-1}, v_n\rangle e_{n-1} + \|v_n - \langle e_1, v_n\rangle e_1 - \cdots - \langle e_{n-1}, v_n\rangle e_{n-1}\| e_n.
\end{aligned}$$

Thus, we see that

$$\begin{bmatrix} e_1 & e_2 & \cdots & e_n \end{bmatrix} \begin{bmatrix} a_1 & \langle e_1, v_2\rangle & \cdots & \langle e_1, v_n\rangle \\ 0 & a_2 & \cdots & \langle e_2, v_n\rangle \\ 0 & 0 & \cdots & \langle e_3, v_n\rangle \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \langle e_{n-1}, v_n\rangle \\ 0 & 0 & \cdots & a_n \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \end{bmatrix} = A,$$

where $a_1 = \|v_1\|$, $a_2 = \|v_2 - \langle e_1, v_2\rangle e_1\|$, $\cdots$, $a_n = \|v_n - \langle e_1, v_n\rangle e_1 - \cdots - \langle e_{n-1}, v_n\rangle e_{n-1}\|$. Thus, we see that $A \in RK$.

We conclude that $M = RK$. □

Problem 146 (14A·1). Consider the matrix $M := \begin{pmatrix} 0 & 0 & -y \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ where y is an indeterminate.

(a) Show that the characteristic polynomial $f_M(X)$ of M is irreducible in $\mathbb{Q}(y)[X]$.

(b) Show that M is diagonalizable over the field $\overline{\mathbb{Q}(y)}$.

(c) Show that M is not diagonalizable over the field $\overline{\mathbb{F}_3(y)}$.

Proof. (a) The characteristic polynomial $f_M(X) = \det(XI - M) = \det \begin{pmatrix} x & 0 & y \\ -1 & x & 0 \\ 0 & -1 & x \end{pmatrix} = X^3 + y \in \mathbb{Z}[y][X]$. Since y is a prime element in $\mathbb{Z}[y]$, $y \mid y$, $y \nmid 1$ and $y^2 \nmid y$, we see that $X^3 + y \in \mathbb{Q}(y)[X]$ is irreducible by Eisenstein's criterion.

(b) Let $a \in \overline{\mathbb{Q}(y)}$ such that $a^3 + y = 0$, and $\omega = e^{\frac{2\pi i}{3}}$, then we see that $a, a\omega, a\omega^2$ are the three roots of $X^3 + y$ in $\overline{\mathbb{Q}(y)}$. So, we see that M has three distinct eigenvalues in $\overline{\mathbb{Q}(y)}$. Let v_1, v_2, v_3 be the eigenvectors associated to $a, a\omega, a\omega^2$ respectively. Then, $\{v_1, v_2, v_3\}$ is a basis for $\overline{\mathbb{Q}(y)}^3$. We see that

$$M \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} \begin{bmatrix} a & & \\ & a\omega & \\ & & a\omega^2 \end{bmatrix},$$

i.e.

$$M = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} \begin{bmatrix} a & & \\ & a\omega & \\ & & a\omega^2 \end{bmatrix} \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix}^{-1}.$$

Thus, M is diagonalizable.

(c) Let $a \in \overline{\mathbb{F}_3(y)}$ such that $a^3 + y = 0$, then $y = -a^3$. Thus, $f_M(X) = X^3 + y = X^3 - a^3 = (X - a)^3$. By direct computation, $M - aI = \begin{pmatrix} -a & 0 & -y \\ 1 & -a & 0 \\ 0 & 1 & -a \end{pmatrix} \neq 0$ and $(M - aI)^2 = \begin{pmatrix} a^2 & -y & 2ay \\ -2a & a^2 & -y \\ 1 & -2a & a^2 \end{pmatrix} \neq 0$. Thus, $f_M(X) = (X - a)^3$ is the minimal polynomial of M. Thus, the Jordan canonical form of M is

$$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix},$$

which implies that M is not diagonalizable over $\overline{\mathbb{F}_3(y)}$. □

Problem 147 (14A·4). State and prove the Cayley-Hamilton Theorem for $T \in \operatorname{End}(V)$ with V a finite-dimensional vector space. (You many use any canonical form you wish.)

Proof. Cayley-Hamilton Theorem: Suppose V is a vector space over a field k. Let $\operatorname{char}_T(X) = \det(XI - T)$ be the characteristic polynomial of T, then $\operatorname{char}_T(T) = 0$.

We may regard V as a $k[t]$-module by $f(t) \cdot v = f(T)(v)$, where $f \in k[t]$. Let $\{e_1, \cdots, e_n\}$ be a basis for V. Then, we see that

$$\begin{aligned} t \cdot e_1 &= a_{11}e_1 + \cdots + a_{1n}e_n \\ \cdots & \\ t \cdot e_n &= a_{n1}e_1 + \cdots + a_{nn}e_n, \end{aligned}$$

with $a_{ij} \in k$. So, we see that

$$(tI - M) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0,$$

where $M = \mathcal{M}(T)$ is the matrix representation of T under basis $e_1, \cdots, e_n$. By multiplying the adjugate matrix $(tI - M)^*$ of $tI - M$, we see that $\det(tI - M)e_i = 0$ for all i as $\det(tI - M) = (tI - M)^*(tI - M)$ by Cramer's rule. Thus, $\det(tI - M) = \mathrm{char}_M(t) = 0$. Since M is the matrix of T, we have $\mathrm{char}_T(X) = \mathrm{char}_M(X)$ i.e. $\mathrm{char}_T(t) = 0$ for $t \in k[t]$. So, for any $v \in V$, we have $\mathrm{char}_T(t) \cdot v = \mathrm{char}_T(T)(v) = 0$. Thus, $\mathrm{char}_T(T) = 0$. □

Problem 148 (15A·3). Let K be a field.

(a) Please prove that, given any non-zero vector $v \in K^n$, v can be completed to a basis, i.e., we can find $v_2, \cdots, v_n \in K^n$ with $\{v, v_2, \cdots, v_n\}$ a basis for K^n.

(b) Under the additional assumption that K is algebraically closed, please prove that, given any $A \in K^{n\times n}$, there are matrices $U, V \in K^{n\times n}$, with V invertible and U upper-triangular, such that $A = V^{-1}UV$.

Proof. (a) Let X be the set of lists of linearly independent vectors containing v, i.e. an element in X is a list $L = \{v, v_2, \cdots, v_r\}$ of linearly independent vectors. Since $\{v\} \in X$, we see that $X \neq \varnothing$. We define a partial order $\leqslant$ on X by $L_1 \leqslant L_2 \Leftrightarrow \mathrm{span}(L_1) \leqslant \mathrm{span}(L_2)$. Take a chain $C = \{L_i : i \in I\}$. Let $L = \bigcup_{i\in I} L_i$, then we see that $L_i \leqslant L$ as $\mathrm{span}(L_i) \leqslant \mathrm{span}(L)$. Thus, by Zorn's lemma, X has a maximal element containing v, say L. We claim that $V := \mathrm{span}(L) = K^n$. If not, then $K^n/V \neq \{0\}$. Then, there exists $u \in K^n$ such that $u + V \neq V$, i.e. $u \notin V$. Then, $L \cup \{u\} \in X$ and $L \leqslant L \cup \{u\}$, a contradiction. Thus, $V = \mathrm{span}(L) = K^n$, i.e. L is a basis of K^n. Since $\dim K^n = n$, we see that $|L| = n$, i.e. $L = \{v, v_2, \cdots, v_n\}$ for some $v_2, \cdots, v_n \in K^n$.

(b) We prove this result by induction on n. If $n = 1$, it is trivial. Suppose now the statement holds for all $B \in K^{\ell\times\ell}$ with $\ell \leqslant n - 1$. Let $A \in K^{n\times n}$. Consider the equation $\det(xI - A) = 0$ in variable x, it has a solution over K as K is algebraically closed. Thus, A must have an eigenvalue $\lambda_1 \in K$. Let $v_1 \in K^n$ be an eigenvector of A associated to λ_1, i.e. $Av_1 = \lambda_1 v_1$. By (a), we can find $u_2, \cdots, u_n \in K^n$ such that $\{v_1, u_2, \cdots, u_n\}$ is a basis for K^n. Let $V_1 = \mathrm{span}(v_1)$ and $V_2 = \mathrm{span}(u_2, \cdots, u_n)$, then we see that $K^n = V_1 \oplus V_2$ and $V_2 = K^n/V_1 \cong K^{n-1}$. Consider the quotient operator

$$\widetilde{A} : K^n/V_1 \to K^n/V_1$$

given by $w + V_1 \mapsto Aw + V_1$. Since $Aw \in V_1$ whenever $w \in V_1$, $\widetilde{A}$ is thus well-defined. Thus, by induction hypothesis, there exists a basis $v_2 + V_1, \cdots, v_n + V_1$ for K^n/V_1 such that

$$\begin{aligned}
Av_2 + V_1 &= \widetilde{A}(v_2 + V_1) = \lambda_2(v_2 + V_1), \\
Av_3 + V_1 &= \widetilde{A}(v_3 + V_1) = a_{23}(v_2 + V_1) + \lambda_3(v_3 + V_1), \\
&\cdots \\
Av_n + V_1 &= \widetilde{A}(v_n + V_1) = a_{2n}(v_2 + V_1) + \cdots + a_{n-1,n}(v_{n-1} + V_1) + \lambda_n(v_n + V_1).
\end{aligned}$$

Thus, we see that

$$\begin{aligned}
Av_1 &= \lambda_1 v_1 \\
Av_2 &= a_{12}v_1 + \lambda_2 v_2 \\
Av_3 &= a_{13}v_1 + a_{23}v_2 + \lambda_3 v_3 \\
&\cdots \\
Av_n &= a_{1n}v_1 + a_{2n}v_2 + \cdots + a_{n-1,n}v_{n-1} + \lambda_n v_n
\end{aligned}$$

for some $a_{12}, a_{13}, \cdots, a_{1n} \in K$. Thus,

$$A\begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix} = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix} \begin{bmatrix} \lambda_1 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & \lambda_2 & a_{23} & \cdots & a_{2n} \\ 0 & 0 & \lambda_3 & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_n \end{bmatrix}$$

Since $v_2 + V_1, \cdots, v_n + V_1$ is a basis for K^n/V_1, we see that $v_1, v_2, \cdots, v_n$ is a basis for K^n. Thus, $\begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}$ is invertible. Let $V = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}^{-1}$ and $U = \begin{bmatrix} \lambda_1 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & \lambda_2 & a_{23} & \cdots & a_{2n} \\ 0 & 0 & \lambda_3 & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_n \end{bmatrix}$, we see that

$$A = V^{-1}UV$$

with V invertible and U upper-triangular. □

Problem 149 (16J·4).

(a) Let A be an $n \times n$ matrix over $\mathbb{C}$. Prove that if $\mathrm{Tr}(A^i) = 0$ for all $i > 0$ then A is nilpotent.

(b) Let A and B be $n \times n$ matrices over $\mathbb{C}$. Prove that if A commutes with $AB - BA$ then $(AB - BA)$ is nilpotent.

Proof. Recall that there exists an invertible matrix V such that $A = V^{-1}UV$ with U an upper-triangular matrix. Since $\mathrm{Tr}(A) = \mathrm{Tr}(V^{-1}UV) = \mathrm{Tr}(U)$, we may assume that A is upper-triangular. Suppose that $A = (a_{ij})$, then $a_{ij} = 0$ if $i > j$. Let $d_i = a_{ii}$ for each $1 \leqslant i \leqslant n$. Then by direct computation, we see that

$$A^k = \begin{pmatrix} d_1^k & & * & \\ & d_2^k & & \\ & & \ddots & \\ & 0 & & d_n^k \end{pmatrix}$$

So, $\mathrm{Tr}(A^k) = d_1^k + \cdots + d_n^k = 0$ for all $k > 0$.

We claim that if there exist $a_1, \cdots, a_n$ all positive such that

$$\begin{cases} a_1 d_1 + \cdots + a_n d_n = 0 \\ a_1 d_1^2 + \cdots + a_n d_n^2 = 0 \\ \cdots \\ a_1 d_1^n + \cdots + a_n d_n^n = 0 \end{cases}$$

then $d_1 = \cdots = d_n = 0$. We prove that the statement by induction on n. If $n = 1$, then $a_1 d_1 = 0$, so $d_1 = 0$ and we are done. Suppose the statement holds for all dimension $\leqslant n-1$. Then we see that if $D = \begin{pmatrix} d_1 & d_2 & \cdots & d_n \\ d_1^2 & d_2^2 & \cdots & d_n^2 \\ \vdots & \vdots & \ddots & \cdots \\ d_1^n & d_2^n & \cdots & d_n^n \end{pmatrix}$ and $x = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$, we have $Dx = 0$. Since $a_1, \cdots, a_n$ are all positive, we see that $x \neq 0$. So, $\det(D) = 0$. Note that $\det(D) = d_1 \cdots d_n \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ d_1 & d_2 & \cdots & d_n \\ \vdots & \vdots & \ddots & \cdots \\ d_1^{n-1} & d_2^{n-1} & \cdots & d_n^{n-1} \end{pmatrix} = d_1 \cdots d_n \prod_{1 \leqslant j < i \leqslant n} (d_i - d_j) = 0$. We see that $d_i = 0$ or $d_i = d_j$ for some $i \neq j$. We may assume that $d_n = 0$ or $d_n = d_{n-1}$. In either cases, we see that there exist positive numbers $b_1, \cdots, b_{n-1}$ such that

$$\begin{cases} b_1 d_1 + \cdots + b_{n-1} d_{n-1} = 0 \\ b_1 d_1^2 + \cdots + b_{n-1} d_{n-1}^2 = 0 \\ \cdots \\ b_1 d_1^{n-1} + \cdots + b_{n-1} d_{n-1}^{n-1} = 0 \end{cases}$$

By induction hypothesis, we see that $d_1 = \cdots = d_{n-1} = 0$. Thus, $d_1 = \cdots = d_n = 0$. Thus, A is nilpotent.

(b) Let $C = AB - BA$, then $\mathrm{Tr}(C) = \mathrm{Tr}(AB) - \mathrm{Tr}(BA) = 0$ and $AC = CA$. Let $i \geqslant 2$, then $C^i = C^{i-1}(AB - BA) = C^{i-1}AB - C^{i-1}BA = A(C^{i-1}B) - (C^{i-1}B)A$. Thus, $\mathrm{Tr}(C^i) = 0$. So, $\mathrm{Tr}(C^i) = 0$ for all $i > 0$. By (a), we see that $C = AB - BA$ is nilpotent. □

Problem 150 (16J·7). Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ denote the linear map defined by $T(x, y) = (x-y, y-x)$ for all $x, y \in \mathbb{R}$. Consider $\mathbb{R}^2$ to be an $\mathbb{R}[x]$-module by letting $p(x) \cdot v = p(T)(v)$ for all $p(x) \in \mathbb{R}[x]$, $v \in \mathbb{R}^2$.

(a) Is $\mathbb{R}^2$ a cyclic $\mathbb{R}[x]$-module? (That is, is $\mathbb{R}^2$ generated by a single element as an $\mathbb{R}[x]$-module?)

(b) Find all the $\mathbb{R}[x]$-submodules of $\mathbb{R}^2$.

Proof. (a) Let $T(x, y) = \lambda(x, y)$ with $(x, y) \neq 0$, we see that $\lambda = 0$ or 2. Thus, the characteristic polynomial of T is $\mathrm{char}_T(x) = x(x-2)$. Since $T \neq 0$, $T - 2I \neq 0$, we see that the minimal polynomial of T is $f(x) = \min_T(x) = x(x-2) = \mathrm{char}_T(x)$.

Note that $\mathbb{R}^2$ is a finitely generated module over $\mathbb{R}[x]$, which is a PID. By the classification theorem of finitely generated module over a PID, there exists an $\mathbb{R}[x]$-module isomorphism

$$\varphi : \mathbb{R}^2 \cong \mathbb{R}[x]^{\oplus r} \oplus \frac{\mathbb{R}[x]}{(f_1)} \oplus \cdots \oplus \frac{\mathbb{R}[x]}{(f_m)},$$

where $f_1 | \cdots | f_m$ are invariant factors. Clearly, φ is a isomorphism of $\mathbb{R}$-vector spaces, so by counting the dimension, we see that $r = 0$, i.e.

$$\varphi : \mathbb{R}^2 \cong \frac{\mathbb{R}[x]}{(f_1)} \oplus \cdots \oplus \frac{\mathbb{R}[x]}{(f_m)}.$$

Recall that f_m is the minimal polynomial of T and $f_1 \cdots f_m$ is the characteristic polynomial of T. Thus, $f_1 = \cdots = f_{m-1} = 1$ and $f_m = f$, i.e. there exists a $\mathbb{R}[x]$-module isomorphism

$$\varphi : \mathbb{R}^2 \cong \mathbb{R}[x]/(f).$$

Since $\mathbb{R}[x]/(f)$ is a cyclic $\mathbb{R}[x]$-module generated by $1+(f)$, we see that $\mathbb{R}^2$ is a cyclic $\mathbb{R}[x]$-module.

(b) To find all the $\mathbb{R}[x]$-submodules of $\mathbb{R}^2$, it suffices to find all $\mathbb{R}[x]$-submodules of $\mathbb{R}[x]/(f)$. Note that an $\mathbb{R}[x]$-submodule of $\mathbb{R}[x]/(f)$ is equivalent to an ideal of $\mathbb{R}[x]/(f)$, which corresponds to an ideal of $\mathbb{R}[x]$ that contains (f). Since $\mathbb{R}[x]$ is a PID, every ideal I is of the form (g) for some $g \in \mathbb{R}[x]$. Then, $I = (g) \supseteq (f) \Leftrightarrow g \mid f$. Thus, $g = 1, x, (x-2)$ or f up to a unit. So, $I = \mathbb{R}[x], (x), (x-2)$ or (f).

Let $\alpha = \varphi^{-1}(\overline{1})$, where $\overline{1} = 1 + (f)$. Then $\varphi^{-1}(\overline{x}) = x \cdot \varphi^{-1}(\overline{1}) = T\alpha$ and $\varphi^{-1}(\overline{x-2}) = (x-2) \cdot \varphi^{-1}(\overline{1}) = T\alpha - 2\alpha$. So, $\mathbb{R}[x]$-submodules of $\mathbb{R}^2$ are $\{0\}, \langle T\alpha\rangle, \langle T\alpha - 2\alpha\rangle$ and $\mathbb{R}^2$.

Moreover, we can give the map φ explicitly by $\varphi : (a,b) \mapsto \overline{a+b-bx}$. Indeed, φ is clearly bijective and $\varphi(x(a,b)) = \varphi(T(a,b)) = \varphi(a-b, b-a) = \overline{ax-bx} = \overline{x(a+b-bx)} = x \cdot \varphi(a,b)$ for all $(a,b) \in \mathbb{R}^2$. In this case, $\alpha = (1,0)$, $T\alpha = (1,-1)$ and $T\alpha - 2\alpha = (-1,-1)$. Then, $\langle T\alpha\rangle = \langle(1,-1)\rangle$ and $\langle T\alpha - 2\alpha\rangle = \langle(-1,-1)\rangle = \langle(1,1)\rangle$.

So, $\mathbb{R}[x]$-submodules of $\mathbb{R}^2$ are $\{0\}, \langle(1,-1)\rangle, \langle(1,1)\rangle$ and $\mathbb{R}^2$. □

Problem 151 (17A·4). Let V be a finite dimensional vector space over $\mathbb{C}$, and suppose we have $\mathbb{C}$-linear maps $A_1, \cdots, A_k : V \to V$ such that for all i, j, we have $A_i \circ A_j = A_j \circ A_i$. Show that there exists a non-zero vector in V that is simultaneously an eigenvector for each of $A_1, \cdots, A_k$ (with possibly different eigenvalues). (Suggestion: use an induction on k.)

Proof. We use the notation $E(A, \lambda)$ to denote the eigenspace of A associated to λ.

We prove the statement by induction on k. For $k = 1$, it holds trivially. Suppsoe the statement holds for $1, 2, \cdots, k-1$. Then, there exists a non-zero vector, say v, in V that is simultaneously an eigenvector for each of $A_1, \cdots, A_{k-1}$. Then, we have $A_i v = \lambda_i v$ for all $1 \leqslant i \leqslant k-1$. So, we see that $A_i(A_k v) = A_k(A_i v) = \lambda_i(A_k v)$ for all $1 \leqslant i \leqslant k-1$. So, $A_k v \in E(A_i, \lambda_i)$ for all $1 \leqslant i \leqslant k-1$.

Now, let $W = \bigcap_{i=1}^{k-1} E(A_i, \lambda_i)$ and $\{v, v_2, \cdots, v_r\}$ a basis for W. Similarly, $A_k v_i \in W$, i.e. W is an invariant subspace of A_k. Then, A_k has an eigenvalue λ and an eigenvector $w \in W$ such that $A_k w = \lambda w$. Then, $w = c_1 v + c_2 v_2 + \cdots + c_r v_r$.

Thus, $A_i w = A_i(c_1 v + c_2 v_2 + \cdots + c_r v_r) = c_1 A_i v + c_2 A_i v_2 + \cdots + c_r A_i v_r = \lambda_i(c_1 v + \cdots + c_r v_r) = \lambda_i w$. Thus, w is simultaneously an eigenvector for each of $A_1, \cdots, A_k$. □

Problem 152 (19J·1). Let T be a linear operator on a nonzero finite dimensional vector space V over a field F. Assume that the only T-invariant subspaces of V are the zero subspace and V itself. Prove that the characteristic polynomial of T is irreducible over F.

(By definition, a subspace W of V is called T-invariant if $T(W) \subseteq W$.)

Proof. We can make V into an $F[x]$-module by $x \cdot v = T(v)$. Then, by the classification theorem of finitely generated modules over a PID, we have an isomorphism of $F[x]$-modules

$$\varphi : V \cong F[x]^{\oplus n} \oplus F[x]/(f_1) \oplus \cdots \oplus F[x]/(f_m),$$

where $f_1 \mid \cdots \mid f_m$. Recall that f_m is the minimal polynomial of T and $f_1 \cdots f_m$ is the characteristic polynomial of T. Note that φ is also an isomorphism of F-vector spaces. So by counting dimension over F, we see that $n = 0$. Since the only T-invariant subspaces of V are the zero subspace and V itself, we see that V is a simple $F[x]$-module, which implies that $m = 1$. Thus, $F[x]/(f_1) \cong V$ is a simple module. Thus, (f_1) is a maximal $F[x]$-submodule of $F[x]$, i.e. a maximal ideal. Thus, f_1 is irreducible. Thus, the characteristic polynomial of T is irreducible over F. □

Problem 153 (19A·5). For the following questions, A is a 3×3 matrix with entries in $\mathbb{C}$ and I is the 3×3 identity matrix.

(a) List all possible 3×3 matrices A in Jordan canonical form having 5 as the only eigenvalue.

(b) Which of the matrices A from part (a) satisfy $\dim(\ker(A - 5I)) = 2$?

(c) Let $V = \mathbb{C}^3$ and let A be any of the matrices from part (a). Consider V to be a $\mathbb{C}[x]$-module via $p(x) \cdot v = p(A)v$ for all $v \in V$, $p(x) \in \mathbb{C}[x]$. For which of the matrices A from part (a) is V a cyclic $\mathbb{C}[x]$-module?

Proof. (a) They are $\begin{pmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}$, $\begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}$, $\begin{pmatrix} 5 & 0 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{pmatrix}$, $\begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{pmatrix}$.

(b) By direct computation, $\begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}$, $\begin{pmatrix} 5 & 0 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{pmatrix}$ satisfy $\dim \ker(A - 5I) = 2$.

(c) $\begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{pmatrix}$ because its minimal polynomial and its characteristic polynomial are all $(x - 5)^3$. □

Problem 154 (20A·5). Let K be a field, let V be a finite dimensional K-vector space, and let $V^* = \mathrm{Hom}_K(V, K)$ be the dual K-vector space of V. For a K-subspace $W \subseteq V$ define the annihilator

$$\mathrm{Ann}(W) := \{\lambda \in V^* : \forall w \in W \text{ we have } \lambda(w) = 0\}.$$

Prove that the following statement holds: If U, W are K-subspaces of V with $U \subseteq W$, then $\mathrm{Ann}(U)/\mathrm{Ann}(W)$ and $(W/U)^*$ are isomorphic as K-vector spaces. Furthermore, provide an explicit isomorphism.

Proof. For any $\lambda \in \mathrm{Ann}(U)$, $\lambda|_W : W \to K$ is a K-linear functional. It induces a K-linear functional

$$\widetilde{\lambda|_W} : W/U \to K$$

by

$$w + U \mapsto \lambda|_W(w) = \lambda(w).$$

If $w + U = v + U$, i.e. $w - v \in U$, then $\lambda(w - v) = 0$. So, $\widetilde{\lambda|_W}(w + U) = \lambda(w) = \lambda(v) = \widetilde{\lambda|_W}(v + U)$. Thus, $\widetilde{\lambda|_W}$ is a well-defined K-linear map, i.e. $\widetilde{\lambda|_W} \in (W/U)^*$.

Thus, we can define a K-linear map

$$\psi : \operatorname{Ann}(U) \to (W/U)^*$$

by

$$\lambda \mapsto \widetilde{\lambda|_W}.$$

Since $\lambda \in \ker\psi \Leftrightarrow \widetilde{\lambda|_W} = 0 \Leftrightarrow \widetilde{\lambda|_W}(w + U) = \lambda(w) = 0$ for all $w \in W \Leftrightarrow \operatorname{Ann}(W)$, we see that $\ker\psi = \operatorname{Ann}(W)$.

Let $\mu \in (W/U)^*$, i.e. $\mu : W/U \to K$ is a K-linear map. Then, we may define $\mu' : W \to K$ by $\mu'(w) = \mu(w + U)$. We see that $\mu'(u) = 0$ for all $u \in U$. Find a subspace T such that $W \oplus T = V$, then we may define a K-linear map $\lambda : V \to K$ by $w + t \mapsto \mu'(w)$. We see that $\lambda \in \operatorname{Ann}(U)$, $\lambda|_W = \mu'$ and $\widetilde{\lambda|_W} = \mu$. Thus, we see that ψ is surjective.

By the first isomorphism theorem, we have an induced isomorphism

$$\widetilde{\psi} : \operatorname{Ann}(U)/\operatorname{Ann}(U) \to (W/U)^*$$

given by

$$\lambda + \operatorname{Ann}(U) \mapsto \psi(\lambda).$$

□

Problem 155 (**21J·4**). Let $F : \mathbb{C}^2 \to \mathbb{C}^2$ be a map given by $F(x, y) = (2x + y, x + y)$,$x, y \in \mathbb{C}$. Consider $\mathbb{C}^2$ to be a $\mathbb{C}[t]$-module by letting $p(t) \cdot v = p(F)(v)$ for any $p(t) \in \mathbb{C}[t]$, $v \in \mathbb{C}^2$.

(a) Is $\mathbb{C}^2$ a cyclic $\mathbb{C}[t]$-module?

(b) Find all the $\mathbb{C}[t]$-submodules of $\mathbb{C}^2$.

Proof. (a) The matrix of F with respect to standard basis $(1, 0), (0, 1)$ is $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$. Its characteristic polynomial is $g(x) = x^2 - 3x + 1$. Thus, F has two distinct eigenvalues λ_1, λ_2. Thus, its minimal polynomial is $f(x) = (x - \lambda_1)(x - \lambda_2) = g(x)$. By the classification theorem of finitely generated modules over a PID, we have a $\mathbb{C}[t]$-module isomorphism

$$\varphi : \mathbb{C}^2 \to \mathbb{C}[t]^{\oplus k} \oplus \mathbb{C}[t]/(f_1) \oplus \cdots \oplus \mathbb{C}[t]/(f_n),$$

where $f_1|\cdots|f_n$, f_n is the minimal polynomial of F and $f_1 \cdots f_n$ is the characteristic polynomial of F. Since φ is also $\mathbb{C}$-vector space isomorphism, we see that $k = 0$.

Since $f = f_n = g = f_1 \cdots f_n$, we see that $n = 1$. Thus, we have a $\mathbb{C}[t]$-module isomorphism

$$\varphi : \mathbb{C}^2 \to \mathbb{C}[t]/(f).$$

Since $\mathbb{C}[t]/(f)$ is a cyclic $\mathbb{C}[t]$-module generated by $\overline{1} = 1 + (f)$. We see that $\mathbb{C}^2$ is a cyclic $\mathbb{C}[t]$-module.

(b) To find all the $\mathbb{C}[t]$-submodules of $\mathbb{C}^2$, it suffices to find all $\mathbb{C}[t]$-submodules of $\mathbb{C}[t]/(f)$. Note that an $\mathbb{C}[t]$-submodule of $\mathbb{C}[t]/(f)$ is equivalent to an ideal of $\mathbb{C}[t]/(f)$, which corresponds to an ideal of $\mathbb{C}[t]$ that contains (f). Since $\mathbb{C}[t]$ is a PID, every ideal I is of the form (g) for some $g \in \mathbb{C}[t]$. Then, $I = (g) \supseteq (f) \Leftrightarrow g \mid f$. Thus, $g = 1, (t - \lambda_1), (t - \lambda_2)$ or f up to a unit. So, $I = \mathbb{C}[t], (t - \lambda_1), (t - \lambda_2)$ or (f).

Let $\alpha = \varphi^{-1}(\overline{1})$, where $\overline{1} = 1 + (f)$. Then $\varphi^{-1}(\overline{t - \lambda_i}) = (t - \lambda_i) \cdot \varphi^{-1}(\overline{1}) = F\alpha - \lambda_i\alpha$. So, $\mathbb{C}[x]$-submodules of $\mathbb{C}^2$ are $\{0\}, \langle F\alpha - \lambda_1\alpha\rangle, \langle F\alpha - \lambda_2\alpha\rangle$ and $\mathbb{C}^2$.

Moreover, we can give the map φ explicitly by $\varphi : (a,b) \mapsto \overline{bt + a - 2b}$. Indeed, φ is clearly bijective and $\varphi(t(a,b)) = \varphi(F(a,b)) = \varphi(2a+b, a+b) = \overline{(a+b)t - b} = \overline{t(bt + a - 2b)} = t \cdot \varphi(a,b)$ for all $(a,b) \in \mathbb{C}^2$. In this case, $\alpha = (1,0)$, $F\alpha = (2,1)$ and $F\alpha - \lambda_i \alpha = (2 - \lambda_i, 1)$. Then, $\langle F\alpha - \lambda_i \alpha \rangle = \langle (2 - \lambda_i, 1) \rangle$.

So, $\mathbb{C}[x]$-submodules of $\mathbb{C}^2$ are $\{0\}, \langle (2-\lambda_1, 1)\rangle, \langle (2-\lambda_2, 1)\rangle$ and $\mathbb{C}^2$, where $\lambda_{1,2} = \frac{3\pm\sqrt{5}}{2}$. □

Problem 156 (21J·8). Consider the matrix $M = \begin{bmatrix} 0 & 0 & y \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ (y is an indeterminate).

(a) Is the characteristic polynomial of M irreducible in $\mathbb{Q}(y)[x]$?

(b) Is M diagonalizable over the field $\overline{\mathbb{Q}(y)}$? ($\overline{\mathbb{Q}(y)}$ denotes an algebraic closure of $\mathbb{Q}(y)$).

Proof. (a) The characteristic polynomial of M is $f(x) = \det \begin{pmatrix} x & 0 & -y \\ -1 & x & 0 \\ 0 & -1 & x \end{pmatrix} = x^3 - y \in \mathbb{Q}(y)[x]$. Take $p = y \in \mathbb{Z}[y]$, which is a prime element in $\mathbb{Z}[y]$. Then, we see that $p \mid (-y)$, $p \nmid 1$ and $p^2 \nmid (-y)$. Thus, the characteristic polynomial of M is irreducible in $\mathbb{Q}(y)[x]$ by Eisenstein's criterion.

(b) Let $a \in \overline{\mathbb{Q}(y)}$ be a root of $x^3 - y$ and $\omega = e^{2\pi i/3}$, then the roots of $x^3 - y$ are $a, a\omega$ and $a\omega^2$. So, we see that M has three distinct eigenvalues in $\overline{\mathbb{Q}(y)}$. Let v_1, v_2, v_3 be the eigenvectors associated to $a, a\omega, a\omega^2$ respectively. Then, $\{v_1, v_2, v_3\}$ is a basis for $\overline{\mathbb{Q}(y)}^3$. We see that

$$M \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} \begin{bmatrix} a & & \\ & a\omega & \\ & & a\omega^2 \end{bmatrix},$$

i.e.

$$M = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} \begin{bmatrix} a & & \\ & a\omega & \\ & & a\omega^2 \end{bmatrix} \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix}^{-1}.$$

Thus, M is diagonalizable. □

5 Fields and Galois Theory

Problem 157 (09J·8). (1) Let F be a field. Let α and β be algebraic over F with minimal polynomials f and g respectively. Show that g is irreducible over $F(\alpha)$ if and only if f is irreducible over $F(\beta)$.

(2) Let L be the splitting field of $x^4 - 6$ over $\mathbb{Q}$. Determine $[L : \mathbb{Q}]$.

Proof. Let $m = \deg f$ and $n = \deg g$.

(1) Suppose g is irreducible over $F(\alpha)$. Then, g is the minimal polynomial of β over $F(\alpha)$, so $[F(\alpha,\beta) : F(\alpha)] = [F(\alpha)(\beta) : F(\alpha)] = \deg g = n$. Thus, $[F(\alpha,\beta) : F] = [F(\alpha,\beta) : F(\alpha)][F(\alpha) : F] = \deg g \cdot \deg f = mn$. Note that $mn = [F(\alpha,\beta) : F] = [F(\alpha,\beta) : F(\beta)][F(\beta) : F] = n[F(\alpha,\beta) : F(\beta)]$. We see that $[F(\alpha,\beta) : F(\beta)] = m$. Let h be the minimal polynomial of α over $F(\beta)$, then $\deg h = m$. Since $f(x) \in F(\beta)[x]$ and $f(\alpha) = 0$, we see that $h|f$. However, $\deg h = \deg f$ implies that $f = ah$ for some $a \in F(\beta)$. So, f is irreducible over $F(\beta)$. The converse statement follows from symmetry.

We conclude that g is irreducible over $F(\alpha)$ if and only if f is irreducible over $F(\beta)$.

(2) Since $x^4-6=(x-\sqrt[4]{6})(x+\sqrt[4]{6})(x-i\sqrt[4]{6})(x+i\sqrt[4]{6})$, we see that $L=\mathbb{Q}(\sqrt[4]{6},\sqrt[4]{6}i)=\mathbb{Q}(\sqrt[4]{6},i)$. So, $[L:\mathbb{Q}]=[\mathbb{Q}(\sqrt[4]{6},i):\mathbb{Q}(\sqrt[4]{6})][\mathbb{Q}(\sqrt[4]{6}):\mathbb{Q}]=2\times 4=8$ as x^2+1 is the minimal polynomial of i over $\mathbb{Q}(\sqrt[4]{6})$ and x^4-6 is the minimal polynomial of $\sqrt[4]{6}$ over $\mathbb{Q}$. □

Problem 158 (09J·9). Let F be a field of characteristic not 2, and let $a,b\in F$. Let L be the splitting field of $(x^2-a)(x^2-b)$.

(1) Suppose that none of a, b, or ab are perfect squares in F. Show that $\mathrm{Gal}(L/F)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

(2) Is the converse of part (1) true? Prove or disprove.

Proof. (1) Let $\pm\alpha$ be roots of x^2-a and $\pm\beta$ be roots of x^2-b, so $\alpha\neq\beta$. Then, $L=F(\alpha,\beta)$. Since ab is not a perfect square, we have $\alpha\beta\notin F$, hence $\beta\notin F(\alpha)$. So, an element of $\mathrm{Gal}(L/F)$ is determined by α,β completely. By the hypothesis, we see that x^2-a and x^2-b are minimal polynomials of α and β respectively. Let $\sigma\in\mathrm{Gal}(L/F)$, then $\sigma(\alpha)^2-a=\sigma(\alpha^2-a)=0$. So, $\sigma(\alpha)=\pm\alpha$. Similarly, $\sigma(\beta)=\pm\beta$. Define $\sigma:L\to L$ by $\alpha\mapsto\alpha$, $\beta\mapsto-\beta$ and $\tau:L\to L$ by $\alpha\mapsto-\alpha$ and $\beta\mapsto\beta$. We see that $\mathrm{Gal}(L/F)=\{\mathrm{id},\sigma,\tau,\tau\sigma\}$ is a group of order 4. By direct computation, we see that $\sigma^2=\tau^2=(\tau\sigma)^2=\mathrm{id}$. Thus, $\mathrm{Gal}(L/F)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

(2) Keep the notation as in (1). Then, $[L:F]\leqslant\deg\alpha\times\deg\beta\leqslant 2\times 2=4$. Since $|\mathrm{Gal}(L/F)|=4$ and recall that $|\mathrm{Gal}(L/F)|\leqslant[L:F]$, we see that $[L:F]=4$. Thus, it follows that $\deg\alpha=\deg\beta=2$. Thus, a,b cannot be perfect squares in F. Argue by contradiction, we assume that ab is a perfect square in F, then $\alpha\beta\in F$, i.e. $\beta\in F(\alpha)$. But this implies that $L=F(\alpha,\beta)=F(\alpha)$ and $[L:F]=\deg\alpha=2$. Thus, ab is also not a perfect square in F.

We conclude that the converse of part (1) is also true. □

Problem 159 (09A·7). Let $K\subseteq F\subseteq L$ be a tower of fields. Let $\theta\in L$ be algebraic over K and let $p(x)$ be the minimal polynomial of θ over K. Prove that $F\otimes_K K[\theta]\cong F[x]/(p(x))$ as F-algebras.

Proof. Recall that $K[\theta]\cong K(\theta)\cong K[x]/(p(x))$. It suffices to show that

$$F\otimes_K K[x]/(p(x))\cong F[x]/(p(x)).$$

Define an F-algebra homomorphism

$$\varphi:F\otimes_K K[x]/(p(x))\to F[x]/(p(x))$$

by

$$\alpha\otimes\overline{f}\mapsto\overline{\alpha f},$$

where $\alpha\in F$ and $f\in K[x]$. If $\varphi(\alpha\otimes\overline{f})=0$, i.e. $\alpha f\in(p(x))$, i.e. $\alpha f=pg$ with $g\in F[x]$. Thus, $f=p(\alpha^{-1}g)\in(p(x))$ if $\alpha\neq 0$. Thus, $\overline{f}=0$ in $K[x]/(p(x))$ if $\alpha\neq 0$. So, $\alpha\otimes\overline{f}=0$. This proves the injectivity of φ.

Let $\overline{f}\in F[x]/(p(x))$ with $f\in F[x]$. Ww may write $f(x)=a_0+a_1x+\cdots+a_nx^n$ where $a_i\in F$. So, $\varphi(a_0\otimes 1+a_1\otimes\overline{x}+\cdots+a_n\otimes\overline{x^n})=\varphi(a_0\otimes 1)+\cdots+\varphi(a_n\otimes\overline{x^n})=\overline{a_0}+\cdots+\overline{a_nx^n}=\overline{f}$. This proves the surjectivity of φ.

We conclude that $F\otimes_K K[\theta]\cong F[x]/(p(x))$ as F-algebras. □

Problem 160 (09A·8). (a) Exhibit a finite field K consisting of 8 elements. (That is, describe or construct such a field explicitly.)

(b) What is the prime subfield F of K?
(c) Is K a Galois extension of F? Describe the group $\mathrm{Aut}(K/F)$.

Proof. (a) Let $K = \mathbb{F}_2[x]/(x^3+x+1)$. Since x^3+x+1 doesn't have roots in $\mathbb{F}_2$, so it is irreducible over $\mathbb{F}_2$. Thus, K is a field consisting of $2^3 = 8$ elements.

(b) Since $\mathrm{char}(K) = 2$, the prime subfield F of K is $\mathbb{F}_2$.

(c) By the Galois theory of finite fields, K/F is Galois and $\mathrm{Aut}(K/F) \cong \langle\sigma\rangle$, where $\sigma : K \to K$ given by $x \mapsto x^2$ is the Frobenius map. □

Problem 161 (09A·9). Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree 3, and G its Galois group. Prove that if G is the cyclic group of order 3, then $f(x)$ splits completely over $\mathbb{R}$.

Proof. Let K be a splitting field of f, then $K/\mathbb{Q}$ is normal. Since $\mathrm{char}\,\mathbb{Q} = 0$, we see that $K/\mathbb{Q}$ is separable. Thus, $K/\mathbb{Q}$ is Galois. Thus, $[K : \mathbb{Q}] = |G| = 3$. Recall that every polynomial of degree 3 has a real root, so we may assume that $f(x) = (x-a)g(x)$, where $a \in \mathbb{R}$ and $g(x) \in \mathbb{R}[x]$ is of degree 2. Let $\alpha, \beta \in K$ be the two roots of $g(x)$. If $g(x)$ is irreducible over $\mathbb{R}$, we see that $\beta = \overline{\alpha}$. Thus, the conjugate map $\sigma : z \mapsto \overline{z}$ is an $\mathbb{R}$-automorphism of K and permutes α, β. In particular, $\sigma \in G$ is an element of order 2. Then, $2 \mid 3$, contradiction. Thus, $g(x)$ is not irreducible over $\mathbb{R}$, i.e. $\alpha, \beta \in \mathbb{R}$.

We conclude that f splits completely over $\mathbb{R}$. □

Problem 162 (10J·6). Find the degree of the splitting field (over $\mathbb{Q}$) of the following polynomials:
(a) $x^3 - x - 2$
(b) $(x^2-2)(x^2-5)$
(c) $(x^2-2)(x^2-5)(x^2-10)$

Proof. (a) Let F be the splitting field of $x^3 - x - 2$ over $\mathbb{Q}$. By rational root theorem, if $\frac{a}{b}$, where $a, b \in \mathbb{Z}, \gcd(a,b) = 1$, is a root of $x^3 - x - 2$, then $a|2$ and $b|1$. Thus, $\frac{a}{b} = \pm 1, \pm 2$. But one can verify that $\pm 1, \pm 2$ are not roots of $x^3 - x - 2$. So, $x^3 - x - 2$ is separable irreducible over $\mathbb{Q}$. The discriminant of $x^3 - x - 2$ is $\Delta^2 = -4(-1)^3 - 27(-2)^2 = -104$, which is not a square of an element in $\mathbb{Q}$. Thus, the Galois group of $x^3 - x - 2$ is $G \cong S_3$. Since $F/\mathbb{Q}$ is Galois, we have $[F : \mathbb{Q}] = |G| = 6$.

(b) The splitting field of $(x^2-2)(x^2-5)$ is $F = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, so $[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$ as $x^2 - 5$ is irreducible over $\mathbb{Q}(\sqrt{2})$ and $x^2 - 2$ is irreducible over $\mathbb{Q}$.

(c) The splitting field of $(x^2-2)(x^2-5)(x^2-10)$ is $F = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, by ($b$) we see that $[F : \mathbb{Q}] = 4$. □

Problem 163 (10J·8). Determine the Galois group of $x^5 - 6x + 3$ over $\mathbb{Q}$ (justify your answer).

Proof. First, consider an irreducible element $3 \in \mathbb{Z}$. Since $3|3$, $3|6$, $3 \nmid 1$, $3^2 \nmid 3$, so by Eisenstein's criterion, we see that $f(x) := x^5 - 6x + 3$ is irreducible over $\mathbb{Q}$. Let G be the Galois group of f, then $5\Big||G|$ and G is isomorphic to a transitive subgroup of S_5. We may now assume that G is a subgroup of S_5. Since $f'(x) = 5x^4 - 6 = (\sqrt{5}x^2 + \sqrt{6})(\sqrt[4]{5}x + \sqrt[4]{6})(\sqrt[4]{5}x - \sqrt[4]{6})$, we see that $f'(x) > 0$ over $(-\infty, -\sqrt[4]{\frac{6}{5}})$; $f'(x) < 0$ over $(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}})$ and $f'(x) > 0$ over $(\sqrt[4]{\frac{6}{5}}, +\infty)$. Thus, f is strictly increasing over $(-\infty, -\sqrt[4]{\frac{6}{5}})$, strictly decreasing over $(-\sqrt[4]{\frac{6}{5}}, \sqrt[4]{\frac{6}{5}})$ and strictly increasing over $(\sqrt[4]{\frac{6}{5}}, +\infty)$. Since $f(\sqrt[4]{\dfrac{6}{5}}) < 0$ and $f(-\sqrt[4]{\dfrac{6}{5}}) > 0$, f has exactly 3 real roots, i.e. f has two nonreal roots, say $a+bi$ and $a-bi$. Thus G has a transposition σ given by conjugation. We may assume that $\sigma=(12)$. Since $5\Big||G|$, G contains an element of order 5, say $\tau=(12345)$. Since S_5 is generated by (12) and (12345), we see that $G\cong S_5$. □

Problem 164 (10A·4). Suppose that $f\in K[x]$ is irreducible of degree n and F is a field extension of K such that $[F:K]=m$ and $\gcd(m,n)=1$. Show that f is irreducible over F.

Proof. Since $[F:K]<\infty$, there exists $a_1,\cdots,a_r\in F$ such that $F=K(a_1,\cdots,a_r)$. Let α be a root of f in a splitting field. Let $L_0=K(\alpha)$ and $L_i=K(\alpha,a_1,\cdots,a_i)$. Let $K_0=K$ and $K_i=K(a_1,\cdots,a_r)$. Then, $[L_i:L_{i-1}]=[K_i(\alpha):K_{i-1}(\alpha)]\leqslant[K_i:K_{i-1}]$. Then,

$$\begin{aligned}[L_r:K]=[L_r:L_0][L_0:K]&=[L_r:L_{r-1}][L_{r-1}:L_{r-2}]\cdots[L_1:L_0][L_0:K]\\&\leqslant[K_r:K_{r-1}][K_{r-1}:K_{r-2}]\cdots[K_1:K_0][L_0:K]\\&=[K_r:K_0][L_0:K]=[F:K][K(\alpha):K]=mn.\end{aligned}$$

Note that $K\subseteq F\subseteq L_r$ and $K\subseteq K(\alpha)\subseteq L_r$, we see that $m=[F:K]\mid[L_r:K]$ and $n=[K(\alpha):K]\mid[L_r:K]$. Since $\gcd(m,n)=1$, we see that $mn\mid[L_r:K]$. Thus, $[L_r:K]=mn$. Since $K\subseteq F\subseteq F(\alpha)=L_r$, we see that $[L_r:K]=[L_r:F][F:K]$. So, $[F(\alpha):F]=[L_r:F]=n$. Therefore, we conclude that f is irreducible over F. □

Problem 165 (10A·6). Find the degree of the splitting field of the polynomial x^6-7 over:

(*a*) $\mathbb{Q}$

(*b*) $\mathbb{Q}(\zeta_3)$ where ζ_3 is a primitive 3rd root of unity.

(*c*) $\mathbb{F}_3$ (the field with 3 elements).

Proof. (*a*) Since $7|7$, $7\nmid 1$, $7^2\nmid 7$, we see that x^6-7 is irreducible over $\mathbb{Q}$. Thus, $[\mathbb{Q}(\sqrt[6]{7}):\mathbb{Q}]=6$. Let $\omega=e^{\frac{\pi i}{3}}$. Then, $\sqrt[6]{7}$, $\sqrt[6]{7}\omega$,$\sqrt[6]{7}\omega^2$,$\sqrt[6]{7}\omega^3$,$\sqrt[6]{7}\omega^4$,$\sqrt[6]{7}\omega^5$ are all (distinct) roots of x^6-7. Thus, we see that $F=\mathbb{Q}(\sqrt[6]{7},\omega)$ is a splitting field of x^6-7. Note that $0=\omega^3+1=(\omega+1)(\omega^2-\omega+1)$. We see that $\omega^2-\omega+1=0$ as $\omega+1\neq0$. Since x^2-x+1 is irreducible over $\mathbb{Q}(\sqrt[6]{7})$ as $\omega\notin\mathbb{Q}(\sqrt[6]{7})$, we see that $[F:\mathbb{Q}(\sqrt[6]{7})]=2$. So, $[F:\mathbb{Q}]=[F:\mathbb{Q}(\sqrt[6]{7})][\mathbb{Q}(\sqrt[6]{7}):\mathbb{Q}]=12$. So, the degree of the splitting field of x^6-7 over $\mathbb{Q}$ is 12.

(*b*) Keep the notation as in (*a*), we see that $\zeta_3=\omega^2$ and $F=\mathbb{Q}(\sqrt[6]{7},\omega)$ is a splitting field of x^6-7. Note that $[F:\mathbb{Q}]=[F:\mathbb{Q}(\zeta_3)][\mathbb{Q}(\zeta_3):\mathbb{Q}]=12$ by (*a*). Since, ζ_3 satisfies x^2+x+1 and $\zeta_3\notin\mathbb{Q}$, we see that $[\mathbb{Q}(\zeta_3):\mathbb{Q}]=2$. So, $[F:\mathbb{Q}(\zeta_3)]=6$.

(*c*) Over $\mathbb{F}_3$, we have $x^6-7=x^6-1=(x^3+1)(x^3-1)=(x+1)(x^2-x+1)(x-1)(x^2+x+1)=(x+1)(x^2-x-2)(x-1)(x^2+x-2)=(x+1)(x+1)(x-2)(x-1)(x-1)(x+2)=(x+1)^2(x-1)^2(x+2)(x-2)$. Thus, $\mathbb{F}_3$ is a splitting field of x^6-7. So, the degree of the splitting field of x^6-7 over $\mathbb{F}_3$ is 1. □

Problem 166 (11J·5). (*a*) Let F be a field and let $R=F[t]$ be the polynomial ring. Let R' be the ring extension $R[x]/(tx-1)$ obtained by adjoining an inverse of t to R. Prove that this ring can be identified as the ring $F[x,x^{-1}]$ of Laurent polynomials which are finite linear combinations of powers of x, negative exponents included.

(*b*) Let F as before be a field. Prove that the ring $F[x,x^{-1}]$ of Laurent polynomials is a principal ideal domain.

Proof. (*a*) Note that $R[x]=F[t][x]=F[x,t]$. Consider a homomorphism $\varphi:R[x]\to F[x,x^{-1}]$ by $x\mapsto x$, $t\mapsto x^{-1}$. Clearly, $(tx-1)\subseteq\ker\varphi$ and φ is surjective. Conversely, take $f\in\ker\varphi$, then $f(x,x^{-1})=0$. Applying Euclidean algorithm, we see that $f(x,t)=g(x,t)(tx-1)+h(t)$.

So, $0 = f(x, x^{-1}) = h(x^{-1})$. Thus, $h = 0$, i.e. $f \in (tx - 1)$. Thus, $\ker \varphi = (tx - 1)$. So, $R[x]/(tx - 1) \cong F[x, x^{-1}]$.

(b) Let I be an ideal of $F[x, x^{-1}]$. Note that every Laurent polynomial in $R[x, x^{-1}]$ can be written as $p(x)x^{-m}$ for some $p \in F[x]$ and $m \in \mathbb{N}^*$. Let $f \in F[x]$ be a polynomial with least degree in I. We claim that $I = (f)$. First, $(f) \subseteq I$. Conversely, take $g(x, x^{-1}) \in I$, we may write $g(x, x^{-1}) = p(x)x^{-m}$ where $p \in F[x]$. So, $p(x) = g(x, x^{-1})x^m \in I$. Using Euclidean algorithm, we see that $p(x) = q(x)f(x) + r(x)$, with $\deg r < \deg f$. We see that $r(x) = p(x) - q(x)f(x) \in I$. Thus, $r = 0$ by our hypothesis. Thus, $p \in (f)$ and so $g(x, x^{-1}) = p(x)x^{-m} \in (f)$. □

Problem 167 (11J·8). Let $\alpha = \sqrt[3]{2}$,$\beta = \sqrt{3}$, and $\gamma = \alpha + \beta$. Let L be the field $\mathbb{Q}(\alpha, \beta)$,and let K be the splitting field of the polynomial $(x^3 - 2)(x^2 - 3)$ over $\mathbb{Q}$.

(a) Determine the irreducible polynomial f for γ over $\mathbb{Q}$, and its roots in $\mathbb{C}$.

(b) Determine the degree $[K : L]$.

(c) Determine the Galois group of $K/\mathbb{Q}$.

Proof. (a) First, we compute $[L : \mathbb{Q}]$. Since $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 3[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 6$ as $x^2 - 3$ is irreducible over $\mathbb{Q}(\alpha)$. Note that $\gamma = \sqrt{3} + \sqrt[3]{2}$. We have $(\gamma - \sqrt{3})^3 = 2$, i.e. $\gamma^3 - 3\sqrt{3}\gamma^2 + 9\gamma - 3\sqrt{3} = 2$. Thus, $\gamma^3 + 9\gamma - 2 = 3\sqrt{3} + 3\sqrt{3}\gamma^2 = 3\sqrt{3}(\gamma^2 + 1)$. So, $(\gamma^3 + 9\gamma - 2)^2 = 27(\gamma^2 + 1)^2$. So, $\gamma^6 - 9\gamma^4 - 4\gamma^3 + 27\gamma^2 - 36\gamma - 23 = 0$. Since $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta) = L$ and $[L : \mathbb{Q}] = 6$, we see that $f(x) = x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$ is the minimal polynomial of γ.

To find the roots of f, we need to solve (b) and (c) first.

(b) Let $\omega = e^{\frac{2\pi i}{3}}$. By definition, $K = \mathbb{Q}(\alpha, \omega, \beta) = L(\omega)$. Since $\omega^2 + \omega + 1 = 0$, and $x^2 + x + 1$ is irreducible over L we see that $[K : L] = 2$.

(c) So, $[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = 2 \times 6 = 12$. Note that if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then $\sigma(\alpha)$ is a root of $x^3 - 2$, $\sigma(\omega)$ is a root of $x^2 + x + 1$ and $\sigma(\beta)$ is a root of $x^2 - 3$. So, we see that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We now back to (a). Note that the normal closure of $L/\mathbb{Q}$ is the splitting field of $\{\min(\alpha, \mathbb{Q}), \min(\beta, \mathbb{Q})\} = \{x^2 - 3, x^3 - 2\}$ as $L = \mathbb{Q}(\alpha, \beta)$, i.e. K is the normal closure of $L/\mathbb{Q}$. Then, we see that $f = \min(\mathbb{Q}, \gamma)$ splits over K. Take $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then $\sigma(\gamma)$ is a root of f. Note that $\sigma(\alpha) = \alpha, \alpha\omega$ or $\alpha\omega^2$, $\sigma(\beta) = \beta$ or $-\beta$. We see that $\sigma(\gamma) = \sigma(\alpha) + \sigma(\beta)$ can take values $\alpha + \beta, \alpha\omega + \beta, \alpha\omega^2 + \beta, \alpha - \beta, \alpha\omega - \beta, \alpha\omega^2 - \beta$. Thus, the roots of f in $\mathbb{C}$ are $\alpha + \beta, \alpha\omega + \beta, \alpha\omega^2 + \beta, \alpha - \beta, \alpha\omega - \beta, \alpha\omega^2 - \beta$. □

Problem 168 (11A·3). Suppose that $[\mathbb{Q}(u) : \mathbb{Q}]$ is odd. Show that $\mathbb{Q}(u^2) = \mathbb{Q}(u)$.

Proof. Let $f = \min(\mathbb{Q}, u)$ and $g = \min(\mathbb{Q}, u^2)$. Suppose $\deg f = n$ and $\deg g = m$. Since $n = [\mathbb{Q}(u) : \mathbb{Q}] = [\mathbb{Q}(u) : \mathbb{Q}(u^2)][\mathbb{Q}(u^2) : \mathbb{Q}] = [\mathbb{Q}(u) : \mathbb{Q}(u^2)] \cdot m$. Let $h(x) = g(x^2)$, then $h(u) = g(u^2) = 0$. We see that $\deg h = 2 \deg g$ and $f | h$. Thus, we see that $[\mathbb{Q}(u) : \mathbb{Q}(u^2)] \cdot m = n = \deg f \leqslant \deg h = 2 \deg g = 2m$. Thus, $[\mathbb{Q}(u) : \mathbb{Q}(u^2)] \leqslant 2$. Since $[\mathbb{Q}(u) : \mathbb{Q}]$ is odd, $[\mathbb{Q}(u) : \mathbb{Q}(u^2)]$ cannot be 2. So, $[\mathbb{Q}(u) : \mathbb{Q}(u^2)] = 1$. We conclude that $\mathbb{Q}(u^2) = \mathbb{Q}(u)$. □

Problem 169 (11A·8). Let θ be a root of $x^3 - 3x + 1$. Prove that the splitting field of this polynomial is $\mathbb{Q}(\theta)$ and find the Galois group over $\mathbb{Q}$. Show that the other roots of this polynomial can be written in the form $a + b\theta + c\theta^2$ for some $a, b, c \in \mathbb{Q}$. Determine the other roots explicitly in terms of θ.

Proof. Let $f(x) = x^3 - 3x + 1$. By rational root test, we see that f is irreducible over $\mathbb{Q}$. Thus, we see that f is the minimal polynomial of θ over $\mathbb{Q}$.

Let K be the splitting field of f. The discriminant of f is $D = -4(-3)^3 - 27 = 81 = 9^2 \in \mathbb{Q}^2$. So, the Galois group $\mathrm{Gal}(K/\mathbb{Q}) = A_3$. Since $K/\mathbb{Q}$ is Galois, we see that $[K : \mathbb{Q}] = |A_3| = 3$. Thus, $3 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\theta)][\mathbb{Q}(\theta) : \mathbb{Q}] = 3[K : \mathbb{Q}(\theta)]$, i.e. $[K : \mathbb{Q}(\theta)] = 1$. Thus, $K = \mathbb{Q}(\theta)$ is the splitting field of f. We now show that $1, \theta, \theta^2$ is linearly independent over $\mathbb{Q}$. Indeed, if there exists a_0, a_1, a_2, not all zero, such that $a_0 + a_1\theta + a_2\theta^2 = 0$, then $f|(a_0 + a_1x + a_2x^2)$ by the properties of the minimal polynomial. Contradiction. Since $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$, we see that $1, \theta, \theta^2$ is a basis for $\mathbb{Q}(\theta)$ as a $\mathbb{Q}$-vector space. Thus, the other roots of this polynomial can be written in the form $a + b\theta + c\theta^2$ for some $a, b, c \in \mathbb{Q}$.

To determine the other roots explicitly in terms of θ, we first claim that if α is a root of f, then $\alpha^2 - 2$ is also a root of f. Indeed, $(\alpha^2 - 2)^3 - 3(\alpha^2 - 2) + 1 = \alpha^6 + 9\alpha^2 - 6\alpha^4 - 1 = (3\alpha - 1)^2 + 9\alpha^2 - 6\alpha(3\alpha - 1) - 1 = 0$.

Thus, the other two root of f are $\theta^2 - 2$ and $(\theta^2 - 2)^2 - 2 = -\theta^2 - \theta + 2$. □

Problem 170 (12J·1). Let K be a field which is an extension of degree n of another field F, i.e. $F \subseteq K$ and $[K : F] = n$. Prove that K is isomorphic to a subring of the ring of $n \times n$ matrices over F. (Thus the ring of $n \times n$ matrices over F contains an isomorphic copy of every extension of F of degree $\leqslant n$.)

Proof. For any $a \in K$, consider the left multiplication map $L_a : K \to K$ by $x \mapsto ax$. Let $e_1, \cdots, e_n$ be a basis of K over F. Then, we see that for each j,

$$L_a e_j = a_{1j}e_1 + a_{2j}e_2 + \cdots + a_{nj}e_n$$

for some $a_{ij} \in F$. Recall that we have an isomorphism $\mathcal{M} : \mathrm{End}_F(K) \cong M_n(F)$ by choosing a fixed basis $\{e_1, \cdots, e_n\}$. Thus, we can associate each $a \in K$ a matrix $(a_{ij}) = \mathcal{M}(L_a)$ over F.

Define a map $\varphi : K \to M_n(F)$ by $a \mapsto \mathcal{M}(L_a)$ as above. If $\varphi(a) = \varphi(b)$, we see that $L_a = L_b$, so $a = b$. Thus, φ is injective. It remains to prove that φ is a ring homomorphism.

(1) For any $a, b \in K$, note that $L_{a+b}x = (a + b)x = ax + bx = L_ax + L_bx = (L_a + L_b)x$ for all $x \in K$. We have $L_a + L_b = L_{a+b}$. Thus, $\varphi(a) + \varphi(b) = \mathcal{M}(L_a) + \mathcal{M}(L_b) = \mathcal{M}(L_a + L_b) = \mathcal{M}(L_{a+b}) = \varphi(a + b)$.

(2) For any $a, b \in K$, note that $L_{ab}x = (ab)x = a(bx) = L_a(bx) = (L_aL_b)x$ for all $x \in K$. Thus, we see that $L_aL_b = L_{ab}$. Thus, $\varphi(ab) = \mathcal{M}(L_{ab}) = \mathcal{M}(L_aL_b) = \mathcal{M}(L_a)\mathcal{M}(L_b) = \varphi(a)\varphi(b)$.

Thus, $K \cong \varphi(K)$, which is a subring of the ring of $n \times n$ matrices over F. Thus the ring of $n \times n$ matrices over F contains an isomorphic copy of every extension of F of degree $\leqslant n$. □

Problem 171 (12J·4). *a*) Recall that the ring of Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain and hence both a PID and a UFD. Use Eisenstein's criteria to show that $X^4 - 3$ is irreducible over the field $\mathbb{Q}(i)$.

b) What is the Galois group of the splitting field F of $X^4 - 3$ over $\mathbb{Q}(i)$ as an extension of $\mathbb{Q}$, i.e. given $\mathbb{Q} \subset \mathbb{Q}(i) \subset F$ find $\mathrm{Gal}(F/\mathbb{Q})$. Justify your answer.

c) Determine all the intermediate fields K with $\mathbb{Q} \subset K \subset F$.

Proof. (*a*) Consider the norm function $N : \mathbb{Z}[i] \to \mathbb{Z}$ given $\alpha \mapsto \alpha\overline{\alpha}$. Suppose $3 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Then, $N(\alpha)N(\beta) = N(3) = 9$. So, we may assume that $N(\alpha) = N(\beta) = 3$ or $N(\alpha) = 1$ and $N(\beta) = 9$. If $N(\alpha) = 1$ and $N(\beta) = 9$, then $\alpha\overline{\alpha} = 1$, i.e. α is a unit. Since the Diophantine equation $N(a + bi) = a^2 + b^2 = 3$ does not have integer solutions, , we see that 3 is irreducible in $\mathbb{Z}[i]$, hence a prime elelment in $\mathbb{Z}[i]$. Since $3|(-3)$, $3 \nmid 1$, $3^2 \nmid (-3)$, by Eisenstein's criteria, $X^4 - 3$ is irreducible over the field $\mathbb{Q}(i)$.

(b) Note that $X^4 - 3 = (X + \sqrt[4]{3}i)(X - \sqrt[4]{3}i)(X + \sqrt[4]{3})(X - \sqrt[4]{3})$. Thus, the splitting field F of $X^4 - 3$ over $\mathbb{Q}(i)$ is $F = \mathbb{Q}(i)(\sqrt[4]{3}i, \sqrt[4]{3}) = \mathbb{Q}(\sqrt[4]{3}, i)$. Let $\tau \in \operatorname{Gal}(F/\mathbb{Q})$, then τ maps $\sqrt[4]{3}$ to $\pm\sqrt[4]{3}$ or $\pm\sqrt[4]{3}i$; maps i to $\pm i$. Thus, $\operatorname{Gal}(F/\mathbb{Q}) = \{\text{id}, \tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6, \tau_7\}$, where

$$\begin{aligned}
\text{id} &: \sqrt[4]{3} \mapsto \sqrt[4]{3}; && i \mapsto i \\
\tau_1 &: \sqrt[4]{3} \mapsto -\sqrt[4]{3}; && i \mapsto i \\
\tau_2 &: \sqrt[4]{3} \mapsto \sqrt[4]{3}i; && i \mapsto i \\
\tau_3 &: \sqrt[4]{3} \mapsto -\sqrt[4]{3}i; && i \mapsto i \\
\tau_4 &: \sqrt[4]{3} \mapsto \sqrt[4]{3}; && i \mapsto -i \\
\tau_5 &: \sqrt[4]{3} \mapsto -\sqrt[4]{3}; && i \mapsto -i \\
\tau_6 &: \sqrt[4]{3} \mapsto \sqrt[4]{3}i; && i \mapsto -i \\
\tau_7 &: \sqrt[4]{3} \mapsto -\sqrt[4]{3}i; && i \mapsto -i
\end{aligned}$$

By direct computation, we find that $\tau_2^2 = \tau_1$, $\tau_2^3 = \tau_3$, $\tau_2^4 = \text{id}$ and $\tau_4^2 = \tau_5^2 = \tau_6^2 = \tau_7^2 = \text{id}$. So, $\langle\tau_2\rangle = \{\text{id}, \tau_2, \tau_1, \tau_3\}$ is a cyclic subgroup of $\operatorname{Gal}(F/\mathbb{Q})$. Note that $\tau_4\tau_2(\sqrt[4]{3}) = -\sqrt[4]{3}i$ and $\tau_2\tau_4(\sqrt[4]{3}) = \sqrt[4]{3}i$, we see that $\tau_2\tau_4 \neq \tau_4\tau_2$, so $\operatorname{Gal}(F/\mathbb{Q})$ is non-abelian. Since quaternion group has exact one element of order 2, we see that $\operatorname{Gal}(F/\mathbb{Q}) \cong D_4$. Moreover, $\tau_4\tau_2\tau_4 = \tau_2^{-1}$. So, $\operatorname{Gal}(F/\mathbb{Q}) = \langle \tau_2, \tau_4 | \tau_2^4 = \tau_4^2 = 1, \tau_4\tau_2\tau_4 = \tau_2^{-1}\rangle$.

(c) Note that $\operatorname{Gal}(F/\mathbb{Q}) = \langle \tau_2, \tau_4 | \tau_2^4 = \tau_4^2 = 1, \tau_4\tau_2\tau_4 = \tau_2^{-1}\rangle$. Thus, the subgroups of the Galois group are then

$$\langle\text{id}\rangle, \langle\tau_2\rangle, \langle\tau_2^2\rangle, \langle\tau_4\rangle, \langle\tau_2\tau_4\rangle, \langle\tau_2^2\tau_4\rangle, \langle\tau_2^3\tau_4\rangle, \langle\tau_2^2, \tau_4\rangle, \langle\tau_2^2, \tau_2\tau_4\rangle, G$$

i.e.

$$\langle\text{id}\rangle, \langle\tau_2\rangle, \langle\tau_1\rangle, \langle\tau_4\rangle, \langle\tau_6\rangle, \langle\tau_5\rangle, \langle\tau_7\rangle, \langle\tau_1, \tau_4\rangle, \langle\tau_1, \tau_6\rangle, G.$$

The corresponding fixed fields are

$$\mathbb{Q}(\sqrt[4]{3}, i), \mathbb{Q}(i), \mathbb{Q}(i, \sqrt{3}), \mathbb{Q}(\sqrt[4]{3}), \mathbb{Q}(\sqrt[4]{3}(1+i)), \mathbb{Q}(\sqrt[4]{3}i), \mathbb{Q}(\sqrt[4]{3}(1-i)), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{3}i), \mathbb{Q}.$$

□

Problem 172 (12A·5). Consider the polynomial $f(X) = X^4 - 2$ over the rational numbers $\mathbb{Q}$.

1) Show $f(X)$ is irreducible over $\mathbb{Q}$.

2) What is the Galois group of the splitting field K of $f(X)$ over $\mathbb{Q}$?

3) Construct two specific automorphisms of K over $\mathbb{Q}$ that generate $\operatorname{Gal}(K/\mathbb{Q})$. Hint: Consider the intermediate fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\alpha)$ where α is the real fourth root of 2.

Proof. (1) 2 is prime in $\mathbb{Z}$, $2|(-2)$, $2 \nmid 1$, $2^2 \nmid (-2)$, by Eisenstein's criterion, we see that $f(X) = X^4 - 2$ is irreducible over $\mathbb{Q}$.

(2) Note that $f(X) = X^4 - 2 = (X^2 + \sqrt{2})(X^2 - \sqrt{2}) = (X + \sqrt[4]{2}i)(X - \sqrt[4]{2}i)(X + \sqrt[4]{2})(X - \sqrt[4]{2})$. Thus, the splitting field $K = \mathbb{Q}(\sqrt[4]{2}, i)$. Let $\tau \in \operatorname{Gal}(K/\mathbb{Q})$, then τ maps $\sqrt[4]{2}$ to $\pm\sqrt[4]{2}$ or $\pm\sqrt[4]{2}i$;

maps i to $\pm i$. So, the Galois group $G_f = \mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6, \tau_7\}$, where

$$\begin{aligned}
\mathrm{id} &: \sqrt[4]{2} \mapsto \sqrt[4]{2}; \qquad i \mapsto i \\
\tau_1 &: \sqrt[4]{2} \mapsto -\sqrt[4]{2}; \qquad i \mapsto i \\
\tau_2 &: \sqrt[4]{2} \mapsto \sqrt[4]{2}i; \qquad i \mapsto i \\
\tau_3 &: \sqrt[4]{2} \mapsto -\sqrt[4]{2}i; \qquad i \mapsto i \\
\tau_4 &: \sqrt[4]{2} \mapsto \sqrt[4]{2}; \qquad i \mapsto -i \\
\tau_5 &: \sqrt[4]{2} \mapsto -\sqrt[4]{2}; \qquad i \mapsto -i \\
\tau_6 &: \sqrt[4]{2} \mapsto \sqrt[4]{2}i; \qquad i \mapsto -i \\
\tau_7 &: \sqrt[4]{2} \mapsto -\sqrt[4]{2}i; \qquad i \mapsto -i
\end{aligned}$$

(3) By direct computation, we find that $\tau_2^2 = \tau_1$, $\tau_2^3 = \tau_3$, $\tau_2^4 = \mathrm{id}$ and $\tau_4^2 = \tau_5^2 = \tau_6^2 = \tau_7^2 = \mathrm{id}$. So, $\langle \tau_2 \rangle = \{\mathrm{id}, \tau_2, \tau_1, \tau_3\}$ is a cyclic subgroup of $\mathrm{Gal}(K/\mathbb{Q})$. By direct computation, $\tau_2\tau_4 = \tau_6$, $\tau_2^2\tau_4 = \tau_5$, $\tau_2^3\tau_4 = \tau_7$. Moreover, $\tau_4\tau_2\tau_4 = \tau_2^{-1}$. So, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau_2, \tau_4 | \tau_2^4 = \tau_4^2 = 1, \tau_4\tau_2\tau_4 = \tau_2^{-1} \rangle \cong D_4$. □

Problem 173 (12A·7). Construct the finite field $\mathbb{F}_9$ with 9 elements and find a generator for the multiplicative group $\mathbb{F}_9^\times$.

Proof. Let $F = \mathbb{F}_3[x]/(x^2+1)$. Since x^2+1 has no roots in $\mathbb{F}_3$, we see that x^2+1 is irreducible over $\mathbb{F}_3$. Thus, F is a field. Every elements of F are of the form $[ax+b]$, where $a, b \in \mathbb{F}_3$. We see that F has nine eleemnts, i.e. $F \cong \mathbb{F}_9$. We see that

$$F = \mathbb{F}_9 = \{[0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2]\}.$$

We show that $[x+1]$ is a generator of $\mathbb{F}_9^\times$ by direct computation:

$$\begin{aligned}
&[x+1]^1 = [x+1]; \\
&[x+1]^2 = [x^2+2x+1] = [2x]; \\
&[x+1]^3 = [2x(x+1)] = [2x^2+2x] = [2x-2] = [2x+1]; \\
&[x+1]^4 = [2x]^2 = [4x^2] = [x^2] = [-1] = [2]; \\
&[x+1]^5 = [2(x+1)] = [2x+2]; \\
&[x+1]^6 = [2x+1]^2 = [4x^2+4x+1] = [x^2+x+1] = [x]; \\
&[x+1]^7 = [x(x+1)] = [x^2+x] = [x+2]; \\
&[x+1]^8 = [2]^2 = [4] = [1].
\end{aligned}$$

□

Problem 174 (13J·6). Let $V = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, and let $K = \mathbb{Q}(\sqrt{2})$.

(a) Show that $V/\mathbb{Q}$ is a Galois extension and determine $\mathrm{Gal}(V/\mathbb{Q})$ up to isomorphism.

(b) Let $T : V \to V$ be defined by $T(\alpha) = (1+\sqrt{2})\alpha$. Verify that T is a linear transformation of V as a vector space over $\mathbb{Q}$. By choosing a basis for V as $\mathbb{Q}$-vector space, represent T as a matrix for this basis and find its characteristic polynomial.

(c) Let Id : $K \to K$ denote the identity map. Find a K-basis of $K \otimes_{\mathbb{Q}} V$ consisting of eigenvectors for the K-linear map

$$\mathrm{Id} \otimes T : K \otimes_{\mathbb{Q}} V \to K \otimes_{\mathbb{Q}} V.$$

Present these eigenvectors as linear combinations of pure tensors.

Proof. (a) We first show that $V = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Inded, $V \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ and $(\sqrt{2}+\sqrt{3})^2 = 2+3+2\sqrt{6} \in V$. So $\sqrt{6} \in V$ and $2\sqrt{3}+3\sqrt{2} = \sqrt{6}(\sqrt{2}+\sqrt{3}) \in V$. Then, $\sqrt{2} = (2\sqrt{3}+3\sqrt{2}) - 2(\sqrt{2}+\sqrt{3}) \in V$ and $\sqrt{3} = (\sqrt{2}+\sqrt{3}) - \sqrt{2} \in V$. So, we see that $V = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Since $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the splitting field of $(x^2-2)(x^2-3)$, which is separable over $\mathbb{Q}$, we see that $V/\mathbb{Q}$ is Galois. Let $\tau \in \mathrm{Gal}(V/\mathbb{Q})$, we then have $\tau(\sqrt{2})$ is a root of x^2-2, i.e. $\tau(\sqrt{2}) = \pm\sqrt{2}$. Similarly, $\tau(\sqrt{3}) = \pm\sqrt{3}$, which imples that $\tau^2 = \mathrm{id}$. Note that $|\mathrm{Gal}(V/\mathbb{Q})| = [V : \mathbb{Q}] = [V : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$. We conclude that $\mathrm{Gal}(V/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) Let $\alpha, \beta \in V$ and $\lambda \in \mathbb{Q}$, then $T(\alpha+\beta) = (1+\sqrt{2})(\alpha+\beta) = (1+\sqrt{2})\alpha + (1+\sqrt{2})\beta = T(\alpha)+T(\beta)$ and $T(\lambda\alpha) = (1+\sqrt{2})(\lambda\alpha) = \lambda(1+\sqrt{2})\alpha = \lambda T(\alpha)$. Thus, T is a linear transformation of V as a vector space over $\mathbb{Q}$. Note that $\{1,\sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ and $\{1,\sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$, we see that $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ is a basis for V as a $\mathbb{Q}$-vector space. Then

$$\begin{aligned} T(1) &= 1+\sqrt{2} \\ T(\sqrt{2}) &= 2+\sqrt{2} \\ T(\sqrt{3}) &= \sqrt{3}+\sqrt{6} \\ T(\sqrt{6}) &= 2\sqrt{3}+\sqrt{6} \end{aligned}$$

Thus,

$$\mathcal{M}(T) = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Its characteristic polynomial is $\det(xI - \mathcal{M}(T)) = \det \begin{pmatrix} x-1 & -2 & 0 & 0 \\ -1 & x-1 & 0 & 0 \\ 0 & 0 & x-1 & -2 \\ 0 & 0 & -1 & x-1 \end{pmatrix} = [(x-1)^2-2]^2 = (x^2-2x-1)^2$.

(c) First, note that $\dim_K K \otimes_{\mathbb{Q}} V = \dim_{\mathbb{Q}} V = [V : \mathbb{Q}] = 4$ and $K \otimes_{\mathbb{Q}} V$ is generated by $\{1\otimes 1, 1\otimes\sqrt{2}, 1\otimes\sqrt{3}, 1\otimes\sqrt{6}, \sqrt{2}\otimes 1, \sqrt{2}\otimes\sqrt{2}, \sqrt{2}\otimes\sqrt{3}, \sqrt{2}\otimes\sqrt{6}\}$ as a $\mathbb{Q}$-vector space. Since $\sqrt{2}\otimes v = \sqrt{2}(1\otimes v)$, we see that $\{1\otimes 1, 1\otimes\sqrt{2}, 1\otimes\sqrt{3}, 1\otimes\sqrt{6}\}$ generates $K \otimes_{\mathbb{Q}} V$ as a K-vector space. By dimension counting, we see that $\{1\otimes 1, 1\otimes\sqrt{2}, 1\otimes\sqrt{3}, 1\otimes\sqrt{6}\}$ is a K-basis of $K \otimes_{\mathbb{Q}} V$. Thus, we see that

$$\begin{aligned} (\mathrm{Id}\otimes T)(1\otimes 1) &= 1\otimes 1 + 1\otimes\sqrt{2} \\ (\mathrm{Id}\otimes T)(1\otimes\sqrt{2}) &= 2(1\otimes 1) + 1\otimes\sqrt{2} \\ (\mathrm{Id}\otimes T)(1\otimes\sqrt{3}) &= 1\otimes\sqrt{3} + 1\otimes\sqrt{6} \\ (\mathrm{Id}\otimes T)(1\otimes\sqrt{6}) &= 2(1\otimes\sqrt{3}) + 1\otimes\sqrt{6} \end{aligned}$$

Thus,

$$\mathcal{M}(\mathrm{Id}\otimes T) = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Its characteristic polynomial is $\det(xI - \mathcal{M}(\mathrm{Id}\otimes T)) = \det \begin{pmatrix} x-1 & -2 & 0 & 0 \\ -1 & x-1 & 0 & 0 \\ 0 & 0 & x-1 & -2 \\ 0 & 0 & -1 & x-1 \end{pmatrix} =$ $[(x-1)^2-2]^2 = (x^2-2x-1)^2$. So, $1 \pm \sqrt{2}$ are eigenvalues of $\mathrm{Id}\otimes\sqrt{2}$ and the eigenspace associated to them are $E(1+\sqrt{2}, \mathrm{Id}\otimes T) = Kv_1 \oplus Kv_2$ and $E(1-\sqrt{2}, \mathrm{Id}\otimes T) = Kv_3 \oplus Kv_4$, where

$$\begin{aligned} v_1 &= \sqrt{2}\otimes 1 + 1 \otimes \sqrt{2} \\ v_2 &= \sqrt{2}\otimes \sqrt{3} + 1 \otimes \sqrt{6} \\ v_3 &= -\sqrt{2}\otimes 1 + 1 \otimes \sqrt{2} \\ v_4 &= -\sqrt{2}\otimes \sqrt{3} + 1 \otimes \sqrt{6} \end{aligned}$$

Then, v_1, v_2, v_3, v_4 is a K-basis of $K\otimes_{\mathbb{Q}} V$ consisting of eigenvectors for the K-linear map $\mathrm{Id}\otimes T$. □

Problem 175 (13J·7). Let $f, g \in \mathbb{Q}[x]$ be non-constant polynomials. Let $H \subseteq \mathbb{C}$ be the splitting field of f, let $K \subseteq \mathbb{C}$ be the splitting field of g, and let $L \subseteq \mathbb{C}$ be the splitting field of fg.

(a) Find an injective group homomorphism

$$\phi : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(H/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q}).$$

(b) For $(\sigma, \tau) \in \mathrm{Gal}(H/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$, find a necessary and sufficient criterion for (σ, τ) to be in the image of ϕ.

Proof. (a) Suppose $a_1, \cdots, a_m$ are roots of f in H and $b_1, \cdots, b_n$ are roots of g in K, then $H = \mathbb{Q}(a_1, \cdots, a_m)$, $K = \mathbb{Q}(b_1, \cdots, b_n)$ and $L = \mathbb{Q}(a_1, \cdots, a_m, b_1, \cdots, b_n)$ by the definition of splitting field. Take $\theta \in \mathrm{Gal}(L/\mathbb{Q})$, then $\theta(a_i)$ is a root of f and $\theta(b_j)$ is a root of g. Thus, $\theta|_H \in \mathrm{Gal}(H/\mathbb{Q})$ and $\theta|_K \in \mathrm{Gal}(K/\mathbb{Q})$. Consider the homomorphism

$$\phi : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(H/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$$

given by

$$\theta \mapsto (\theta|_H, \theta|_K).$$

Let $\theta \in \ker\phi$, we have $\theta|_H = \mathrm{id}_{\mathrm{Gal}(H/\mathbb{Q})}$ and $\theta|_K = \mathrm{id}_{\mathrm{Gal}(K/\mathbb{Q})}$, i.e. $\theta(a_i) = a_i$ for all $i = 1, \cdots, m$ and $\theta(b_j) = b_j$ for all $j = 1, \cdots, n$. Thus, $\theta = \mathrm{id}_{\mathrm{Gal}(L/\mathbb{Q})}$. So, ϕ is an injective group homomorphism.

(b) We claim that $(\sigma, \tau) \in \mathrm{Im}\ \phi \Leftrightarrow \sigma|_{H\cap K} = \tau|_{H\cap K}$.

$\Rightarrow$: There exists $\theta \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\theta|_H = \sigma$ and $\theta|_K = \tau$. Thus, $\sigma|_{H\cap K} = (\theta|_H)|_K = \theta|_{H\cap K} = (\theta_K)|_H = \tau|_{H\cap K}$.

$\Leftarrow$: Conversely, suppose $\sigma|_{H\cap K} = \tau|_{H\cap K}$. Since a $\mathbb{Q}$-automomorphism of L only depends on the generating set $\{a_1, \cdots, a_m, b_1, \cdots, b_n\}$, We may define a $\mathbb{Q}$-automorphism of L by

$$\begin{aligned} \theta(a_i) &= \sigma(a_i),\ i = 1, \cdots, m; \\ \theta(b_j) &= \tau(b_j),\ j = 1, \cdots, n. \end{aligned}$$

Let $\alpha \in H \cap K$, then $\alpha = \frac{f(a_1,\cdots,a_m)}{g(a_1,\cdots,a_m)} = \frac{p(b_1,\cdots,b_n)}{q(b_1,\cdots,b_n)}$ for some $f, g \in \mathbb{Q}[x_1, \cdots, x_m]$ and $p, q \in \mathbb{Q}[x_1, \cdots, x_n]$ with $g(a_1, \cdots, a_m)$ and $q(b_1, \cdots, b_n)$ non-zero. Then, we see that

$$\theta\left(\frac{f(a_1,\cdots,a_m)}{g(a_1,\cdots,a_m)}\right) = \frac{f(\theta(a_1),\cdots,\theta(a_m))}{g(\theta(a_1),\cdots,\theta(a_m))} = \frac{f(\sigma(a_1),\cdots,\sigma(a_m))}{g(\sigma(a_1),\cdots,\sigma(a_m))} = \sigma\left(\frac{f(a_1,\cdots,a_m)}{g(a_1,\cdots,a_m)}\right) = \sigma(\alpha)$$

and

$$\theta\left(\frac{p(b_1,\cdots,b_n)}{q(b_1,\cdots,b_n)}\right) = \frac{p(\theta(b_1),\cdots,\theta(b_n))}{q(\theta(b_1),\cdots,\theta(b_n))} = \frac{p(\tau(b_1),\cdots,\tau(b_n))}{q(\tau(b_1),\cdots,\tau(b_n))} = \tau\left(\frac{p(b_1,\cdots,b_n)}{q(a_1,\cdots,b_n)}\right) = \tau(\alpha).$$

Since $\alpha \in H \cap K$ and $\sigma|_{H\cap K} = \tau|_{H\cap K}$, we have $\sigma(\alpha) = \tau(\alpha)$. Thus,

$$\theta\left(\frac{f(a_1,\cdots,a_m)}{g(a_1,\cdots,a_m)}\right) = \theta\left(\frac{p(b_1,\cdots,b_n)}{q(b_1,\cdots,b_n)}\right).$$

So, θ is well-defined and $\theta \in \mathrm{Gal}(L/\mathbb{Q})$. Moreover, $\phi(\theta) = (\theta|_H, \theta|_K) = (\sigma, \tau)$ as desired. □

Problem 176 (13A·3). Let $g = x^2 + 2x - 1 \in \mathbb{F}_5[x]$.

(a) Let E be the quotient ring $\mathbb{F}_5[x]/(g)$. Show that E is a field. What is $|E|$ and why?

(b) Let α denote $x + (g) \in E$. What is the order of α in $E^\times$ and why?

Proof. (a) Note that $g(0) = -1 \neq 0$, $g(1) = 2 \neq 0$, $g(2) = 2 \neq 0$, $g(3) = 4 \neq 0$ and $g(4) = 3 \neq 0$. We see that $g \in \mathbb{F}_5[x]$ is irreducible. Thus, $E = \mathbb{F}_5[x]/(g)$ is a field. $|E| = 5^2 = 25$ as elements in E are of the form $[ax + b]$, where $a, b \in \mathbb{F}_5$.

(b) Since E is a finite field, we see that $E^\times$ is a cyclic group of order $25 - 1 = 24$. Since $\alpha^2 = [x^2] = [1-2x] = [1+3x]$, $\alpha^3 = [x(1+3x)] = [x+3(1+3x)] = [3]$, $\alpha^4 = [1+6x+9x^2] = [3x]$, $\alpha^6 = [3^2] = [4]$, $\alpha^{12} = [4^2] = [1]$. Thus, we see that the order of α is 12. □

Problem 177 (13A·6). Let p be an odd prime number, and

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x].$$

(a) Show that f is irreducible in $\mathbb{Q}[x]$ using Eisenstein's criterion.

(b) Let $\zeta = e^{2\pi i/p} \in \mathbb{C}$, and let $K = \mathbb{Q}(\zeta)$. Show that K is the splitting field of f over $\mathbb{Q}$.

(c) Let $G = \mathrm{Gal}(K/\mathbb{Q})$. For $\sigma \in G$, show that there is a unique integer $m(\sigma) \in \{1, \cdots, p-1\}$ such that

$$\sigma(\zeta) = \zeta^{m(\sigma)}.$$

(d) Prove that the function $m : G \to (\mathbb{Z}/p\mathbb{Z})^\times$ defined in (c) is a group isomorphism.

Proof. (a) Let $g(x) = f(x+1) = \frac{(x+1)^p-1}{x+1-1} = \frac{(x+1)^p-1}{x} = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}$. Since $p|\binom{p}{i}$ for all $1 \leqslant i \leqslant p-1$, $p \nmid 1$ and $p^2 \nmid \binom{p}{1}$, we see that $g(x)$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion. Note that $f = pq$ with $p, q \in \mathbb{Q}[x]$ non-zero non-units implies $g(x) = f(x+1) = p(x+1)q(x+1)$ is a product of non-zero non-units. Thus, we see that f is irreducible in $\mathbb{Q}[x]$ as g is.

(b) $f(x) = 0 \Leftrightarrow x^p - 1 = 0$ and $x - 1 \neq 0 \Leftrightarrow x = \zeta^i$ for $i = 1, 2, \cdots, p-1$. Thus, $K = \mathbb{Q}(\zeta)$ is the splitting field of f over $\mathbb{Q}$.

(c) Since $f(\zeta) = 0$, we see that $f(\sigma(\zeta)) = \sigma(f(\zeta)) = \sigma(0) = 0$ as $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Thus, $\sigma(\zeta)$ is a root of f. Recall that a $\mathbb{Q}$-automorphism of K is completely determined by the generating set, i.e. $\{\zeta\}$. Thus, there is a unique integer $m(\sigma) \in \{1, \cdots, p-1\}$ such that

$$\sigma(\zeta) = \zeta^{m(\sigma)}.$$

(d) Let $\sigma, \tau \in G$. Since $\sigma\tau(\zeta) = \sigma(\zeta^{m(\tau)}) = (\sigma(\zeta))^{m(\tau)} = (\zeta^{m(\sigma)})^{m(\tau)} = \zeta^{m(\sigma)m(\tau)}$. By ($c$) we see that $m(\sigma\tau) = m(\sigma)m(\tau)$. Thus, $m : G \to (\mathbb{Z}/p\mathbb{Z})^\times$ is a group homomorphism. Since a $\mathbb{Q}$-automorphism of K is completely determined by the generating set, i.e. $\{\zeta\}$, we see that m is injective. The surjectivity is trivial. Thus, m is a group isomorphism. □

Problem 178 (14J·6). Consider a finite field $\mathbb{F}$ with $q = p^n$ elements, where p is a prime number and n is a positive integer.

(a) Explain why every element of $\mathbb{F}$ is a root of the polynomial $x^{p^n} - x$.

(b) Show that if r divides $p^n - 1$ then all the roots of the polynomial $x^r - 1$ lie in $\mathbb{F}$.

(c) Show that the polynomial $x^4 + 1$ is reducible over any finite field. (Hint: It is enough to show it over the prime fields with p elements. Consider the cases $p = 2$ and p odd separately and observe that for p odd, $p^2 - 1$ is congruent to $0 \bmod 8$, and $x^8 - 1 = (x^4 - 1)(x^4 + 1)$.)

Proof. (a) Since $\mathbb{F}$ is a finite field, $\mathbb{F}^\times$ is a cyclic group under multiplication. Since $|\mathbb{F}^\times| = p^n - 1$, we see that for all $a \in \mathbb{F}^\times$ we have $a^{p^n-1} = 1$, i.e. $a^{p^n} - a = 0$ for all $a \in \mathbb{F}^\times$. Note that $0^{p^n} - 0 = 0$, we see that every element of $\mathbb{F}$ is a root of $x^{p^n} - x$.

(b) For any root a of $x^r - 1$, we have $a^r = 1$. If r divides $p^n - 1$, then $a^{p^n-1} = 1$, i.e. $a^{p^n} - a = 0$. Thus, roots of $x^r - 1$ must be roots of $x^{p^n} - x$. Since $x^{p^n} - x$ has at most p^n roots, its roots must lie in $\mathbb{F}$. Thus, we see that roots of $x^r - 1$ must lie in $\mathbb{F}$.

(c) Since every finite field of charateristic p contains the prime field $\mathbb{F}_p$, it suffices to show that $x^4 + 1$ is reducible over $\mathbb{F}_p$ for all prime p.

Case I: $p = 2$. Then $1^4 + 1 = 2 = 0$ in $\mathbb{F}_2$, i.e. 1 is a root of $x^4 + 1$. So, $x^4 + 1 = (x-1)(x^3 + x^2 + x + 1)$ is reducible.

Case II: p is an odd prime. Since $p^2 - 1 = (p+1)(p-1) \equiv 0 \pmod 8$, we see that all the roots of $x^8 - 1$ lie in $\mathbb{F}_{p^2}$ by (b). Since $x^8 - 1 = (x^4 - 1)(x^4 + 1)$, we see that all the roots of $x^4 + 1$ lie in $\mathbb{F}_{p^2}$. Suppose $x^4 + 1$ is irreducible over $\mathbb{F}_p$, and let $a \in \mathbb{F}_{p^2}$ be a root of $x^4 + 1$, then $[\mathbb{F}_p(a) : \mathbb{F}_p] = 4$. But $[\mathbb{F}_{p^2} : \mathbb{F}_p] = [\mathbb{F}_{p^2} : \mathbb{F}_p(a)][\mathbb{F}_p(a) : \mathbb{F}_p] = 2$, contradiction. Thus, $x^4 + 1$ is reducible over $\mathbb{F}_p$. □

Problem 179 (14J·7). Let $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$, let $\mathbb{E}$ be its splitting field contained in $\mathbb{C}$, and let G be the Galois group of $\mathbb{E}$ over $\mathbb{Q}$. Without simply citing a theorem about Galois groups of quartic polynomials, prove that G is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Find a generator for G and determine how it acts on the roots of $f(x)$. It may help to first identify an intermediate subfield $\mathbb{F}$, where $\mathbb{Q} \subsetneq \mathbb{F} \subsetneq \mathbb{E}$.

Proof. The roots of f are $\pm\sqrt{2 \pm \sqrt{2}}$. Let $\alpha = \sqrt{2 + \sqrt{2}}$, then $\alpha^2 = 2 + \sqrt{2}$, so $\sqrt{2} = \alpha^2 - 2$. Thus, $-\sqrt{2+\sqrt{2}} = -\alpha$, $\sqrt{2-\sqrt{2}} = \frac{\sqrt{2-\sqrt{2}}\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = \frac{\alpha^2-2}{\alpha}$, and $-\sqrt{2-\sqrt{2}} = -\frac{\alpha^2-2}{\alpha}$ are the other three roots of f. So, we see that $E = \mathbb{Q}(\alpha)$ and $|G| = |\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 4$ as $E/\mathbb{Q}$ is Galois.

Consider $\sigma \in G$ with $\alpha \mapsto \frac{\alpha^2-2}{\alpha}$, we see that $\sigma^2(\alpha) = \sigma\left(\frac{\alpha^2-2}{\alpha}\right) = \frac{\sigma(\alpha)^2-2}{\sigma(\alpha)} = \frac{\alpha^4-6\alpha^2+4}{\alpha^3-2\alpha} = -\alpha$. Thus, $\sigma^2 \neq \mathrm{id}_G$. Thus, σ is of order 4. So, we see that $G = \langle\sigma\rangle \cong \mathbb{Z}/4\mathbb{Z}$.

The σ above is a generator of G and we see that $\sigma = (r_1 r_2 r_3 r_4)$, where $r_1 = \alpha$, $r_2 = \frac{\alpha^2-2}{\alpha}$, $r_3 = -\alpha$ and $r_4 = -\frac{\alpha^2-2}{\alpha}$. □

Problem 180 (**14J·8**)**.** Let p and q be prime numbers.

(a) Define a surjective map $\phi : \mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q}) \to \mathbb{Q}(\sqrt{p}, \sqrt{q})$ that is both $\mathbb{Q}$-linear and a ring homomorphism.

(b) If p and q are distinct, show that ϕ is an isomorphism.

(c) If $p = q$, what is a $\mathbb{Q}$-basis for the kernel of ϕ?

Proof. (a) Define $\phi : x \otimes y \mapsto xy$ and extend it $\mathbb{Q}$-linearly to $\mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q})$, then ϕ is a ring homomorphism. Indeed, $\phi((x_1 \otimes y_1)(x_2 \otimes y_2)) = \phi(x_1x_2 \otimes y_1y_2) = x_1x_2y_1y_2 = x_1y_1x_2y_2 = \phi(x_1 \otimes y_1)\phi(x_2 \otimes y_2)$ for all $x_1, x_2 \in \mathbb{Q}(\sqrt{p})$ and $y_1, y_2 \in \mathbb{Q}(\sqrt{q})$.

Note that $\{1 \otimes 1, 1 \otimes \sqrt{q}, \sqrt{p} \otimes 1, \sqrt{p} \otimes \sqrt{q}\}$ is a basis for $\mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q})$ as $\mathbb{Q}$-vector space and $\{1, \sqrt{q}, \sqrt{p}, \sqrt{pq}\}$ generates $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ as $\mathbb{Q}$-vector space. By the definition of ϕ, we have $\phi(1 \otimes 1) = 1$, $\phi(1 \otimes \sqrt{q}) = \sqrt{q}$, $\phi(\sqrt{p} \otimes 1) = \sqrt{p}$ and $\phi(\sqrt{p} \otimes \sqrt{q}) = \sqrt{pq}$. Thus, ϕ is surjective.

(b) If $p \neq q$, we have that $\{1, \sqrt{q}, \sqrt{p}, \sqrt{pq}\}$ is a basis for $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ as $\mathbb{Q}$-vector space. So, ϕ is an isomorphism as it maps a basis of $\mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q})$ to a basis of $\mathbb{Q}(\sqrt{p}, \sqrt{q})$.

(c) If $p = q$, then $\phi : \mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{p}) \to \mathbb{Q}(\sqrt{p})$ is given by $a \otimes b \mapsto ab$. Moreover, $\{1 \otimes 1, 1 \otimes \sqrt{p}, \sqrt{p} \otimes 1, \sqrt{p} \otimes \sqrt{p}\}$ is a basis for $\mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{p})$ as $\mathbb{Q}$-vector space and $\{1, \sqrt{p}\}$ is a basis for $\mathbb{Q}(\sqrt{p})$ as $\mathbb{Q}$-vector space. Note that $p \otimes 1 - \sqrt{p} \otimes \sqrt{p} \in \ker \phi$ and $\sqrt{p} \otimes 1 - 1 \otimes \sqrt{p} \in \ker \phi$. Let $a(p \otimes 1 - \sqrt{p} \otimes \sqrt{p}) + b(\sqrt{p} \otimes 1 - 1 \otimes \sqrt{p}) = 0$ with $a, b \in \mathbb{Q}$. Then,

$$ap(1 \otimes 1) + b(\sqrt{p} \otimes 1) - b(1 \otimes \sqrt{p}) - a(\sqrt{p} \otimes \sqrt{p}) = 0.$$

Then, $a = b = 0$ as $\{1 \otimes 1, 1 \otimes \sqrt{p}, \sqrt{p} \otimes 1, \sqrt{p} \otimes \sqrt{p}\}$ is a basis for $\mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{p})$ as $\mathbb{Q}$-vector space. So, $p \otimes 1 - \sqrt{p} \otimes \sqrt{p}, \sqrt{p} \otimes 1 - 1 \otimes \sqrt{p}$ is linearly independent. By the fundamental theorem of linear algebra, we see that $\dim \ker \phi = 4 - 2 = 2$. Thus, $p \otimes 1 - \sqrt{p} \otimes \sqrt{p}, \sqrt{p} \otimes 1 - 1 \otimes \sqrt{p}$ is a $\mathbb{Q}$-basis for $\ker \phi$. □

Problem 181 (**14A·2**)**.** Suppose that $K \subset D \subset F$ where D is an integral domain and K, F are fields.

(a) Show that if $[F : K] < \infty$ then D is a field.

(b) Show, by example, that D can fail to be a field if $[F : K] = \infty$.

Proof. (a) Let $a \in D - \{0\}$, then $K[a] \subseteq D$. Since $a \in D \subseteq F$ and $[F : K] < \infty$, we see that a is algebraic over K. Thus, $K[a] = K(a) \subseteq D$. Thus, $a^{-1} \in D$. It follows that D is a field.

(b) Take $K = \mathbb{Q}$, $D = \mathbb{Q}[x]$ and $F = \mathbb{Q}(x)$. Clearly that $[F : K] = \infty$ and $\mathbb{Q}[x]$ is not a field. □

Problem 182 (**14A·7**)**.** Let F_1 and F_2 be finite dimensional Galois extension fields of K, such that $F_i \subset \overline{K}$ for some fixed algebraic closure $\overline{K}$ of K. Show that the compositum $F_1 \cdot F_2$ is also Galois over K.

Proof. Since F_i/K is Galois and $F_i \subseteq \overline{K}$, then F_i is the splitting field of some separable polynomial $f_i \in K[x]$, i.e. $F_i = K(a_1^i, a_2^i, \cdots, a_{n_i}^i)$ and $a_1^i, a_2^i, \cdots, a_{n_i}^i$ are roots of f_i. So, we see that $F_1 \cdot F_2 = K(a_1^1, \cdots, a_{n_1}^1, a_1^2, \cdots, a_{n_2}^2)$. Note that a_j^i, $j = 1, \cdots, n_i$, is a root of f_1f_2 and f_1f_2 is clearly splits over $F_1 \cdot F_2$. Thus, F_1F_2 is the splitting field of f_1f_2, which is separable over $K[x]$ as each f_i is. Thus, F_1F_2 is also Galois over K. □

Problem 183 (**15J·5**)**.** Consider the polynomial $f = x^5 - 6x + 3$ over $\mathbb{Q}$ and its splitting field F.

(a) Prove that f is irreducible over $\mathbb{Q}$.

(b) Prove that the Galois group G of the extension F over $\mathbb{Q}$ is a subgroup of S_5.

(c) Prove that G contains a 5-cycle.

(d) Prove that G contains a transposition.

(e) Determine G.

Hint 1: If you do not know how to do some part of the problem, skip it and assume it in the next part of the problem.

Hint 2: In part (d) take for granted that f has exactly 3 real roots.

Proof. (a) Take $p = 3$ and use Eisenstein's criterion.

(b) By (a) and char($\mathbb{Q}$), we see that f is separable. Thus, f has no repeated roots. Let $x_1, \cdots, x_5$ be the five distinct roots of f. Take $\tau \in G$, then $\tau(x_i)$ is a root of f as $f(\tau(x_i)) = \tau(f(x_i)) = 0$. So, τ permutes the elements of the set $X := \{x_1, \cdots, x_5\}$. Define a map

$$\Psi : G \mapsto S_X$$

by

$$\tau \mapsto \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ \tau(x_1) & \tau(x_2) & \tau(x_3) & \tau(x_4) & \tau(x_5) \end{pmatrix}.$$

Since $F = \mathbb{Q}(X)$, and a $\mathbb{Q}$-automorphism τ is determined by the action on the generating set X, we see that Ψ is injective. Thus, $G \leqslant S_X \cong S_5$.

(c) Let a be a root of f, then $[\mathbb{Q}(a) : \mathbb{Q}] = \deg f = 5$. By the fundamental theorem of Galois theory, $\mathbb{Q}(a)$ corresponds to a subgroup $H = \mathrm{Gal}(F/\mathbb{Q}(a))$ of G. We see that $[G : H] = [\mathbb{Q}(a) : \mathbb{Q}] = 5$. Thus, $5 \mid |G|$. So, by first Sylow's theorem, G contains an element of order 5, which is a 5-cycle.

(d) We have known that f has exactly 3 real roots, say x_3, x_4, x_5, which means that f has exactly two non-real roots $x_1 = a + bi$ and $x_2 = a - bi$. Consider the complex conjugation $\mathbb{C} \to \mathbb{C}$ given by $z \mapsto \overline{z}$, we see that it permutes x_1, x_2 and fixes x_3, x_4, x_5. Thus, the complex conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$, hence an $\mathbb{R}$-automorphism of F, denoted by (x_1x_2). Then, we see that G has a transposition (x_1x_2).

(e) By (c), we see that G has a 5-cycle, say $\sigma = (x_1t_2t_3t_4t_5)$, where t_2, t_3, t_4, t_5 is a permutation of $\{x_2, x_3, x_4, x_5\}$. Since $\sigma^2 = (x_1t_3t_5t_2t_4)$, $\sigma^3 = (x_1t_4t_4t_5t_3)$ and $\sigma^4 = (x_1t_5t_4t_3t_2)$, we see that there exists $1 \leqslant k \leqslant 4$ such that $\sigma^k = (x_1x_2a_3a_4a_5)$, where a_3, a_4, a_5 is a permutation of x_3, x_4, x_5. Recall that (12345) and (12) generates S_5, we see that σ^k and (x_1x_2) generates S_X. Thus, $G = S_X \cong S_5$. □

Problem 184 (15J·6). Prove that $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial over $\mathbb{Q}$.

Proof. Argue by contradiction, we assume that $\mathbb{Q}(\sqrt[4]{2})$ is the splitting field of some polynomial over $\mathbb{Q}$. Then $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is Galois and in particular normal. Then $\min(\sqrt[4]{2}, \mathbb{Q}) = x^4 - 2$ splits over $\mathbb{Q}(\sqrt[4]{2})$. However, $x^4 - 2 = (x + \sqrt[4]{2}i)(x - \sqrt[4]{2}i)(x + \sqrt[4]{2})(x - \sqrt[4]{2})$ implies that $i \in \mathbb{Q}(\sqrt[4]{2})$, contradiction. Therefore, $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial over $\mathbb{Q}$. □

Problem 185 (15A·5). Suppose $p, q \in \mathbb{N}$, p is prime, q is a prime power, and $\mathbb{F}_q$ is a field with exactly q elements. Also let $\phi^{(k)}$ denote the k-fold composition of an endomorphism ϕ with itself.

(a) Please prove that if $x^{p^n} - x - 1$ is irreducible in $\mathbb{F}_p[x]$ then

(i) $\phi(y) := y^{p^n}$ defines an automorphism of $\mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$, and

(ii) $\phi^{(p)}$ is the identity map on $\mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$.

(b) Suppose f is irreducible in $\mathbb{F}_q[x]$. Please prove that f divides $x^{q^n} - x$ if and only if the degree of f divides n.

(c) Please prove that $x^{47^n} - x - 1$ is not irreducible in $\mathbb{F}_{47}[x]$ for $n \geqslant 2$.

Proof. (a) If $x^{p^n} - x - 1$ is irreducible in $\mathbb{F}_p[x]$ then, $F := \mathbb{F}_p[x]/(x^{p^n} - x - 1)$ is a field and $[F : \mathbb{F}_p] = p^n$.

(i) Note that $\operatorname{char} F = p$. We have $\phi(y_1 + y_2) = (y_1 + y_2)^{p^n} = y_1^{p^n} + y_2^{p^n} = \phi(y_1) + \phi(y_2)$. We also have $\phi(y_1 y_2) = (y_1 y_2)^{p^n} = y_1^{p^n} y_2^{p^n} = \phi(y_1)\phi(y_2)$. Thus, $\phi : F \to F$ is a homomorphism of fields. Thus, $\ker \phi = 0$ or F. Note that $\phi(1) = 1$, we see that $\ker \phi = 0$, i.e. ϕ is injective. Note that $|F|$ is finite, we see that $|\text{Im } \phi| = |F|$ as ϕ is injective. Thus, Im $\phi = F$, i.e. ϕ is surjective. Thus, ϕ is an automorphism of F.

(ii) In F, we have $x^{p^n} = x + 1$, so $\{1, x, x^2, \cdots, x^{p^n - 1}\}$ generates F as a $\mathbb{F}_p$-vector space. Note that F is a $\mathbb{F}_p$-vector space of dimension p^n, we see that $\{1, x, x^2, \cdots, x^{p^n-1}\}$ is a $\mathbb{F}_p$-basis for F. Let $t = n^p$, then we have $\phi(x) = x^t = x + 1$ and $\phi^{(p)}(x) = x + p = x$. So, $\phi^{(p)}(x^i) = \phi^{(p)}(x)^i = x^i$ for all $1 \leqslant i \leqslant p^n - 1$. Clearly, $\phi^{(p)}(1) = 1$ and $\phi^{(p)}$ is an automorphism of F. Let $a \in \mathbb{F}_p$, we have $a^{p-1} = 1$ or $a^p = a$. So, $\phi(a) = a^{p^n} = a$. Thus, $\phi^{(p)}(a) = a$ for all $a \in \mathbb{F}_p$. Thus, for any $y \in F$, $y = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p^n-1} x^{p^n-1}$ for some $a_i \in \mathbb{F}_p$. So, $\phi^{(p)}(y) = \phi^{(p)}(a_0 + a_1 x + a_2 x^2 + \cdots + a_{p^n-1} x^{p^n-1}) = \phi^{(p)}(a_0) + \phi^{(p)}(a_1)\phi^{(p)}(x) + \cdots + \phi^{(p)}(a_{p^n-1})\phi^{(p)}(x^{p^n-1}) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p^n-1} x^{p^n-1} = y$. Thus, $\phi^{(p)}$ is the identity map on $\mathbb{F}_p[x]/\langle x^{p^n} - x - 1 \rangle$.

(b) First, note that $\mathbb{F}_{q^n}^*$ is a cyclic group of order $q^n - 1$. Thus, for all $a \in \mathbb{F}_{q^n}^*$, we have $a^{q^n - 1} = 1$. Thus, $a^{q^n} = a$ for all $a \in \mathbb{F}_{q^n}$. So, $\mathbb{F}_{q^n}$ is exactly the set of zeros of $x^{q^n} - x$ as $x^{q^n} - x$ at most q^n roots, i.e.

$$\mathbb{F}_{q^n} = \{a : a \text{ is a root of } x^{q^n} - x\}.$$

Let $m = \deg f$ and suppose f is irreducible. Let a be a root of f in its splitting field, then $K := \mathbb{F}_q(a)$ is a field containing $\mathbb{F}_q$ and $[K : \mathbb{F}_q] = m$. Since K is a finite field with q^m elements, we have that K^* is a cyclic group of order $q^m - 1$. Thus, for any $y \in K^*$, we have $y^{q^m - 1} = 1$. Thus, $y^{q^m} - y = 0$ for all $y \in K$. In particular, $a^{q^m} - a = 0$. So, we see that $a \in \mathbb{F}_{q^m}$. Thus, if L is the splitting field of f, we must have $L \subseteq \mathbb{F}_{q^m}$. In particular, $K(a) \subseteq L \subseteq \mathbb{F}_{q^m}$. Since $|K(a)| = |\mathbb{F}_{q^m}| = q^m$, we see that $L = K(a) = \mathbb{F}_{q^m}$.

If $f | (x^{q^n} - x)$, then every root a of f is a root of $x^{q^n} - x$, hence $a \in \mathbb{F}_{q^n}$. So, $K(a) \subseteq \mathbb{F}_{q^n}$. Thus, $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K(a)][K(a) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K(a)] \cdot m$. Thus, m divides n.

Conversely, suppose $m | n$, say $n = mt$. Let a be a root of f, by the discussion above, we see that $a^{q^m} = a$. Define $\psi(y) := y^{q^m}$, we see that $\psi(a) = a$. So, $a^{q^n} = a^{(q^m)^t} = \psi^{(t)}(a) = a$. So, we see that a is a root of $x^{q^n} - x$. Thus, every root of f is a root of $x^{q^n} - x$. So, f divides $x^{q^n} - x$.

(c) Let $f(x) = x^{47^n} - x - 1 \in \mathbb{F}_q[x]$ and assume that f is irreducible. Let $p = 47$. Then, $K := \mathbb{F}_p[x]/(f)$ is a field of order p^{p^n}, i.e.

$$K = \mathbb{F}_{p^{p^n}} = \{a : a \text{ is a root of } x^{p^{p^n}} - x\}.$$

So, K^* is a cyclic group of order $p^{p^n} - 1$. By $(a)(ii)$, we see that $\phi^{(p)}$ is the identity map on K. Thus, for all $y \in K$, we have $\phi^{(p)}(y) = y^{(p^n)^p} = y^{p^{np}} = y$. It follows that $y^{p^{np} - 1} = 1$. So, if we take y to be the generator of K^*, we have $(p^{p^n} - 1) | (p^{np} - 1)$. But $p^n > np$ for $n \geqslant 2$, this is a contradiction. So, f is not irreducible.

□

Problem 186 (15A·6). Suppose $p \geqslant 3$ is prime.

(a) Please prove that $F(x) := x^p$ defines an automorphism of $\mathbb{F}_{p^2}$ fixing $\mathbb{F}_p$.

(b) Please prove that the polynomial $x^p + x - 2$ has exactly p roots in $\mathbb{F}_{p^2}$.

Proof. (a) Since $\operatorname{char}(\mathbb{F}_{p^2}) = p$, we see that $F(x + y) = (x + y)^p = x^p + y^p = F(x) + F(y)$ for all $x, y \in \mathbb{F}_{p^2}$. We also have $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$. Thus, F is a homomorphism. Since

$\ker F$ is an ideal of $\mathbb{F}_{p^2}$, we see that $\ker F = 0$ or $\mathbb{F}_{p^2}$. Notice that $F(1) = 1$, we have $\ker F = 0$, i.e. F is injective. Thus $|\text{Im } F| = |\mathbb{F}_{p^2}|$, which implies that $\text{Im } F = \mathbb{F}_{p^2}$. Thus, F is surjective. By Fermat's little theorem, we see that for all non-zero $a \in \mathbb{F}_p$, we have $a^{p-1} = 1$, i.e. $F(a) = a^p = a$. So, F is an automorphism of $\mathbb{F}_{p^2}$ fixing $\mathbb{F}_p$.

(b) Note that α is a root of $x^p + x$ if and only if $\alpha+1$ is a root of $x^p + x - 2$ as $(\alpha+1)^p + \alpha + 1 - 2 = \alpha^p + \alpha$. Thus, we only need to show that $x^p + x$ has exactly p roots in $\mathbb{F}_{p^2}$. Recall that $\mathbb{F}_{p^2}^*$ is a cyclic group of order $p^2 - 1$. Thus, for all $\alpha \in \mathbb{F}_{p^2}^*$, we have $\alpha^{p^2-1} = 1$, i.e. $\alpha^{p^2} - \alpha = 0$. Thus, the set of zeros of $x^{p^2} - x$ is exactly $\mathbb{F}_{p^2}$ as $x^{p^2} - x$ has at most p^2 roots.

Note that

$$\begin{aligned}
x^{p^2} - x &= x^{p^2} + x^p - (x^p + x) \\
&= (x^p + x)(x^{p^2-p} - x^{p^2-2p+1} + x^{p^2-3p+2} + \cdots + (-1)^k x^{p^2-(k+1)p+k} + \cdots + x^{p-1}) - (x^p + x) \\
&= (x^p + x)(x^{p^2-p} - x^{p^2-2p+1} + x^{p^2-3p+2} + \cdots + (-1)^k x^{p^2-(k+1)p+k} + \cdots + x^{p-1} - 1).
\end{aligned}$$

We see that $x^p + x$ has exactly p roots in $\mathbb{F}_{p^2}$.

□

Problem 187 (15A·8). Please find an explicit univariate polynomial in $\mathbb{Z}[x]$ with Galois group $\mathbb{Z}/210\mathbb{Z}$ over $\mathbb{Q}$, and prove why your polynomial satisfies this property.

Proof. Take a prime number $p = 211$. Let $f(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p-1}{x-1}$. Let $g(x) = f(x+1) = \frac{(x+1)^p-1}{(x+1)-1} = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}$. Note that $p \mid \binom{p}{i}$ for all $1 \leqslant i \leqslant p-1$, $p \mid 1$ and $p^2 \nmid \binom{p}{1}^2$. By Eisenstein's criterion, we see that g is irreducible over $\mathbb{Q}$. Assume that f is reducible over $\mathbb{Q}$, then $f = pq$ for some non-units $p, q \in \mathbb{Q}[x]$. So, $g(x) = f(x+1) = p(x+1)q(x+1)$ and $p(x+1), q(x+1)$ are non-units. Then, g is reducible, contradiction. Thus, f is irreducible over $\mathbb{Q}$.

Let $Z(f)$ be the set of zeros of f. Then, we see that $Z(f) \subseteq Z(x^p - 1) - \{1\}$ as $(x-1)f(x) = x^p - 1$. Conversely, let $a \in Z(x^p - 1) - \{1\}$, then $(a-1)f(a) = a^p - 1 = 0$, so $f(a) = 0$ as $a \neq 1$. Thus, $a \in Z(f)$. So, $Z(f) = Z(x^p - 1) - \{1\} = \{\omega, \omega^2, \cdots, \omega^{p-1}\}$, where $\omega = e^{\frac{2\pi i}{p}}$. So, we see that $\mathbb{Q}(\omega)$ is the splitting field of f over $\mathbb{Q}$. So, $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois and $|\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg f = p - 1 = 210$. Let $\tau \in \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$, we see that $\tau(\omega) = \omega^i$ for some $1 \leqslant i \leqslant 210$. So, $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\sigma_i : 1 \leqslant i \leqslant 210\}$, where $\sigma_i : \omega \mapsto \omega^i$. Note that there exists a primitive root of modulo p. Let k be a primitive root of modulo p, then $k^j \not\equiv 1 \pmod{p}$ for all $1 \leqslant j \leqslant p-1$ and $k^{p-1} \equiv 1 \pmod{p}$. So, $\sigma_k^j(\omega) = \omega^{k^j} \not\equiv \omega$ for all $1 \leqslant j \leqslant p-1$ and $\sigma_k^{p-1}(\omega) = \omega^{k^{p-1}} = \omega$. Thus, $\sigma_k \in \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ has order $p-1$. So, $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ is cyclic of order $p - 1 = 210$. □

Problem 188 (16J·8). Let $\alpha = \sqrt{2 + \sqrt{2}}$ in $\mathbb{R}$.

(a) Find the minimal polynomial f of α over $\mathbb{Q}$.

(b) What is $[\mathbb{Q}(\alpha) : \mathbb{Q}]$?

(c) Show that $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$.

(d) Show that $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Proof. (a) Since $\alpha = \sqrt{2 + \sqrt{2}}$, we see that $\alpha^2 = 2 + \sqrt{2}$, so $(\alpha^2 - 2)^2 = 2$, i.e. $\alpha^4 - 4\alpha^2 + 2 = 0$. Let $f(x) = x^4 - 4x^2 + 2$ and $p = 2$. Then, we see that $p \mid 2$, $p \mid (-4)$, $p \nmid 1$ and $p^2 \nmid 2$. Thus f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Thus, f is the minimal polynomial of α over $\mathbb{Q}$.

(b) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 4$.

(c) The four roots of f are $\sqrt{2 + \sqrt{2}}, -\sqrt{2 + \sqrt{2}}, \sqrt{2 - \sqrt{2}}$ and $-\sqrt{2 - \sqrt{2}}$, i.e. $\alpha, -\alpha, \frac{\alpha^2-2}{\alpha}$ and $-\frac{\alpha^2-2}{\alpha}$. They are all in $\mathbb{Q}(\alpha)$. So, we see that $\mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$.

(*d*) By Galois Theory, we see that $|\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha):\mathbb{Q}] = 4$. Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ such that $\alpha \mapsto \frac{\alpha^2-2}{\alpha}$, then $\tau^2(\alpha) = -\alpha \neq \alpha$. Thus, τ is an element of order 4. Thus, $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. □

Problem 189 (16J·9). Let $f(x) \in \mathbb{Q}[x]$, and let G be the Galois group of f.

(*a*) Suppose $f(x)$ is a polynomial of degree 2. Find all possible Galois groups G and state conditions on the coefficients of f under which each such group occurs.

(*b*) Suppose $f(x)$ is a polynomial of degree 3. Prove that if G is a cyclic group of order 3, then $f(x)$ splits completely over $\mathbb{R}$.

Proof. (*a*) Suppose $f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{Q}$. The roots of f are $x_{1,2} = \dfrac{-b \pm \sqrt{\Delta}}{2a}$, where $\Delta = b^2 - 4ac$. So, the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{\Delta})$.

Case I: $\sqrt{\Delta} \in \mathbb{Q}$, i.e. $b^2 - 4ac$ is a square of a rational number, then $G = \{1\}$.

Case II: $\sqrt{\Delta} \notin \mathbb{Q}$, i.e. $b^2 - 4ac$ is not a square of a rational number, then $G \cong \mathbb{Z}/2\mathbb{Z}$.

(*b*) Let $K \subseteq \mathbb{C}$ be the splitting field of f over $\mathbb{Q}$. Recall that every polynomial of degree 3 has at least one real root, we may assume that $f(x) = (x-a)g(x)$, where $a \in \mathbb{R}$ and $g \in \mathbb{R}[x]$. Let $\alpha, \beta \in K$ be the two roots of $g(x)$. If $g(x)$ is irreducible over $\mathbb{R}$, we see that $\beta = \overline{\alpha}$. Thus, the conjugate map $\sigma : z \mapsto \overline{z}$ is an $\mathbb{R}$-automorphism of K and permutes α, β. In particular, $\sigma \in G$ is an element of order 2 as $\mathbb{R}$-automorphisms are $\mathbb{Q}$-automorphisms. Then, $2 \mid 3$, contradiction. Thus, $g(x)$ is not irreducible over $\mathbb{R}$, i.e. $\alpha, \beta \in \mathbb{R}$. Thus, $f(x)$ splits completely over $\mathbb{R}$. □

Problem 190 (16A·4). Let $p_1, p_2, \cdots, p_n$, $n \geqslant 1$, be **distinct** primes in $\mathbb{N}$.

(*a*) Show that:

(*i*) For all $n \geqslant 1$, the field $K_n = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_n})$ is Galois over $\mathbb{Q}$.

(*ii*) The Galois group $\mathrm{Aut}_{\mathbb{Q}}(K_n)$ of K_n over $\mathbb{Q}$ is isomorphic to

$$\underbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}}_{n \text{ copies}}.$$

(*iii*) There are $2^n - 1$ quadratic extensions of $\mathbb{Q}$ contained in K_n. Determine these fields explicitly in terms of the $p_i, i = 1, \cdots, n$.

(Hint: Prove (*i*), (*ii*) and (*iii*) together using induction. In order to get full credit you must give complete convincing proofs of (*i*), (*ii*), and (*iii*). Just saying “it follows by induction” is not sufficient.)

(*b*) Determine explicitly all quadratic extensions of $\mathbb{Q}$ contained in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. You may use part (*a*).

Proof. (*a*) (*i*) Note that K_n is the splitting field of $(x^2 - p_1)\cdots(x^2 - p_n)$ over $\mathbb{Q}$. Thus, K_n is Galois over $\mathbb{Q}$.

(*ii*) Let $\tau \in \mathrm{Aut}_{\mathbb{Q}}(K_n)$, then $\tau(\sqrt{p_i}) = \pm\sqrt{p_i}$ as $\tau(\sqrt{p_i})$ is a root of $x^2 - p_i$. Consider the map

$$\pi : \mathrm{Aut}_{\mathbb{Q}}(K_n) \to \underbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}}_{n \text{ copies}}$$

given by $\tau \mapsto (\tau_1, \cdots, \tau_n)$, where $\tau_i(\sqrt{p_i}) = \tau(\sqrt{p_i})$. Clearly, π is an isomorphism of groups.

(*iii*) There are $\binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = (1+1)^n - \binom{n}{0} = 2^n - 1$ quadratic extensions. These extensions are $\mathbb{Q}(\sqrt{p_{i_1}p_{i_2}\cdots p_{i_j}})$, where $1 \leqslant j \leqslant n$.

(*b*) By (*a*), we see that $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt{15}), \mathbb{Q}(\sqrt{30})$ are all quadratic extensions of $\mathbb{Q}$ contained in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. □

Problem 191 (16A·5). Suppose z is any generator for the unit group of $\mathbb{F}_{4^k}, k \geqslant 1$. Prove that $x^{2^k} + x + z^{2^k} + z$ has exactly 2^k roots in $\mathbb{F}_{4^k}$, $k \geqslant 1$. Here $\mathbb{F}_q, q \geqslant 2$, is the finite field with q elements.

Proof. Note that $\operatorname{char} \mathbb{F}_{4^k} = 2$, so $x^{2^k} + x + z^{2^k} + z = (x+z)^{2^k} + (x+z)$. Thus, a is a root of $y^{2^k} + y$ if and only if $a - z$ is a root of $x^{2^k} + x + z^{2^k} + z$. Thus, it remains to show that $y^{2^k} + y$ has exactly 2^k roots in $\mathbb{F}_{4^k}$.

Let $n = 2^k$, then $n^2 = 2^{2k} = 4^k$. Notice that $G := \mathbb{F}_{n^2}^*$ is a cyclic group of order $n^2 - 1$. Thus, for all elements $a \in G$, we have $a^{n^2-1} = 1$, i.e. $a^{n^2} = a$. Since $0^{n^2} = 0$, we see that $a^{n^2} = a$ for all $a \in \mathbb{F}_{n^2}$. Thus, the elements of $\mathbb{F}_{n^2}$ are all roots of $y^{n^2} - y$. Since $y^{n^2} - y$ has at most n^2 roots, we see that $\mathbb{F}_{n^2}$ is exactly the set of roots of $y^{n^2} - y$.

Note that

$$\begin{aligned} y^{n^2} - y &= y^{n^2} + y^n - (y^n + y) \\ &= (y^n + y)(y^{n^2-n} - y^{n^2-2n+1} + y^{n^2-3n+2} + \cdots + (-1)^k y^{n^2-(k+1)n+k} + \cdots - y^{n-1}) - (y^n + y) \\ &= (y^n + y)(y^{n^2-n} - y^{n^2-2n+1} + y^{n^2-3n+2} + \cdots + (-1)^k y^{n^2-(k+1)n+k} + \cdots - y^{n-1} - 1). \end{aligned}$$

We see that $y^n + y$ has exactly n roots in $\mathbb{F}_{n^2}$.

Thus, $x^{2^k} + x + z^{2^k} + z$ has exactly 2^k roots in $\mathbb{F}_{4^k}$, $k \geqslant 1$. □

Problem 192 (16A·9). Let $f(x) = x^5 + x + 1 \in \mathbb{Q}[x]$.

(*a*) Find the degree $[K : \mathbb{Q}]$ of the splitting field K of $f(x)$ over $\mathbb{Q}$.

(*b*) Compute the Galois group $\operatorname{Aut}_{\mathbb{Q}}(K)$ of $f(x)$.

(You can use the fact that the discriminant of $x^3 - x^2 + 1$ equals 23.)

In both parts (*a*) and (*b*) simply writing down the correct answer is **not** sufficient: you must also justify your answer fully.

Proof. (*a*) First, $f(x) = (x^3 - x^2 + 1)(x^2 + x + 1)$. Since $f'(x) = 5x^4 + 1 > 0$, we see that f is strictly increasing, which implies that f has exactly one real root. Note that $g(x) := x^2 + x + 1$ has no real roots and $h(x) := x^3 - x^2 + 1$ has exactly one real roots, say x_3. Let x_1, x_2 be the two non-real roots of h and x_4, x_5 be the two non-real roots of g. Let $L = \mathbb{Q}(x_4, x_5) = \mathbb{Q}(\sqrt{-3})$, then we see that $[L : \mathbb{Q}] = \deg g = 2$.

Note that the discriminant $\Delta^2 = 23 \in L$. Let $\sigma \in G = \operatorname{Gal}(K/L)$, then $\sigma(\Delta)^2 = \sigma(\Delta^2) = \Delta^2$. Thus, $\sigma(\Delta) = \pm\Delta$. So, $\sigma \in \operatorname{Gal}(K/L)$ is an even permutation if and only if $\sigma(\Delta) = \Delta$. Thus, by the fundamental theorem of the Galois theory, we see that the field $L(\Delta)$ corresponds to $G \cap A_3$. Indeed, $\sigma \in G \cap A_3 \Leftrightarrow \sigma$ is an even permutation $\Leftrightarrow \sigma(\Delta) = \Delta \Leftrightarrow \sigma \in \operatorname{Gal}(K/L(\Delta))$. Thus, $G \cap A_3 = \operatorname{Gal}(K/L(\Delta))$. So, $[G : G \cap A_3] = [L(\Delta) : L] = 2$ as $\Delta \notin L$. Thus, $G \cong S_3$. So, we see that $[K : L] = |G| = 3! = 6$. It follows that $[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = 6 \times 2 = 12$.

(*b*) Let $H = \mathbb{Q}(x_1, x_2, x_3)$, then we see that $K = LH$. Using the same argument as in (*a*), we see that $\operatorname{Gal}(H/\mathbb{Q}) \cap A_3 = \operatorname{Gal}(H/\mathbb{Q}(\Delta))$. So, $[\operatorname{Gal}(H/\mathbb{Q}) : \operatorname{Gal}(H/\mathbb{Q}) \cap A_3] = [\mathbb{Q}(\Delta) : \mathbb{Q}] = 2$ as $\Delta \notin \mathbb{Q}$. Thus, $\operatorname{Gal}(H/\mathbb{Q}) \cong S_3$.

Define a map

$$\Psi : \operatorname{Gal}(K/\mathbb{Q}) \mapsto \operatorname{Gal}(H/\mathbb{Q}) \times \operatorname{Gal}(L/\mathbb{Q})$$

by

$$\tau \mapsto (\tau|_H, \tau|_L).$$

Clearly, τ is injective. Since $K/\mathbb{Q}$ is Galois, we see that $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 12$. Note that $|\mathrm{Gal}(H/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})| = |\mathrm{Gal}(H/\mathbb{Q})||\mathrm{Gal}(L/\mathbb{Q})| = 3! \times 2 = 12$, we see that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(H/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \cong S_3 \times \mathbb{Z}_2$. □

Problem 193 (17J·8). Let k be a field, $a \in k$, and let p be a prime number. Prove that the polynomial $x^p + a$ is either irreducible or has a root in k.

Proof. Note that if $p = 2$, then $x^2 + a$ has no roots in k if and only if $x^2 + a$ is irreducible over k. Thus, we may assume that p is an odd prime. Let $K = \overline{k}$ be an algebraic closure of k. Let $a_1, \cdots, a_p$ be all roots of $x^p + a$ in K. Suppose $x^p + a$ is not ireeducible, i.e. $x^p + a = f(x)g(x)$ with $f, g \in k[x]$ non-trivial proper factors of $x^p + a$. We may assume that $f(x) = (x - a_1)(x - a_2)\cdots(x - a_m)$ and $g(x) = (x - a_{m+1})\cdots(x - a_p)$ such that m is even. Let $t = a_1 \cdots a_m \in k$, then we see that $t^p = a_1^p \cdots a_m^p = (-a)\cdots(-a) = a^m$. Sicne $\gcd(p, m) = 1$, there exist $s, r \in \mathbb{Z}$ such that $sp + rm = 1$. So, $(a^s t^r)^p = a^{sp} a^{mr} = a^{sp+mr} = a$. So, we see that $-a^s t^r$ is a root of $x^p + a$ in k. □

Problem 194 (17J·9). Let $g = (x^2 - 2)(x^2 + 3) \in \mathbb{Q}[x]$. Let E be the splitting field of g over $\mathbb{Q}$.

(a) What is $[E : \mathbb{Q}]$?

(b) Construct the Galois group $G = \mathrm{Gal}(E/\mathbb{Q})$.

(c) Show explicitly the correspondence between the intermediate fields $\mathbb{Q} \subseteq F \subseteq E$ and the subgroups $H \leqslant G$.

Proof. (a) By definition $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}i)$, so $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. Note that $x^2 + 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, we see that $[E : \mathbb{Q}(\sqrt{2})] = 2$. So, $[E : \mathbb{Q}] = 2 \times 2 = 4$.

(b) Let $\tau \in \mathrm{Gal}(E/\mathbb{Q})$, then $\tau(\sqrt{2}) = \pm\sqrt{2}$ and $\tau(\sqrt{3}i) = \pm\sqrt{3}i$. Thus, $\mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}, \tau_1, \tau_2, \tau_3\}$, where

$$\begin{aligned}
\tau_1 &: \sqrt{2} \mapsto -\sqrt{2}, \quad \sqrt{3}i \mapsto \sqrt{3}i \\
\tau_2 &: \sqrt{2} \mapsto \sqrt{2}, \quad \sqrt{3}i \mapsto -\sqrt{3}i \\
\tau_3 &: \sqrt{2} \mapsto -\sqrt{2}, \quad \sqrt{3}i \mapsto -\sqrt{3}i
\end{aligned}$$

So, $\tau^2 = \mathrm{id}$ for all $\tau \in G$. Thus, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) Subgroups of $G = \mathrm{Gal}(E/\mathbb{Q})$ are $\{\mathrm{id}\}$, $\langle\tau_1\rangle$, $\langle\tau_2\rangle$, $\langle\tau_3\rangle$ and G.

First, the fixed field of $\{\mathrm{id}\}$ is E and the fixed field of G is $\mathbb{Q}$.

The fixed field of $\langle\tau_1\rangle$ is $\mathbb{Q}(\sqrt{3}i)$. Indeed, $\mathbb{Q}(\sqrt{3}i)$ is fixed by τ_1, i.e. $\langle\tau_1\rangle \subseteq \mathrm{Gal}(E/\mathbb{Q}(\sqrt{3}i))$, and $|\mathrm{Gal}(E/\mathbb{Q}(\sqrt{3}i))| = [E : \mathbb{Q}(\sqrt{3}i)] = 2 = |\langle\tau_1\rangle|$.

Using a similar argument, we see that the fixed field of $\langle\tau_2\rangle$ is $\mathbb{Q}(\sqrt{2})$ and the fixed field of $\langle\tau_3\rangle$ is $\mathbb{Q}(\sqrt{6}i)$. □

Problem 195 (17A·7). Let $\alpha = \sqrt{1 + \sqrt{2}} \in \mathbb{R}$.

(a) What is the irreducible polynomial of α over $\mathbb{Q}$?

(b) Prove that $\mathbb{Q}(\alpha)$ is not the splitting field over $\mathbb{Q}$ of any polynomial in $\mathbb{Q}[x]$.

Proof. (a) Since $\alpha = \sqrt{1 + \sqrt{2}}$, we see that $\alpha^2 - 1 = \sqrt{2}$ and $(\alpha^2 - 1)^2 - 2 = 0$, i.e. $\alpha^4 - 2\alpha^2 - 1 = 0$. Let $f(x) = x^4 - 2x^2 - 1$ and $g(x) = f(x-1) = (x-1)^4 - 2(x-1)^2 - 1 = x^4 - 4x^3 + 4x^2 - 2$. Take $p = 2$, then $p \mid (-2)$, $p \mid 4$, $p \mid (-4)$, $p \nmid 1$ and $p^2 \nmid (-2)$. So, by Eisenstein's criterion, we see that g is irreducible over $\mathbb{Q}$. Thus, f is also irreducible over $\mathbb{Q}$.

(b) The roots of f are $\pm\sqrt{1 + \sqrt{2}}$ and $\pm\sqrt{1 - \sqrt{2}}$. Note that $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ and $\pm\sqrt{1 - \sqrt{2}} \notin \mathbb{R}$. Thus, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not normal. Thus, $\mathbb{Q}(\alpha)$ is not the splitting field over $\mathbb{Q}$ of any polynomial in $\mathbb{Q}[x]$ since the splitting field over $\mathbb{Q}$ of any polynomial in $\mathbb{Q}[x]$ is Galois over $\mathbb{Q}$. □

Problem 196 (**17A·8**)**.** Let $f = x^3 - 2 \in \mathbb{Q}[x]$, and let $g = x^2 - 2 \in \mathbb{Q}[x]$. Let K, L, and M be subfields of $\mathbb{C}$ such that K is the splitting field of f, L is the splitting field of g, and M is the splitting field of fg.

(a) Construct an automorphism $\beta \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\beta(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ and $\beta(\omega) = \omega^2$, where $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ is a cube root of unity.

(b) What is the order of β in $\mathrm{Gal}(K/\mathbb{Q})$? What is the fixed field of the subgroup generated by β?

(c) Determine $[M : \mathbb{Q}]$.

(d) Construct an element $\rho \in \mathrm{Gal}(M/\mathbb{Q})$ that has order 6, and determine its action on the roots of fg.

(e) What is the fixed field of the subgroup generated by the element ρ you constructed in (d)?

Proof. First, the roots of f are $\sqrt[3]{2}, \omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, so $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. The roots of g are $\pm\sqrt{2}$, so $L = \mathbb{Q}(\sqrt{2})$. Then, $M = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \omega)$. Thus, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \times 3 = 6$ and $[L : \mathbb{Q}] = 2$.

(a) Note that $x^2 + x + 1$ is the minimal polynomial of ω and $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$. If $\tau : K \to K$ is a $\mathbb{Q}$-endomorphism, then τ is completely determined by its values on the generating set $\{\sqrt[3]{2}, \omega\}$. So, $\tau(\sqrt[3]{2})$ is a root of $x^3 - 2$, i.e. $\tau(\sqrt[3]{2})$ can be $\sqrt[3]{2}, \omega\sqrt[3]{2}$ or $\omega^2\sqrt[3]{2}$. Similarly, $\tau(\omega)$ can be ω or ω^2. So, there is a $\mathbb{Q}$-endomorphism $\beta : K \to K$ such that $\beta(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ and $\beta(\omega) = \omega^2$.

Note that $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \omega\sqrt[3]{2}, \omega(\sqrt[3]{2})^2\}$ is a $\mathbb{Q}$-basis for K as a vector space. We see that the action of β on this basis is

$$\begin{aligned} 1 &\mapsto 1 \\ \sqrt[3]{2} &\mapsto \omega\sqrt[3]{2} \\ (\sqrt[3]{2})^2 &\mapsto -(\sqrt[3]{2})^2 - \omega(\sqrt[3]{2})^2 \\ \omega &\mapsto -1 - \omega \\ \omega\sqrt[3]{2} &\mapsto \sqrt[3]{2} \\ \omega(\sqrt[3]{2})^2 &\mapsto \omega(\sqrt[3]{2})^2 \end{aligned}$$

Since $\{1, \omega\sqrt[3]{2}, -(\sqrt[3]{2})^2 - \omega(\sqrt[3]{2})^2, -1 - \omega, \sqrt[3]{2}, \omega(\sqrt[3]{2})^2\}$ is also a $\mathbb{Q}$-basis for K, we see that β is bijective. Thus, $\beta \in \mathrm{Gal}(K/\mathbb{Q})$ is the desired automorphism.

(b) Let $G = \mathrm{Gal}(K/\mathbb{Q})$. By direct computation, $\beta^2(\sqrt[3]{2}) = \sqrt[3]{2}$ and $\beta^2(\omega) = \omega$. Thus, β is of order 2. Let F be the fixed field of $\langle\beta\rangle$. Note that $\beta(\omega^2\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$, we have $\mathbb{Q}(\omega^2\sqrt[3]{2}) \subseteq F$. Since $[F : \mathbb{Q}] = [G : \langle\beta\rangle] = 3$ and $[\mathbb{Q}(\omega^2\sqrt[3]{2}) : \mathbb{Q}] = 3$ as the minimal polynomial of $\omega^2\sqrt[3]{2}$ is $f(x) = x^3 - 2$. Thus, we see that $F = \mathbb{Q}(\omega^2\sqrt[3]{2})$.

(c) $[M : \mathbb{Q}] = [M : K][K : \mathbb{Q}] = 2 \times 6 = 12$. Indeed, $M = K(\sqrt{2})$ and $x^2 - 2$ is irreducible over K.

(d) Define $\rho \in \mathrm{Gal}(M/\mathbb{Q})$ by $\rho(\sqrt[3]{2}) = \omega\sqrt[3]{2}$, $\rho(\omega) = \omega$ and $\rho(\sqrt{2}) = -\sqrt{2}$. By direct computation, we see that $\rho^6(\sqrt[3]{2}) = \sqrt[3]{2}$, $\rho(\omega) = \omega$ and $\rho^6(\sqrt{2}) = \sqrt{2}$. Thus, $\rho^6 = \mathrm{id}$. So, the order of ρ can be $1, 2, 3$ or 6. Again, by direct computation, we see that $\rho^2(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$, $\rho^3(\sqrt{2}) = -\sqrt{2}$, so $\rho^2 \neq \mathrm{id}$ and $\rho^3 \neq \mathrm{id}$. Thus, we conclude that ρ is of order 6.

(e) Let F be the fixed field of $\langle\rho\rangle$, then $[F : \mathbb{Q}] = [\mathrm{Gal}(M/\mathbb{Q}) : \langle\rho\rangle] = 2$. Note that $\rho(\omega) = \omega$, we see that $\mathbb{Q}(\omega) \subseteq F$. Since $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, we see that $F = \mathbb{Q}(\omega)$. □

Problem 197 (**18J·8**)**.** Is it possible to have a field extension $F \subset K$ with degree 2, $[K : F] = 2$, where both fields are isomorphic to the field $\mathbb{Q}(x)$ of rational functions in one variable? Either exhibit such an extension or prove that it is impossible.

Proof. Take $K = \mathbb{Q}(x)$ and $F = \mathbb{Q}(x^2) \cong \mathbb{Q}(x)$. We claim that $[K : F] = 2$. Consider the polynomial $f(t) = t^2 - x^2 \in \mathbb{Q}(x^2)[t]$, which is irreducible over $\mathbb{Q}(x^2)$. Note that f is the minimal polynomial of x over $\mathbb{Q}(x^2)$ and $K = F(x)$, we see that $[K : F] = \deg f = 2$. □

Problem 198 (18J·9). Let $f(x) = x^5 - 2 \in \mathbb{Q}[x]$.

(*a*) Let E be the splitting field of f over $\mathbb{Q}$. Show that E contains both $\mathbb{Q}(\sqrt[5]{2})$ and $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/5}$. What is $[E : \mathbb{Q}]$?

(*b*) Prove that there exist $\sigma, \tau \in \mathrm{Gal}(E/\mathbb{Q})$ such that

(*i*) $\sigma(\sqrt[5]{2}) = \zeta\sqrt[5]{2}$ and $\sigma(\zeta) = \zeta$.

(*ii*) $\tau(\sqrt[5]{2}) = \sqrt[5]{2}$ and $\tau(\zeta) = \zeta^2$.

Use this to show that every element in $\mathrm{Gal}(E/\mathbb{Q})$ can be expressed uniquely as $\sigma^i\tau^j$ for $0 \leqslant i \leqslant 4$ and $0 \leqslant j \leqslant 3$. Hint: Note that every automorphism is determined by its action on $\sqrt[5]{2}$ and ζ. Show that these automorphisms act differently on these elements of E.

(*c*) Let $H \subseteq \mathrm{Gal}(E/\mathbb{Q})$ be the subgroup generated by $\tau\sigma$. What is the fixed field of H?

Proof. (*a*) The roots of f are $\sqrt[5]{2}, \zeta\sqrt[5]{2}, \zeta^2\sqrt[5]{2}, \zeta^3\sqrt[5]{2}, \zeta^4\sqrt[5]{2}$. Thus, by definition, we see that $E = \mathbb{Q}(\sqrt[5]{2}, \zeta\sqrt[5]{2}, \zeta^2\sqrt[5]{2}, \zeta^3\sqrt[5]{2}, \zeta^4\sqrt[5]{2}) = \mathbb{Q}(\sqrt[5]{2}, \zeta)$. So, E contains both $\mathbb{Q}(\sqrt[5]{2})$ and $\mathbb{Q}(\zeta)$. Note that $\zeta^5 - 1 = (\zeta-1)(\zeta^4+\zeta^3+\zeta^2+\zeta+1) = 0$ and $\zeta \neq 1$. We have $g(\zeta) = 0$, where $g(x) = x^4+x^3+x^2+x+1$. Consider $h(x) = g(x+1) = \frac{(x+1)^5-1}{(x+1)-1} = x^4 + \binom{5}{4}x^3 + \binom{5}{3}x^2 + \binom{5}{2}x + \binom{5}{1}$. Take $p = \binom{5}{1} = 5$, then $p \mid \binom{5}{i}$ for all $1 \leqslant i \leqslant 4$, $p \nmid 1$, $p^2 \nmid \binom{5}{1}$. So, h is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Thus, g is also irreducible over $\mathbb{Q}$. Thus, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg g = 4$. Then, $[E : \mathbb{Q}] = [E : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = 4[E : \mathbb{Q}(\zeta)]$, i.e. $4 \mid [E : \mathbb{Q}]$. Similarly, $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[5]{2})][\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5[E : \mathbb{Q}(\sqrt[5]{2})]$, i.e. $5 \mid [E : \mathbb{Q}]$. Thus, $20 \mid [E : \mathbb{Q}]$. Let $h = \min(\zeta, \mathbb{Q}(\sqrt[5]{2})) \in \mathbb{Q}(\sqrt[5]{2})[x]$ and $h' = \min(\zeta, \mathbb{Q}) \in \mathbb{Q}[x]$. Then, $h' \in \mathbb{Q}(\sqrt[5]{2})[x]$ and so $h \mid h'$. Thus, $[E : \mathbb{Q}(\sqrt[5]{2})] \leqslant [\mathbb{Q}(\zeta) : \mathbb{Q}]$ and it follows that $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[5]{2})][\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] \leqslant [\mathbb{Q}(\zeta) : \mathbb{Q}][\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 20$ as f is irreducible over $\mathbb{Q}$.

So, we see that $[E : \mathbb{Q}] = 20$.

(*b*) Let $\chi = \sqrt[5]{2}$. Since the action of σ on a set of generators of E is characterized by

$$\chi \mapsto \zeta\chi \mapsto \zeta^2\chi \mapsto \zeta^3\chi \mapsto \zeta^4\chi,$$

$$\chi^2 \mapsto \zeta^2\chi^2 \mapsto \zeta^4\chi^2 \mapsto \zeta\chi^2 \mapsto \zeta^3\chi^2,$$

$$\chi^3 \mapsto \zeta^3\chi^3 \mapsto \zeta\chi^3 \mapsto \zeta^4\chi^3 \mapsto \zeta^2\chi^3,$$

$$\chi^4 \mapsto \zeta^4\chi^4 \mapsto \zeta^3\chi^4 \mapsto \zeta^2\chi^4 \mapsto \zeta\chi^4,$$

and fixing $1, \zeta, \zeta^2, \zeta^3, \zeta^4$. Thus, we see that $\sigma : E \to E$ is surjective as a $\mathbb{Q}$-linear map and hence bijective. Thus, there exist $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\sigma(\sqrt[5]{2}) = \zeta\sqrt[5]{2}$ and $\sigma(\zeta) = \zeta$.

Using a similar arguement, we see that there exist $\tau \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\tau(\sqrt[5]{2}) = \sqrt[5]{2}$ and $\tau(\zeta) = \zeta^2$.

Thus, we see that $\sigma^i\tau^j \in \mathrm{Gal}(E/\mathbb{Q})$ for all $0 \leqslant i \leqslant 4$ and $0 \leqslant j \leqslant 3$. Let X be the set of elements of the form $\sigma^i\tau^j$, where $0 \leqslant i \leqslant 4$ and $0 \leqslant j \leqslant 3$. Then, $X \subseteq \mathrm{Gal}(E/\mathbb{Q})$ and $|X| = 20$. Since $E/\mathbb{Q}$ is Galois, we have $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 20$ by (*a*). Thus, every element in $\mathrm{Gal}(E/\mathbb{Q})$ can be expressed uniquely as $\sigma^i\tau^j$ for $0 \leqslant i \leqslant 4$ and $0 \leqslant j \leqslant 3$.

(*c*) Let $G = \mathrm{Gal}(E/\mathbb{Q})$ and F be the fixed field of $H = \langle\tau\sigma\rangle$. Note that $\tau\sigma(\zeta^3\chi) = \tau(\zeta^4\chi) = \tau(\zeta)^4\tau(\chi) = \zeta^8\chi = \zeta^3\chi$. Then, $\mathbb{Q}(\zeta^3\chi) \subseteq F$.

We now calculate the order of $\theta := \tau\sigma$. Note that $\theta(\chi) = \tau(\zeta\chi) = \zeta^2\chi$ and $\theta(\zeta) = \tau(\zeta) = \zeta^2$. Then, the action of θ on ζ, χ is characterized by

$$\chi \mapsto \zeta^2\chi \mapsto \zeta\chi \mapsto \zeta^4\chi \mapsto \chi$$

and

$$\zeta \mapsto \zeta^2 \mapsto \zeta^4 \mapsto \zeta^3 \mapsto \zeta.$$

Thus, the order of θ is 4, and $|H| = 4$.

Since $(\zeta^3\chi)^5 = \chi^5 = 2$, we see that $\zeta^3\chi$ is a root of $f(x) = x^5 - 2$, which is irreducible. Thus, $[\mathbb{Q}(\zeta^3\chi) : \mathbb{Q}] = 5$. Note that $[F : \mathbb{Q}] = [G : H] = 5$. We conclude that $F = \mathbb{Q}(\zeta^3\chi)$. □

Problem 199 (18A·8). Let K be a field of characteristic 0 such that every odd degree polynomial $f(x) \in K[x]$ has a root in K. Let L/K be a finite extension. Show that $[L : K]$ is a power of 2.

Proof. We first show that $[L : K]$ is even if $L \neq K$. Indeed, if $[L : K]$ is odd, take $a \in L - K$, then $[K(a) : K]$ is odd. Let $f(x) = \min(a, K)$, then $\deg f = \deg a = [K(a) : K]$ is odd. Since f is irreducible over K, we see that f is linear. Thus, $K(a) = K$ and $a \in K$. This is a contradiction.

By replacing L with the normal closure of L/K, we may assume that L/K is normal. Hence, L/K is finite Galois as $\text{char}(K) = 0$. Let $G = \text{Gal}(L/K)$, then $|G| = 2^n k$ for some $k \in \mathbb{N}^*$ and $\gcd(2, k) = 1$. By first Sylow's theorem, we see that G has a subgroup of order 2^n, say H. Let F be the fixed field of H, then by the fundamental theorem of Galois theory, we see that $[F : K] = [G : H] = k$ is odd. Thus, by the discussion above, we see that $F = K$ and $k = 1$. Thus, $[L : K]$ is a power of 2. □

Problem 200 (18A·9). Find the Galois group of the splitting field of $x^4 - 3$ over $\mathbb{Q}[\sqrt{-1}]$.

Proof. Let $\chi = \sqrt[4]{3}$, then the roots of $x^4 - 3$ are $\chi, \chi i, \chi i^2, \chi i^3$. Thus, the splitting field E of $x^4 - 3$ over $\mathbb{Q}(i)$ is $E = \mathbb{Q}(i, \chi)$. Then, we see that $[E : \mathbb{Q}(i)] \leqslant \deg(x^4 - 3) = 4$. Let $\tau \in G = \text{Gal}(E/\mathbb{Q}(i))$ such that $\chi \mapsto \chi i$. Then, $\tau^2(\chi) = \tau(\chi i) = i\tau(\chi) = i \cdot \chi i = -\chi$, $\tau^3(\chi) = \tau(-\chi) = -\tau(\chi) = -\chi i$ and $\tau^4(\chi) = \tau(-\chi i) = -i\tau(\chi) = (-i) \cdot (\chi i) = \chi$. Thus, τ is an element of order 4 in G. This means that $[E : \mathbb{Q}(i)] = |G| \geqslant 4$. Thus, $[E : \mathbb{Q}(i)] = 4$ and $G = \langle \tau \rangle \cong \mathbb{Z}_4$. □

Problem 201 (19J·7). Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree 3, and G its Galois group. Prove that if G is the cyclic group of order 3, then $f(x)$ splits completely over $\mathbb{R}$.

Proof. Let E be the splitting field of F over $\mathbb{Q}$, then $G = \text{Gal}(E/\mathbb{Q})$. Since f is of degree 3, we see that $f(x) = (x - a)g(x)$ for some $a \in \mathbb{R}$ and $g \in \mathbb{R}[x]$. If g is irreducible over $\mathbb{R}$, then g has exactly two non-real roots. Then the complex conjugation map $\sigma : \mathbb{C} \to \mathbb{C}$ is an $\mathbb{R}$-automorphism and it follows that $\sigma|_E$ is a $\mathbb{Q}$-automorphism. Thus, $\sigma|_E \in G$. Note that $\sigma|_E$ is of order 2 and $|G| = 3$. This is impossible as $2 \nmid 3$. So, g is reducible over $\mathbb{R}$, i.e. $f(x)$ splits completely over $\mathbb{R}$. □

Problem 202 (19J·8). Let p be a prime number and let F_p denote the finite field of order p. Let $f(x) \in F_p[x]$ be the polynomial $f(x) := x^p - x + 1$, and let K be the splitting field of $f(x)$ over F_p. Let $\alpha \in K$ be any root of f.

(a) Let $\beta \in K$ be another root of f. Prove that $\alpha - \beta \in F_p$.

(b) Prove that $K = F_p(\alpha)$.

Proof. (a) Since $\alpha^p - \alpha + 1 = 0$ and $\beta^p - \beta + 1 = 0$. Thus, $(\alpha^p - \beta^p) - (\alpha - \beta) = (\alpha^p - \alpha + 1) - (\beta^p - \beta + 1) = 0$. So, we see that $(\alpha - \beta)^p = \alpha - \beta$. Note that all elements of F_p are roots of $x^p - x$ and $x^p - x$ has at most p roots. We see that $\alpha - \beta \in F_p$.

(b) Let $a_1, \cdots, a_p$ be all roots of f in K, where $a_1 = \alpha$. Then, $K = F_p(a_1, \cdots, a_p)$. By ($a$), $\alpha - a_i \in F_p$, i.e. $a_i = \alpha + b_i$ for some $b_i \in F_p$. Thus, $a_i \in F_p(\alpha)$. Thus, $K = F_p(\alpha)$. □

Problem 203 (19J·9). Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Let P denote the set of all odd prime numbers, and for $p \in P$ let r_p denote p-th root of 7 in $\mathbb{R}$. Given a subset A of P, show that there exists an automorphism σ of $\overline{\mathbb{Q}}$ such that $\sigma(r_p) = r_p$ for all $p \in A$, and $\sigma(r_p) \neq r_p$ for all $p \in P - A$.

Proof. First, we have $[\mathbb{Q}(r_p) : \mathbb{Q}] = p$ for all $p \in P$ as $x^p - 7$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion.

Let $X_A = \{r_p \in \overline{\mathbb{Q}} : p \in A\}$ and $E = \mathbb{Q}(X_A)$. For any $p \in P - A$, let $f_p(x) = \min(r_p, E)$ be the minimal polynomial of r_p over E. If $\deg f_p = 1$ for some $p \in P - A$, then $r_p \in E$. Thus, $r_p \in \mathbb{Q}(r_{p_1}, \cdots, r_{p_n})$, where $p_1, \cdots, p_n \in A$. So, $\mathbb{Q}(r_p) \subseteq \mathbb{Q}(r_{p_1}, \cdots, r_{p_n})$. Note that $[\mathbb{Q}(r_{p_1}, \cdots, r_{p_n}) : \mathbb{Q}] \leqslant \prod_{i=1}^{n}[\mathbb{Q}(r_{p_i}) : \mathbb{Q}] = p_1 \cdots p_n$. Then, by $\mathbb{Q}(r_{p_i}) \subseteq \mathbb{Q}(r_{p_1}, \cdots, r_{p_n})$ we see that $p_i \mid [\mathbb{Q}(r_{p_1}, \cdots, r_{p_n}) : \mathbb{Q}]$. Since $\gcd(p_1, \cdots, p_n) = 1$, we have $p_1 \cdots p_n \mid [\mathbb{Q}(r_{p_1}, \cdots, r_{p_n}) : \mathbb{Q}]$. Thus, we see that $[\mathbb{Q}(r_{p_1}, \cdots, r_{p_n}) : \mathbb{Q}] = p_1 \cdots p_n$. Since $[\mathbb{Q}(r_p) : \mathbb{Q}] = p$, we see that $p \mid p_1 \cdots p_n$, contradiction. Thus, $\deg f_p > 1$. We may choose another root $s_p \neq r_p$ of each $f_p(x)$. By isomorphism extension theorem, we see that there exists an isomorphism $\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ such that $\sigma(r_p) = s_p$ for each $p \in P - A$ and $\sigma|_E = \text{id}$. So, we see that $\sigma(r_p) = r_p$ for all $p \in A$. □

Problem 204 (19A·8). Let $f(x) = x^4 - 4$ in $\mathbb{Q}[x]$.

(a) Find the splitting field K of f over $\mathbb{Q}$.

(b) Find the Galois group $\text{Gal}(K/\mathbb{Q})$.

Proof. (a) The roots of f are $\sqrt{2}, \sqrt{2}i, -\sqrt{2}, -\sqrt{2}i$. Thus, $K = \mathbb{Q}(\sqrt{2}, \sqrt{2}i, -\sqrt{2}, -\sqrt{2}i) = \mathbb{Q}(\sqrt{2}, \sqrt{2}i) = \mathbb{Q}(\sqrt{2}, i)$.

(b) Note that $\min(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ and $\min(i, \mathbb{Q}) = x^2 + 1$. Let $\tau \in \text{Gal}(K/\mathbb{Q})$, then $\tau(\sqrt{2})$ is a root of $x^2 - 2$ and $\tau(i)$ is a root of $x^2 + 1$. Thus, $\tau(\sqrt{2}) = \pm\sqrt{2}$, $\tau(i) = \pm i$.

So, $\text{Gal}(K/\mathbb{Q}) = \{\text{id}, \tau_1, \tau_2, \tau_3\}$, where

$$\tau_1 : \sqrt{2} \mapsto \sqrt{2}, i \mapsto -i$$
$$\tau_2 : \sqrt{2} \mapsto -\sqrt{2}, i \mapsto i$$
$$\tau_3 : \sqrt{2} \mapsto -\sqrt{2}, i \mapsto -i$$

By direct computation, we see that $\tau_i^2 = \text{id}$ for all $i = 1, 2, 3$. Thus, we see that $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Problem 205 (19A·9). Let K be a field extension of F such that $K = F(\alpha, \beta)$ for elements α, β of K. Suppose $[F(\alpha) : F] = m$ and $[F(\beta) : F] = n$ for some positive integers m, n.

(a) Prove that if m, n are relatively prime, then $[K : F] = mn$.

(b) Does the conclusion of (a) necessarily hold in the absence of the relatively prime hypothesis? Prove or give a counterexample.

Proof. (a) Since $F \subseteq F(\alpha) \subseteq F(\alpha, \beta)$, we see that $[K : F] = [K : F(\alpha)][F(\alpha) : F]$, i.e. $m \mid [K : F]$. Similarly, $n \mid [K : F]$. Since $\gcd(m, n) = 1$, then we have $mn \mid [K : F]$. Let $f(x) = \min(\beta, F)$ and $g(x) = \min(\beta, F(\alpha))$. Then, we see that $f \in F(\alpha)[x]$, so $g \mid f$. Thus, $\deg f \geqslant \deg g$. We see that $[K : F(\alpha)] = \deg g \leqslant \deg f = [F(\beta) : F]$. Thus, $[K : F] = [K : F(\alpha)][F(\alpha) : F] \leqslant [F(\beta) : F][F(\alpha) : F] = mn$. Thus, we see that $[K : F] = mn$.

(b) No. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt[4]{2})$, then $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. But, $K = \mathbb{Q}(\sqrt[4]{2})$ and so $[K : \mathbb{Q}] = 4$. Thus, $[K : F] \neq 2 \times 4 = 8$. □

Problem 206 (**20J·6**)**.** The goal of this problem is to prove that $\mathbb{C}$ is an algebraically closed field. (So, do NOT use this fact in your solution!)

(a) Let $K/\mathbb{R}$ be a finite extension. Prove that if $[K : \mathbb{R}]$ is odd, then $K = \mathbb{R}$.

(b) Let $L/\mathbb{R}$ be a finite Galois extension of $\mathbb{R}$. Prove that $[L : \mathbb{R}]$ is a power of 2. (Hint: Sylow's Theorem)

(c) Prove that there is no extension $K/\mathbb{C}$ with $[K : \mathbb{C}] = 2$.

(d) Let $K/\mathbb{C}$ be any finite extension. Show that there is some finite Galois extension $L/\mathbb{R}$ with $\mathbb{R} \subseteq \mathbb{C} \subseteq K \subseteq L$. Show that $L = \mathbb{C}$, and deduce that $K = \mathbb{C}$.

Proof. (a) Let $\alpha \in K$, then $[\mathbb{R}(\alpha) : \mathbb{R}]$ is odd. Let $f(x) = \min(\alpha, \mathbb{R})$, we have $\deg f = [\mathbb{R}(\alpha) : \mathbb{R}]$ is odd. Then, f must have a root, say a, in $\mathbb{R}$ by intermediate value theorem. Then $f(x) = (x-a)g(x)$ for some $a \in \mathbb{R}$ and $g(x) \in \mathbb{R}[x]$. Since f is irreducible, we see that $g(x)$ is a unit in $\mathbb{R}$. Thus, $[\mathbb{R}(\alpha) : \mathbb{R}] = \deg f = 1$, i.e. $\alpha \in \mathbb{R}$. So, we see that $K = \mathbb{R}$.

(b) Suppose $L \neq \mathbb{R}$, then $[L : \mathbb{R}]$ is even by (a). Suppose $[L : \mathbb{R}] = 2^k m$ with $\gcd(2, m) = 1$. Let $G = \mathrm{Gal}(L/\mathbb{R})$, we see that $|G| = 2^k m$. By first Sylow's theorem, G has a subgroup H of order 2^k. Let F be the fixed field of H. Then, by the fundamental theorem of Galois theory, we see that $[F : \mathbb{R}] = [G : H] = m$ is odd. By (a), we see that $F = \mathbb{R}$. So, $m = 1$. Hence, $[L : \mathbb{R}]$ is a power of 2.

(c) Suppose $K/\mathbb{C}$ is a field extension such that $[K : \mathbb{C}] = 2$. Let $\alpha \in K - \mathbb{C}$, then $[\mathbb{C}(\alpha) : \mathbb{C}] = 2$. Let $f(x) = \min(\alpha, \mathbb{C})$. Then, $\deg f = [\mathbb{C}(\alpha) : \mathbb{C}] = 2$. We may assume that $f(x) = x^2 + bx + c$ with $b, c \in \mathbb{C}$. So, $\alpha = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2} \in \mathbb{C}$, contradiction. So, there is no extension $K/\mathbb{C}$ with $[K : \mathbb{C}] = 2$.

(d). Let L be the normal closure of $K/\mathbb{R}$, then $L/\mathbb{R}$ is normal and separable by definition. Since $K/\mathbb{R}$ is finite, then $L/\mathbb{R}$ is also finite. Indeed, $K = \mathbb{R}(a_1, \cdots, a_n)$ for some $a_1, \cdots, a_n \in K$. Let $f_i(x) = \min(a_i, \mathbb{R})$, then L is the splitting field of $\{f_1, \cdots, f_n\}$, which is a finite extension over $\mathbb{R}$.

By (a), $[L : \mathbb{R}] = 2^n$ for some $n \geqslant 1$. Suppose $n \geqslant 2$. Then, $|\mathrm{Gal}(L/\mathbb{C})| = [L : \mathbb{C}] = 2^{n-1}$. By first Sylow's theorem, $\mathrm{Gal}(L/\mathbb{C})$ has a subgroup of order 2^{n-2}, say H. Let F be the fixed field of H such that $\mathbb{C} \subseteq F \subseteq L$. Then, $[F : \mathbb{C}] = [\mathrm{Gal}(L/\mathbb{C}) : H] = 2$. By ($c$) there is no extension of degree 2 over $\mathbb{C}$. This is a contradiction. Thus, we see that the only possibility is $n = 1$. Thus, $[L : \mathbb{R}] = 2$ and $L = \mathbb{C}$. It follows that $K = \mathbb{C}$. □

Problem 207 (**20J·7**)**.** Let F be a finite field, let f be a monic irreducible polynomial in $F[x]$, and let $\alpha \in \overline{F}$ be a root of f. Prove the following:

(a) $F(\alpha)$ is the splitting field for f over F, and

(b) the set of roots of f is $\{\alpha^{|F|^r} \mid r \geqslant 1\}$.

Proof. (a) Suppose K is a finite field with $\mathrm{char}(K) = p$ and $|K| = p^n$. Then, $K^\times$ is a cyclic group of order $p^n - 1$. Thus, for all $a \in K^\times$, we have $a^{p^n - 1} = 1$, i.e. $a^{p^n} = a$. Since $0^{p^n} = 0$, we see that each element of K is a root of $x^{p^n} - x$. Since $x^{p^n} - x$ has at most p^n roots in K, we see that K is exactly the set of roots of $x^{p^n} - x$.

Suppose $\mathrm{char}(F) = p$, $\deg f = d$ and $[F : \mathbb{F}_p] = n$. Then, $[F(\alpha) : F] = \deg f = d$. So, $[F(\alpha) : \mathbb{F}_p] = [F(\alpha) : F][F : \mathbb{F}_p] = dn$. Thus, $|F(\alpha)| = p^{dn}$. By the discussion above, we see that

$$F(\alpha) = \{a \in \overline{F} : a \text{ is a root of } x^{p^{dn}} - x\}.$$

In particular, α is a root of $x^{p^{dn}} - x$. Thus, $f \mid x^{p^{dn}} - x$. Thus, each root of f is an element of $F(\alpha)$. Thus, $F(\alpha)$ is the splitting field for f over F.

(b) Since $F(\alpha)/F$ is Galois, we have $|\mathrm{Gal}(F(\alpha)/F)| = [F(\alpha) : F] = d$. Define a homomorphism $\sigma : F(\alpha) \to F(\alpha)$ by $a \mapsto a^{p^n}$. If $a^{p^n} = 0$, then $a = 0$. Thus, σ is injective. So, Im $\sigma \cong F(\alpha)$ and $|\text{Im } \sigma| = |F(\alpha)|$. Thus, σ is surjective. So, we see that σ is an automorphism. For any $a \in F$, we have $a^{p^n} = a$ by (a). Thus, we see that $\sigma \in \mathrm{Gal}(F(\alpha)/F)$. Let $\mathcal{F}(\sigma) = \{a \in F(\alpha) : \sigma(a) = a^{p^n} = a\}$ be the fixed field of σ. Then, $\mathcal{F}(\sigma) \supseteq F$. Every element of $\mathcal{F}(\sigma)$ is a root of $x^{p^n} - x$, so it lies in F, i.e. $\mathcal{F}(\sigma) = F$. Thus, we see that $\langle\sigma\rangle = \mathrm{Gal}(F(\alpha)/F)$, i.e. a cyclic group of order d generated by σ.

Note that $\sigma^i(a) = a^{p^{ni}}$ for all $i = 1, 2, \cdots, d$. Then, for each $r = 1, 2, \cdots, d$, $\sigma^r(a)$ is a root of f. Thus, the set of roots of f is $\{\alpha^{p^{nr}} : r = 1, 2, \cdots, d\} = \{\alpha^{|F|^r} \mid r \geqslant 1\}$. □

Problem 208 (20A·7). Let $f(x) = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1 \in \mathbb{Q}[x]$ be irreducible, and let E be the splitting field of f contained in $\mathbb{C}$. The reciprocal polynomial of f is the polynomial $g(x) := x^6 f(1/x)$. Now we know that $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to a subgroup of S_6. If $f = g$, then prove that $\mathrm{Gal}(E/\mathbb{Q})$ is **not** isomorphic to all of S_6.

Proof. Clearly, 0 is not a root of f. From $f = g$, we see that $f(x) = x^6 f(\frac{1}{x})$. So, if $a \in E$ is a root of f, then $a^6 f(\frac{1}{a}) = f(a) = 0$, i.e. $\frac{1}{a} \in E$ is also a root of f. Suppose $a, b, c, \frac{1}{a}, \frac{1}{b}, \frac{1}{c}$ are the six roots of f, then $E = \mathbb{Q}(a, b, c)$. So, $[E : \mathbb{Q}] = [\mathbb{Q}(a, b, c) : \mathbb{Q}] \leqslant [\mathbb{Q}(a) : \mathbb{Q}][\mathbb{Q}(b) : \mathbb{Q}][\mathbb{Q}(c) : \mathbb{Q}] \leqslant 6^3 < 6! = |S_6|$. Thus, $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] < |S_6|$.

Thus, we see that $\mathrm{Gal}(E/\mathbb{Q})$ is not isomorphic to all of S_6. □

Problem 209 (20A·8). Consider the real number $\alpha = \sqrt{2 + \sqrt{2}}$.

(a) What is the irreducible polynomial f of α over $\mathbb{Q}$? (Be sure to prove that the polynomial you find is irreducible.)

(b) Determine the splitting field $E \subseteq \mathbb{C}$ of f over $\mathbb{Q}$. What is $[E : \mathbb{Q}]$?

(c) Determine the Galois group $G = \mathrm{Gal}(E/\mathbb{Q})$ and determine how each automorphism in G acts on the roots of f.

(d) For each subgroup $H \subseteq G$, what is the fixed field E^H?

Proof. (a) First, $\alpha^2 - 2 = \sqrt{2}$, so $(\alpha^2 - 2)^2 = 2$, i.e. $\alpha^4 - 4\alpha^2 + 2 = 0$. Let $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$. Take $p = 2$, then $p \mid 2, p \mid (-4), p \nmid 1$ and $p^2 \nmid 2$. So, by Eisenstein's criterion, we see that f is irreducible over $\mathbb{Q}$.

(b) The roots of f are $\pm\sqrt{2 + \sqrt{2}} = \pm\alpha, \pm\sqrt{2 - \sqrt{2}} = \pm\frac{\alpha^2 - 2}{\alpha}$. So, the splitting field of f is $E = \mathbb{Q}(\alpha)$.

$[E : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 4$.

(c) Let $\tau \in G$ given by $\alpha \mapsto \frac{\alpha^2 - 2}{\alpha}$. Then, by direct computation, $\tau^2(\alpha) = -\alpha$. Thus, τ is an element of order 4. So, $G = \langle\tau\rangle \cong \mathbb{Z}/4\mathbb{Z}$.

$\tau : \alpha \mapsto \frac{\alpha^2-2}{\alpha} \mapsto -\alpha \mapsto -\frac{\alpha^2-2}{\alpha} \mapsto \alpha$.

$\tau^2 : \alpha \mapsto -\alpha, \frac{\alpha^2-2}{\alpha} \mapsto -\frac{\alpha^2-2}{\alpha}$.

$\tau^3 : \alpha \mapsto -\frac{\alpha^2-2}{\alpha} \mapsto -\alpha \mapsto \frac{\alpha^2-2}{\alpha} \mapsto \alpha$.

(d) G has exactly one non-trivial proper subgroup $H = \langle\tau^2\rangle$. We see that τ^2 fixes $\alpha^2 - 2 = \sqrt{2}$. Then, $E^H \supseteq \mathbb{Q}(\sqrt{2})$. Since $[E^H : \mathbb{Q}] = [G : H] = 2$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Thus, $E^H = \mathbb{Q}(\sqrt{2})$.

For $H = \{1\}$, we see that $E^H = E$. For $H = G$, we have $E^H = \mathbb{Q}$. □

Problem 210 (21J·9). Consider the polynomial $f(x) = x^5 - 4x - 2$ over $\mathbb{Q}$ and its splitting field F.

(a) Prove that f is irreducible over $\mathbb{Q}$.

(b) Determine the number of real roots of f.

(c) Prove that the Galois group G of the extension F over $\mathbb{Q}$ is a subgroup of the symmetric group S_5.

(d) Prove that G contains a transposition.

(e) Prove that G contains a 5-cycle.

(f) Determine G.

(g) Is the equation $x^5 - 4x - 2 = 0$ solvable by radicals over $\mathbb{Q}$?

Proof. (a) Take $p = 2$, then $p \mid (-2)$, $p \mid (-4)$, $p \nmid 1$ and $p^2 \nmid (-2)$. Thus, f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion.

(b) First, $f'(x) = 5x^4 - 4 = (\sqrt{5}x^2 + 2)(\sqrt{5}x^2 - 2)$. Let $a = \sqrt{\frac{2}{\sqrt{5}}}$, then we see that $f'(x) > 0$ if $x \in (-\infty, -a) \cup (a, \infty)$ and $f'(x) < 0$ if $x \in (-a, a)$. Thus, f is strictly increasing over $(-\infty, -a)$, strictly decreasing over $(-a, a)$ and strictly increasing over (a, ∞). Since $f(a) = a^5 - 4a - 2 = a(a^4 - 4) - 2 = a(4/5 - 4) - 2 < 0$ and $f(-a) = -a^5 + 4a - 2 = a(4 - a^4) - 2 = \frac{16a}{5} - 2 > 0$, we see that f has exactly 1 real root in $(-a, a)$. Since $\lim\limits_{x \to \infty} f(x) = \infty$ and $\lim\limits_{x \to -\infty} f(x) = -\infty$, there exists exactly 1 root in $(-\infty, -a)$ and (a, ∞) respectively. Thus, f has exactly 3 real roots.

(c) By (b), we see that f has 5 distinct roots. Let $x_1, \cdots, x_5$ be the five roots of f. Take $\tau \in G$, then $\tau(x_i)$ is a root of f as $f(\tau(x_i)) = \tau(f(x_i)) = 0$. So, τ permutes the elements of the set $X := \{x_1, \cdots, x_5\}$. Define a map

$$\Psi : G \mapsto S_X$$

by

$$\tau \mapsto \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ \tau(x_1) & \tau(x_2) & \tau(x_3) & \tau(x_4) & \tau(x_5) \end{pmatrix}.$$

Since $F = \mathbb{Q}(X)$, and a $\mathbb{Q}$-automorphism τ is determined by the action on the generating set X, we see that Ψ is injective. Thus, $G \leqslant S_X \cong S_5$.

(d) We have known that f has exactly 3 real roots, say x_3, x_4, x_5, which means that f has exactly two non-real roots $x_1 = a + bi$ and $x_2 = a - bi$. Consider the complex conjugation $\mathbb{C} \to \mathbb{C}$ given by $z \mapsto \overline{z}$, we see that it permutes x_1, x_2 and fixes x_3, x_4, x_5. Thus, the complex conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$, hence an $\mathbb{R}$-automorphism of F, denoted by $(x_1 x_2)$. Then, we see that G has a transposition $(x_1 x_2)$.

(e) Let a be a root of f, then $[\mathbb{Q}(a) : \mathbb{Q}] = \deg f = 5$. By the fundamental theorem of Galois theory, $\mathbb{Q}(a)$ corresponds to a subgroup $H = \mathrm{Gal}(F/\mathbb{Q}(a))$ of G. We see that $[G : H] = [\mathbb{Q}(a) : \mathbb{Q}] = 5$. Thus, $5 \mid |G|$. So, by first Sylow's theorem, G contains an element of order 5, which is a 5-cycle.

(f) By (e), we see that G has a 5-cycle, say $\sigma = (x_1 t_2 t_3 t_4 t_5)$, where t_2, t_3, t_4, t_5 is a permutation of $\{x_2, x_3, x_4, x_5\}$. Since $\sigma^2 = (x_1 t_3 t_5 t_2 t_4)$, $\sigma^3 = (x_1 t_4 t_4 t_5 t_3)$ and $\sigma^4 = (x_1 t_5 t_4 t_3 t_2)$, we see that there exists $1 \leqslant k \leqslant 4$ such that $\sigma^k = (x_1 x_2 a_3 a_4 a_5)$, where a_3, a_4, a_5 is a permutation of x_3, x_4, x_5. Recall that (12345) and (12) generates S_5, we see that σ^k and $(x_1 x_2)$ generates S_X. Thus, $G = S_X \cong S_5$.

(g) Since $\{1\} \lhd A_5 \lhd S_5$ is a composition series, we see that the composition factors of S_5 are A_5 and $\mathbb{Z}_2$. Since A_5 is not abelian, we see that S_5 is not solvable. So $G \cong S_5$ is not solvable, then by Galois theory, the equation $x^5 - 4x - 2 = 0$ is not solvable by radicals over $\mathbb{Q}$. □