Contents

HOMEWORK C1 - SOLUTIONS

Problem 1. Prove that an artinian integral domain is a field.

Solution. Let A be an artinian integral domain and $x \in A$ be non-zero. The descending chain of ideals $(x) \supset (x^2) \supset \cdots$ terminates, so $(x^n) = (x^{n+1})$ for some n. Thus there exists $y \in A$ such that $x^{n+1}y = x^n$, so $x^n(1 - xy) = 0$. Since A is an integral domain and $x \neq 0$, we have $1 - xy = 0$, so x is invertible with inverse y. Hence A is a field. □

Problem 2. Let $f : M \to M$ be a surjective endomorphism of a noetherian module M over a commutative ring. Show that f is an isomorphism.

Solution. By the first isomorphism theorem, $M/\ker f \cong M$ with isomorphism induced by f, so by induction, $M/\ker(f^n) \cong M$. Since M is noetherian, $\ker f \subset \ker(f^2) \subset \cdots$ terminates, so $\ker(f^n) = \ker(f^{n+1})$ for some n. Then

$$\ker(f : M \to M) \cong \ker(f : M/\ker(f^n) \to M) = \ker(f^{n+1})/\ker(f^n) = 0,$$

so f is injective, hence an isomorphism. □

Problem 3. Let M be a noetherian module over a commutative ring R. Show that for every multiplicative subset $S \subset R$, the $S^{-1}R$-module $S^{-1}M$ is noetherian.

Solution. Let $N \subset S^{-1}M$ be an $S^{-1}R$-submodule of M and let $N' = \{m \in M \mid m/1 \in N\}$. Then $N' \subset M$ as an R-module, so N' is finitely generated by some $m_1, \ldots, m_n$. For any $m/s \in N$, we write $m = a_1m_1 + \cdots + a_nm_n$ with $a_i \in R$, and then $m/s = (a_1/s)m_1 + \cdots + (a_n/s)m_n$, so $m_1, \ldots, m_n$ generate N' as an $S^{-1}R$-module. Since every submodule of $S^{-1}M$ is finitely generated, $S^{-1}M$ is noetherian. □

Problem 4. Let F be an algebraically closed field and let $M \subset F[x_1, \ldots, x_n]$ be a maximal ideal. Prove that there exists $a_1, \ldots, a_n \in F$ such that $M = \{f \in F[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0\}$.

Solution. By Problem 5, $B = F[x_1, \ldots, x_n]/M$ is a finite field extension of F. Then $B = F$ since F is algebraically closed. Let $a_i = \overline{x}_i \in F$. Then $f(a_1, \ldots, a_n) = \overline{f(x_1, \ldots, x_n)} = 0$ for all $f \in M$, so $M \subset I = \{f \in F[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0\}$. Since $1 \notin I$, we have $M = I$. □

Problem 5. Let F be a field and let $M \subset F[x_1, \ldots, x_n]$ be a maximal ideal. Show that the quotient ring $F[x_1, \ldots, x_n]/M$ is a finite field extension of F.

Solution. We proceed by induction. The case $n = 1$ is clear.

Let $\overline{x}_i = x_i + M$, then let $A = F[\overline{x}_1]$ and $K = F(\overline{x}_1)$. Since $B = F[x_1, \ldots, x_n]/M = F[\overline{x}_1, \ldots, \overline{x}_n]$ is a field, $K \subset B$ and $B = K[\overline{x}_2, \ldots, \overline{x}_n]$. By the inductive hypothesis, B/K is a finite field extension. In particular, each $\overline{x}_i$ for $i \geq 2$ satisfies a monic polynomial equation with coefficients of the form f/g for $f, g \in A$. Choosing a polynomial for each one and letting h be the product of all denominators which appear, B is integral over $A_h = \{f/h^n \mid f \in A \text{ and } n \geq 0\}$.

Suppose $\overline{x}_1$ is transcendental over A. Then A is integrally closed, so A_h is integrally closed. However, its field of fractions is K, which is integral over A_h, so $A_h = K$. This is a contradiction, hence $\overline{x}_1$ is algebraic over A, so K/F is a finite field extension. By the tower law, so is B/F. □

Problem 6. Show that the ring of all 2×2 matrices $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ such that $a \in \mathbb{Z}$ and $b, c \in \mathbb{Q}$ is right noetherian but not left noetherian.

Solution. To see that this ring R is not left noetherian, we take the chain $I_1 \subsetneq I_2 \subsetneq \cdots$ with

$$I_n = \left\{ \begin{pmatrix} 0 & a/2^n \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Z} \right\}.$$

That each I_n is a left ideal follows from the computation

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}, \tag{$*$}$$

with $d = f = 0$ and $a \in \mathbb{Z}$.

To see that R is right noetherian, we find all of the right ideals of R. Let I be a right ideal, and first suppose that no matrix in I has a non-zero upper left entry. Referring to $(*)$ with $a = 0$, given $\begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \in I$, we have $\begin{pmatrix} 0 & bf \\ 0 & cf \end{pmatrix} \in I$ for all $f \in \mathbb{Q}$. If I contains two matrices whose second columns are linearly independent, then every rational vector is attained in the second column by taking linear combinations, so the possible right ideals in this case are

$$I_{0,0} = 0, \qquad I_{0,1;b,c} = \left\{ \begin{pmatrix} 0 & bf \\ 0 & cf \end{pmatrix} \mid f \in \mathbb{Q} \right\}, \qquad I_{0,2} = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \mid b, c \in \mathbb{Q} \right\}. \tag{I}$$

Now suppose I contains a matrix with non-zero upper left entry, and suppose $n > 0$ is the smallest such positive entry. Referring to $(*)$ with $a = n$, by choosing e appropriately, we can attain any rational number in the upper right entry of I, while in the upper left entry, we can attain any multiple of n by choosing d appropriately. It follows that every upper left entry of a matrix in I must be a multiple of n, as otherwise we can get a smaller positive entry in the upper left by dividing and extracting the remainder. If I contains a matrix with a non-zero lower right entry, then we can attain any rational number in the lower right entry by choosing f appropriately. Therefore, the possible right ideals in this case are

$$I_{n,0} = \left\{ \begin{pmatrix} nd & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{Q} \text{ and } d \in \mathbb{Z} \right\}, \qquad I_{n,1} = \left\{ \begin{pmatrix} nd & b \\ 0 & c \end{pmatrix} \mid b, c \in \mathbb{Q} \text{ and } d \in \mathbb{Z} \right\}. \tag{II}$$

Maximal strictly ascending chains of right ideals of type (I) are of the form $I_{0,0} \subsetneq I_{0,1;b,c} \subsetneq I_{0,2}$. For type (II), $I_{n,i} \subset I_{m,j}$ if and only if $m \mid n$ and $i \leq j$, so we cannot have an infinite strictly ascending chain of right ideals of type (II). Therefore, R has no infinite strictly ascending chains of right ideals, as every right ideal of R is of type (I) or (II), so R is right noetherian. $\square$

Problem 7. Show that the ring of all 2×2 matrices $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ such that $a \in \mathbb{Q}$ and $b, c \in \mathbb{R}$ is right artinian but not left artinian.

Solution. To see that this ring R is not left artinian, we take the chain $I_1 \supsetneq I_2 \supsetneq \cdots$ with

$$I_n = \left\{ \begin{pmatrix} 0 & 2^{1/2^n} a \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Q} \right\}.$$

That each I_n is a left ideal follows from $(*)$ [Problem 6].
To see that R is right artinian, we find all of the right ideals of R. Let I be a right ideal, and first suppose that no matrix in I has a non-zero upper left entry. By the same argument as in the corresponding case for Problem 6, the ideals of this form are

$$I_{0,0} = 0, \qquad I_{0,1;b,c} = \left\{ \begin{pmatrix} 0 & bf \\ 0 & cf \end{pmatrix} \mid f \in \mathbb{R} \right\}, \qquad I_{0,2} = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \mid b, c \in \mathbb{R} \right\}. \tag{I}$$

If I contains a matrix with non-zero upper left entry, then by choosing d and e appropriately in $(*)$, we can attain any rational number in the upper left entry and any real number in the upper right entry. Therefore, the two possible right ideals in this case are

$$I_{1,0} = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Q} \text{ and } b \in \mathbb{R} \right\}, \qquad I_{1,1} = R. \tag{II}$$

Maximal strictly descending chains of right ideals of type I are of the form $I_{0,2} \supsetneq I_{0,1;b,c} \supsetneq I_{0,0}$, while there are only two right ideals of type II, so R has no infinite strictly descending chains of right ideals, i.e. R is right artinian. □

Problem 8. Let I be an ideal of a commutative ring R. The *radical* of I is

$$\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n\}.$$

Prove that $\sqrt{I}$ is an ideal in R.

Solution. It is clear that $0 \in \sqrt{I}$. If $x, y \in \sqrt{I}$ with $x^n, y^m \in I$, then $(x+y)^{n+m} \in I$, since each term is of the form $ax^k y^{n+m-k}$ with either $k \geq n$ or $n+m-k \leq m$. Hence $x+y \in \sqrt{I}$. Finally, if $x \in \sqrt{I}$ with $x^n \in I$, and $a \in R$, then $(ax)^n = a^n x^n \in I$, so $ax \in \sqrt{I}$. □

Problem 9. Let F be an algebraically closed field and $I \subset F[x_1, \ldots, x_n]$ be an ideal. Denote by $S(I)$ the subset in F^n consisting of all n-tuples $(a_1, \ldots, a_n) \in F^n$ such that $f(a_1, \ldots, a_n) = 0$ for all $f \in I$. A subset $S \subset F^n$ is called *closed* if $S = S(I)$ for some ideal $I \subset F[x_1, \ldots, x_n]$. Prove that the union of two closed subsets and the intersection of any family of closed subsets are closed.

Solution. Let S_1, S_2 be closed with $S_1 = S(I_1)$ and $S_2 = S(I_2)$. We claim that $S_1 \cup S_2 = S(I_1 I_2)$. If $fg \in I_1 I_2$ with $f \in I_1$ and $g \in I_2$, and $a \in S_1 \cup S_2$, then $f(a) = 0$ if $a \in S_1$ and $g(a) = 0$ if $a \in S_2$, so $(fg)(a) = 0$. Hence $S_1 \cup S_2 \subset S(I_1 I_2)$, as $I_1 I_2$ is generated by these products. Conversely, if $a \in S(I_1 I_2)$, then $(fg)(a) = 0$ for all $f \in I_1$ and $g \in I_2$. Suppose $a \notin S_1$, so there exists $f \in I_1$ such that $f(a) \neq 0$. Then $g(a) = 0$ for all $g \in I_2$, so $a \in S_2$.

Let $\{S_i\}$ be closed with $S_i = S(I_i)$. We claim that $\bigcap_i S_i = S(I)$, where I is the ideal generated by $\bigcup_i I_i$. If $a \in \bigcap_i S_i$, then for each i, we have $f(a) = 0$ for all $f \in I_i$. Hence $f(a) = 0$ for all $f \in \bigcup_i I_i$, so $\bigcap_i S_i \subset S(I)$. Conversely, if $a \in S(I)$, then for each i, we have $f(a) = 0$ for all $f \in I_i$, so $a \in S_i$. Hence $a \in \bigcap_i S_i$. □

Problem 10. For any closed subset $S \subset F^n$, denote by $I(S)$ the set of all $f \in F[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in S$. Show that $I(S)$ is an ideal in $F[x_1, \ldots, x_n]$ such that $I(S) = \sqrt{I(S)}$ (i.e. $I(S)$ is a *radical ideal*).

Solution. It is clear that $0 \in I(S)$, and if $f, g \in I(S)$ and $h \in F[x_1, \ldots, x_n]$, then for all $a \in S$, we have $(f + g)(a) = f(a) + g(a) = 0$ and $(hf)(a) = h(a)f(a) = 0$, so $I(S)$ is an ideal.

If $f^m \in I(S)$ for some $f \in F[x_1, \ldots, x_n]$ and $m \geq 1$, then $f(a)^m = 0$ for all $a \in S$. Hence $f(a) = 0$ for all $a \in S$, so $f \in I(S)$. □

HOMEWORK C2 - SOLUTIONS

Problem 1. Prove that every ideal in a Dedekind domain can be generated by two elements.

Solution. Let A be a Dedekind domain and $\mathfrak{a} \subset A$ be non-zero. Pick $a \in \mathfrak{a}$ non-zero, then factor

$$(a) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}, \qquad \mathfrak{a} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n}.$$

Since $(a) \subset \mathfrak{a}$, we have $e_i \geq f_i$ for each i. By the Chinese remainder theorem,

$$\mathfrak{a}/(a) \cong \prod_{i=1}^{n} \mathfrak{p}_i^{f_i}/\mathfrak{p}_i^{e_i}.$$

Let $b_i \in \mathfrak{p}_i \backslash \mathfrak{p}_i^2$. Then $\mathfrak{p}_i^{e_i} \subset b_i^{f_i} A + \mathfrak{p}_i^{e_i} \subset \mathfrak{p}_i^{f_i}$, but $b_i^{f_i} \notin \mathfrak{p}_i^{f_i+1}$, so in fact $b_i^{f_i} A + \mathfrak{p}_i^{e_i} = \mathfrak{p}_i^{f_i}$. Hence $b_i^{f_i}$ generates $\mathfrak{p}_i^{f_i}/\mathfrak{p}_i^{e_i}$. The Cartesian product of principal ideals is principal in the product ring, so $\mathfrak{a}/(a)$ is principal, generated by some b. Pulling back to the original ring, a and b generate $\mathfrak{a}$. □

Problem 2. Is $\mathbb{Z}[\sqrt{5}]$ a Dedekind domain?

Solution. The quotient field of $\mathbb{Z}[\sqrt{5}]$ is $\mathbb{Q}(\sqrt{5})$, which contains $(1+\sqrt{5})/2$. This is a root of $x^2 - x - 1 \in (\mathbb{Z}[\sqrt{5}])[x]$ which does not lie in $\mathbb{Z}[\sqrt{5}]$, so $\mathbb{Z}[\sqrt{5}]$ is not integrally closed in its quotient field, hence not a Dedekind domain. □

Problem 3. Prove that a noetherian integral domain R is a Dedekind domain if and only if each localization $R_\mathfrak{p}$ at a non-zero prime ideal $\mathfrak{p}$ is a DVR.

Solution. If R is a field, then the result is clear. Henceforth, suppose that R is not a field.

($\Longrightarrow$) Let $\mathfrak{p}$ be a non-zero prime ideal. Every non-zero ideal in R factors as $\mathfrak{p}^v \mathfrak{a}$ for some ideal $\mathfrak{a}$ not divisible by $\mathfrak{p}$. In the localization at $\mathfrak{p}$, the ideal $\mathfrak{a}$ becomes the unit ideal, so the ideals in $R_\mathfrak{p}$ are precisely those of the form $\mathfrak{p}^v$. (Every ideal of the localization comes from extension of an ideal in the original ring.) In particular, $R_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p}$, and $\mathfrak{p} = (\pi)$ for any $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$. Hence $R_\mathfrak{p}$ is a local PID, so it is a DVR. (The corresponding discrete valuation on its field of fractions is the $\mathfrak{p}$-adic valuation.)

($\Longleftarrow$) It suffices to show that R is integrally closed and that $\dim R \leq 1$.

Let F be the quotient field of R and suppose $\alpha \in F$ is integral over R. For any non-zero prime ideal $\mathfrak{p}$, the localization $R_\mathfrak{p}$ is a DVR, and in particular is integrally closed. Thus $\alpha \in R_\mathfrak{p}$ for every non-zero prime ideal $\mathfrak{p} \subset R$, so $\alpha \in R$. (The denominator of α is not in any prime ideal, hence a unit in R.)

Let $\mathfrak{p}$ be a non-zero prime ideal of R and let $\mathfrak{m} \supset \mathfrak{p}$ be a maximal ideal. Then $\mathfrak{p}R_\mathfrak{m}$ is a prime ideal in the DVR $R_\mathfrak{m}$, so $\mathfrak{p}R_\mathfrak{m} = \mathfrak{m}R_\mathfrak{m}$. Hence

$$\mathfrak{p} = R \cap \mathfrak{p}R_\mathfrak{m} = R \cap \mathfrak{m}R_\mathfrak{m} = \mathfrak{m},$$

so every non-zero prime ideal is maximal.

□

Problem 4. Show that $R = \mathbb{Q}[x,y]/(x^2+y^2-1)$ is a Dedekind domain. Is R a PID?

Solution. Let $A = \mathbb{Q}[x]$ and $K = \mathbb{Q}(x)$ be its field of fractions. To see that R is a Dedekind domain, it suffices to show that R is the integral closure of A in $L = K[y]/(y^2+x^2-1)$, which is a finite extension of K with basis $(1, y)$.

Let $\alpha = f + g \cdot y \in L$ be integral over A and let $m_\alpha = t^2 - 2f \cdot t + (f^2 - g^2 \cdot (x^2-1)) \in K[t]$ be its minimal polynomial over K. Since A is a UFD, Gauss's lemma implies that $m_\alpha \in A[t]$, so $2f \in A$ and $f^2 - g^2 \cdot (x^2-1) \in A$. From $2f \in A$, we get $f \in A$. Then $g^2 \cdot (x^2-1) \in A$, but $x^2 - 1 \in A$ is square-free, so in fact $g \in A$.

The elements $1 \pm x$ and y are irreducible in R (by considering field norm), but $(1+x)(1-x) = y^2$, so R is not a UFD, hence not a PID. □

Problem 5. Prove that for every two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a Dedekind domain, $\mathfrak{ab} = (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})$.

Solution. By unique factorization of ideals in a Dedekind domain, we can write

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_n^{k_n} \qquad \text{and} \qquad \mathfrak{b} = \mathfrak{p}_1^{l_1} \cdots \mathfrak{p}_n^{l_n},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct prime ideals and $k_1, \ldots, k_n, l_1, \ldots, l_n \geq 0$. We claim that

$$\mathfrak{a}+\mathfrak{b} = \mathfrak{p}_1^{\min(k_1,l_1)} \cdots \mathfrak{p}_n^{\min(k_n,l_n)} \qquad \text{and} \qquad \mathfrak{a}\cap\mathfrak{b} = \mathfrak{p}_1^{\max(k_1,l_1)} \cdots \mathfrak{p}_n^{\max(k_n,l_n)}.$$

For the first, let $\mathfrak{c}$ be the product on the right hand side. We can then factor the left hand side as $\mathfrak{a}+\mathfrak{b} = (\mathfrak{a}'+\mathfrak{b}')\mathfrak{c}$, where $\mathfrak{a}'$ and $\mathfrak{b}'$ have no prime ideal factors in common by construction. If $\mathfrak{a}'+\mathfrak{b}' = R$, then we are done. Otherwise, $\mathfrak{a}, \mathfrak{b} \subset \mathfrak{a}'+\mathfrak{b}' \subset \mathfrak{p}$ for some prime ideal $\mathfrak{p}$, but then $\mathfrak{p}$ divides both $\mathfrak{a}'$ and $\mathfrak{b}'$, a contradiction. Thus we have proved the first identity.

For the second, by inspection, the product $\mathfrak{d}$ on the right hand side lies in $\mathfrak{a}\cap\mathfrak{b}$. Conversely, if we factor $\mathfrak{a}\cap\mathfrak{b}$ as a product of primes, then the exponent of $\mathfrak{p}_i$ must be at least k_i and l_i to have inclusion into $\mathfrak{a}$ and $\mathfrak{b}$, so $\mathfrak{a}\cap\mathfrak{b}$ lies in $\mathfrak{d}$ as well.

From these formulæ, the result follows from $k_i + l_i = \min(k_i, l_i) + \max(k_i, l_i)$. □

Problem 6. Prove that the ring of rational functions $f/g \in F(x)$ with $\deg f \leq \deg g$ is a DVR.

Solution. Define $\nu : F(x)^\times \to \mathbb{Z}$ by $\nu(f/g) = \deg g - \deg f$. This is well-defined, and we claim that ν is a discrete valuation on $F(x)$. That ν is a group homomorphism is clear, so it remains to check that $\nu(f_1/g_1 + f_2/g_2) \geq \min(\nu(f_1/g_1), \nu(f_2/g_2))$. For this,

$$\begin{aligned}\nu\left(\frac{f_1}{g_1}+\frac{f_2}{g_2}\right) = \nu\left(\frac{f_1g_2+f_2g_1}{g_1g_2}\right) &= \deg g_1 + \deg g_2 - \deg(f_1g_2+f_2g_1)\\ &\geq \deg g_1 + \deg g_2 - \max(\deg f_1 + \deg g_2, \deg f_2 + \deg g_1)\\ &= \min(\deg g_1 - \deg f_1, \deg g_2 - \deg f_2).\end{aligned}$$

The corresponding discrete valuation ring is the ring of rational functions f/g with $\nu(f/g) \geq 0$, i.e. the rational functions with $\deg f \leq \deg g$. □

Problem 7. Let $d \neq 0, 1$ be an integer. Suppose that d is not divisible by the square of a prime integer. Let $R = \mathbb{Z}[(1+\sqrt{d})/2]$ if $d \equiv 1 \pmod 4$ and $R = \mathbb{Z}[\sqrt{d}]$ otherwise. Prove that R is a Dedekind domain.

Solution. It suffices to show that R is the integral closure of $\mathbb{Z}$ in $K = \mathbb{Q}(\sqrt{d})$ in either case.

Let $\alpha = a + b\sqrt{d} \in K$ be integral over $\mathbb{Z}$. Since $\mathbb{Z}$ is a UFD, it follows from Gauss's lemma that the minimal polynomial of α is in $\mathbb{Z}[x]$. Therefore, $\operatorname{tr}(\alpha) = 2a$ and $N(\alpha) = a^2 - db^2$ are integers, so $a = a'/2$ for some $a' \in \mathbb{Z}$. Then $(a')^2/4 - db^2$ is an integer, so if a' is even, then $b \in \mathbb{Z}$, while if a' is odd, then $b = b'/2$ for some odd integer b'. Moreover, $(a')^2 \equiv (b')^2 \equiv 1 \pmod 4$, so we must have $d \equiv 1 \pmod 4$ to get an integer norm.

When $d \equiv 1 \pmod 4$, the element $(1+\sqrt{d})/2$ is a root of $x^2 - x - (d-1)/4$, so is integral. Therefore, R is an integral extension of $\mathbb{Z}$, and it contains all elements of K which could possibly be integral over $\mathbb{Z}$. Hence R is the integral closure of $\mathbb{Z}$ in K.

When $d \not\equiv 1 \pmod 4$, the elements $a + b\sqrt{d}$ with a, b both half-integers cannot be integral either, so the only integral elements are in $\mathbb{Z}[\sqrt{d}]$. Since $\sqrt{d}$ is integral over $\mathbb{Z}$, we have again that R is an integral extension of $\mathbb{Z}$ which contains all elements of K which are integral over R, so R is the integral closure of $\mathbb{Z}$ in K. □

Problem 8. Let p be a prime integer. Prove that if $p \equiv 3 \pmod 4$, then pR is a prime ideal in the ring of Gaussian integers $R = \mathbb{Z}[i]$. Prove that if $p \equiv 1 \pmod 4$, then pR is a product of two distinct prime ideals of R. Find a prime ideal $\mathfrak{P}$ in R such that $2R = \mathfrak{P}^2$.

Solution. We use the fact that the Gaussian integers are a Euclidean domain with the square complex magnitude as a multiplicative Euclidean function. Therefore, factorization of pR into prime ideals is equivalent to factorization of p into irreducibles in R. If $p = ab$, then $p^2 = N(p) = N()N(b)$, so if a and b are not units, then $N(a) = N(b) = p$. Therefore, p factors into at most two irreducibles, and if p factors into two irreducibles, then they both have norm p.

If $p \equiv 3 \pmod 4$ and $a = u + iv$, then $u^2 + v^2 = p$, but modulo 4, we can only have $u^2 + v^2 \equiv 0, 1, 2 \pmod 4$, so this is a contradiction. Therefore, p is irreducible in R, so pR is prime.

If $p \equiv 1 \pmod 4$, then there exists t such that $t^2 \equiv -1 \pmod p$, so then $p \mid t^2 + 1 = (t+i)(t-i)$. However, p does not divide $t \pm i$, as $t/p \pm i/p \notin R$, so p is not prime in R. If $u + iv$ is an irreducible divisor of p, then the other divisor is $u - iv$, as it has the same norm p and their product is a positive real number. This gives us a factorization $pR = (u+iv)R \cdot (u-iv)R$, with $(u \pm iv)R$ prime. To see that they are not the same ideal, we have $(u+iv)/(u-iv) = (u^2 - v^2)/p + (2uv)i/p$. Since $p \neq 2$ and $p \nmid u, v$, this is not in R, so $u + iv$ and $u - iv$ are not associates in R. Thus they generate distinct prime ideals.

In the case $p = 2$, we can explicitly find $2R = (1+i)R \cdot (1-i)R$, with $1 \pm i$ irreducible in R. Since $(1-i)i = 1 + i$, these two ideals are the same, so $2R = ((1+i)R)^2$. □

Problem 9. Let $R = \mathbb{Z}[\sqrt{-5}]$. Factor $14R$ into a product of prime ideals.

Solution. The factorization is

$$14R = (2R)(7R) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5}).$$

To check that these indeed multiply correctly,

$$(2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = (4, 6, 2 \pm 2\sqrt{-5}) = (2, 2 \pm 2\sqrt{-5}) = 2R,$$
$$(7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5}) = (49, 14, 21 \pm 7\sqrt{-5}) = (7, 21 \pm 7\sqrt{-5}) = 7R.$$

To check that these are prime, we have

$$R/(2, 1 \pm \sqrt{-5}) \cong \mathbb{Z}[x]/(x^2 + 5, 2, x \pm 1) \cong \mathbb{F}_2[x]/(x^2 + 1, x + 1) \cong \mathbb{F}_2[x]/(x + 1) \cong \mathbb{F}_2,$$
$$R/(7, 3 \pm \sqrt{-5}) \cong \mathbb{Z}[x]/(x^2 + 5, 7, x \pm 3) \cong \mathbb{F}_7[x]/(x^2 + 5, x \pm 3) \cong \mathbb{F}_7[x]/(x \pm 3) \cong \mathbb{F}_7.$$

□

Problem 10. Let R be a Dedekind ring and $S \subset R$ be a multiplicative subset. Prove that the localization $S^{-1}R$ is also a Dedeking domain.

Solution. **$S^{-1}R$ is noetherian.** Let $\mathfrak{a}_1 \cdot S^{-1}R \subset \mathfrak{a}_2 \cdot S^{-1}R \subset \cdots$ be an ascending chain of ideals in $S^{-1}R$. Since R is noetherian, the corresponding chain $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ stabilizes in R, so the original chain in $S^{-1}R$ also stabilizes.

$S^{-1}R$ has Krull dimension 1. If $\mathfrak{p} \cdot S^{-1}R$ is non-zero prime, where $\mathfrak{p} \cap S = \emptyset$, then since $\mathfrak{p} \subset R$ is maximal, $S^{-1}R/\mathfrak{p} \cdot S^{-1}R \cong R/\mathfrak{p}R$ is a field, so $\mathfrak{p} \cdot S^{-1}R$ is maximal in $S^{-1}R$.

$S^{-1}R$ is integrally closed in its quotient field. Let F be the quotient field of R and $S^{-1}R$. Suppose $\alpha \in F$ is integral over $S^{-1}R$, so $\alpha^n + (a_{n-1}/s_{n-1})\alpha^{n-1} + \cdots + a_0/s_0 = 0$ for some $a_i \in R$ and $s_i \in S$. Let $s = s_0 \cdots s_{n-1}$. Clearing denominators, $(s\alpha)^n + \cdots + a_0 s^n/s_0 = 0$, and the coefficients are in R. Therefore, $s\alpha \in R$ since R is integrally closed in F, so $\alpha \in S^{-1}R$.

□

HOMEWORK C3 - SOLUTIONS

Problem 1. Prove that a Dedekind domain with finitely many maximal ideals is a PID.

Solution. Let R be a Dedekind domain with non-zero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. It suffices to show that each $\mathfrak{p}_i$ is principal; we do the proof for $\mathfrak{p}_1$. Since $\mathfrak{p}_1 \not\subset \mathfrak{p}_i$ for $i \geq 2$ and $\mathfrak{p}_1 \not\subset \mathfrak{p}_1^2$, by the prime avoidance lemma, there exists $a \in \mathfrak{p}_1$ which is not in $\mathfrak{p}_1^2$ or any $\mathfrak{p}_i$ for $i \geq 2$. Then $aR \subset \mathfrak{p}_1$, so $aR = \mathfrak{p}_1\mathfrak{a}$ for some ideal $\mathfrak{a}$. However, by the choice of a, no $\mathfrak{p}_i$ divides $\mathfrak{a}$, so $\mathfrak{a} = R$ and $\mathfrak{p}_1 = aR$. □

Problem 2. Let $R = F[x, y]/(y^2 - x^3)$, where F is a field. Determine the integral closure of R in its quotient field.

Solution. The quotient field of R is $K = F(x)[y]/(y^2 - x^3)$, as it must contain $F(x)$ and y, and $y^2 - x^3$ is irreducible in $F(x)[y]$, so $F(x)[y]/(y^2 - x^3)$ is a finite field extension of $F(x)$. Note that R is integral over its subring $A = F[x]$, so it suffices to determine the integral closure of A in K.

Let $\varphi = f + g \cdot y \in K$ be integral over A. Since A is a Dedekind domain, $\mathrm{tr}(\varphi) = 2f \in A$ and $N(\varphi) = f^2 - g^2 \cdot y^2 = f^2 - g^2 \cdot x^3 \in A$. From the first, $f \in A$, and from the second, $g^2 \cdot x^3 \in A$, so $g = h/x$ for some $h \in A$. Hence the integral closure of R in K is $\{f + h \cdot y/x \mid f, g \in A\}$. □

Problem 3. Let R be a normal domain with $2 \in R^\times$, let F be the quotient field of R, and let $L = F(\sqrt{d})$ be a quadratic field extension of F.

(a) Prove that an element $u + v\sqrt{d}$ with $u, v \in F$ is integral over R if and only if $u, dv^2 \in R$.

(b) Suppose that R is a Dedekind domain and the ideal dR is not divisible by the square of a prime ideal. Prove that the ring $R[\sqrt{d}]$ is a Dedekind domain.

Solution. (a) Let $\alpha = u + v\sqrt{d}$ be integral over R. Then $\mathrm{tr}\,\alpha = 2u \in F$ and $N(\alpha) = u^2 - dv^2 \in F$ are integral over R, so $2u \in R$ and $u^2 - dv^2 \in R$ since R is normal. Since $2 \in R^\times$, this means that $u \in R$, so $dv^2 \in R$.

(b) It suffices to show that $R[\sqrt{d}]$ is the integral closure of R in L. From part (a), $u \in R$ and $dv^2 \in R$, so we must show that $v \in R$. If $v = 0$, then we are done. Otherwise, factor $dR = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_n^{k_n}$ and $vR = \mathfrak{p}_1^{l_1} \cdots \mathfrak{p}_n^{l_n}$, where $k_1, \dots, k_n \in \{0, 1\}$ since $dR \subset R$ is not divisible by the square of a prime, and $l_1, \dots, l_n \in \mathbb{Z}$. Then $dv^2R = \mathfrak{p}_1^{k_1+2l_1} \cdots \mathfrak{p}_n^{k_n+2l_n}$ satisfies $k_i + 2l_i \geq 0$ for all i since $dv^2 \in R$. Since $k_i \leq 1$, this means $l_i \geq 0$ for all i, so $vR \subset R$, i.e. $v \in R$.

□

Problem 4. Let F be a field of characteristic not 2 and let $a, b \in F^\times$. Prove that the quotient ring $F[x, y]/(ax^2 + by^2 - 1)$ is a Dedekind domain.

Solution. By rescaling, it suffices to show that $R = F[x, y]/(y^2 + ax^2 - b)$ is a Dedekind domain (with $a, b \in F\times$ not necessarily the same as in the problem statement). Since $\mathrm{char}\, F \neq 2$, it follows that $ax^2 - b$ is not divisible by a non-trivial square, so by Eisenstein, $y^2 + ax^2 - b$ is irreducible. Hence the field of fractions of R is $K = F(x)[y]/(y^2 + ax^2 - b)$, which is a finite field extension of the quotient field $F(x)$ of the Dedekind domain $A = F[x]$. To show that R is a Dedekind domain, it suffices to show that R is the integral closure of A in K.

Letting $\varphi = f + g \cdot y \in K$ be integral over A, we have as in the argument for Problem 2 that $f \in A$ and $g^2 \cdot (b - ax^2) \in A$. Since $b - ax^2$ is square-free, $g \in A$, so $\varphi \in R$. □

Problem 5. Let M be a module over a Dedekind domain R such that $aM = 0$ for some non-zero $a \in R$. Let S be the set of all elements in R that do not belong to any prime ideal that contains a. Prove that S is a multiplicative subset of R and the localization $S^{-1}R$ is a PID. Show that M has a natural structure of an $S^{-1}R$-module. Deduce the structure theorems on finitely generated torsion modules over R.

Solution. It follows from definition that S is the set of all elements s for which sR is coprime to aR. If $s, t \in S$, then

$$aR + stR = (aR + sR)(aR + tR) = RR = R,$$

so $st \in S$. Since $1 \in S$ as well, S is a multiplicative subset of R. Factoring $aR = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, the prime ideals of $S^{-1}R$ are just $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, so by Problem 1, $S^{-1}R$ is a PID.

To show that M has the structure of an $S^{-1}R$-module, we claim that for any $s \in S$, the map $m \mapsto sm$ is an isomorphism. Since sR and aR are coprime, there exist $t, b \in R$ such that $st + ab = 1$, so if $sm = 0$, then $m = (st + ab)m = 0$. This shows that the map is injective, and for surjectivity, we have $m = (st + ab)m = s(tm)$ for any $m \in M$. Therefore, we can define the action of s^{-1} on M as the inverse of the action of s on M. This gives M the structure of an $S^{-1}R$-module.

Since $S^{-1}R$ is a PID,

$$M \cong \prod_{i=1}^{r} S^{-1}R/\mathfrak{q}_i^{f_i} \cdot S^{-1}R, \qquad \mathfrak{q}_i \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$$

as $S^{-1}R$-modules. The canonical map $R \to S^{-1}R$ is injective since R is a domain, so pulling back along the canonical map, we also have isomorphism as R-modules. Moreover, from our earlier characterization of S, it follows that $S^{-1}R/\mathfrak{q}_i^{f_i} \cdot S^{-1}R \cong R/\mathfrak{q}_i^{f_i}$. Hence we have the elementary divisor form for finitely generated torsion modules over R, and the invariant factor form follows from the Chinese remainder theorem. □

Problem 6. Let R be a Dedekind domain and $a \in R$ be non-zero. Prove that R/aR is artinian.

Solution. Factor $aR = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$. Ideals of R/aR correspond to ideals of R containing a, which must factor as $\mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n}$ with $f_i \leq e_i$ for each i. There are only finitely many such ideals, so there are finitely many ideals in R/aR. In particular, R/aR is artinian. □

Problem 7. Let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero ideals of a Dedekind ring R. Prove that the R-modules $\mathfrak{a}/\mathfrak{ab}$ and $R/\mathfrak{b}$ are isomorphic.

Solution. By the prime avoidance lemma for Dedekind domains, we can find $\mathfrak{a}'$ such that $\mathfrak{a}' \cong \mathfrak{a}$ and $\mathfrak{a}' + \mathfrak{b} = R$. Then by the second isomorphism theorem,

$$\mathfrak{a}/\mathfrak{ab} \cong \mathfrak{a}'/\mathfrak{a}'\mathfrak{b} = \mathfrak{a}'/(\mathfrak{a}' \cap \mathfrak{b}) \cong (\mathfrak{a}' + \mathfrak{b})/\mathfrak{b} = R/\mathfrak{b}.$$

□

Problem 8. Let R be a ring of algebraic integers and $p \in \mathbb{Z}$ be a prime number. Prove that the set A of all prime ideals $\mathfrak{p} \subset R$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ is finite and non-empty. Show that $pR = \prod \mathfrak{p}^{e_\mathfrak{p}}$ for some positive integers $e_\mathfrak{p}$, where the product is taken over all $\mathfrak{p} \in A$.

Solution. Since R is a Dedekind domain and $pR \neq 0$, we can factor $pR = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ with $e_i \geq 1$. If $\mathfrak{p} \subset R$ is a prime ideal with $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then $pR \subset \mathfrak{p}$, so $\mathfrak{p} = \mathfrak{p}_i$ for some i. Hence $A = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ is finite and non-empty, and

$$pR = \prod_{\mathfrak{p} \in A} \mathfrak{p}^{e_\mathfrak{p}}$$

with $e_\mathfrak{p} = e_i$ if $\mathfrak{p} = \mathfrak{p}_i$. □

Problem 9. In the conditions of the previous problem, let n be the degree of the quotient field of R over $\mathbb{Q}$. Show that for every $\mathfrak{p} \in A$, the quotient ring $R/\mathfrak{p}$ is a finite field of $p^{f_\mathfrak{p}}$ elements for some integer $f_\mathfrak{p}$. Prove that $n = \sum e_\mathfrak{p} f_\mathfrak{p}$, where the sum is taken over all $\mathfrak{p} \in A$.

Solution. Let K be the quotient field of R, so that $R = \mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, and let $F = \mathbb{Z}/p\mathbb{Z}$. Then R is freely generated of rank n over $\mathbb{Z}$, so R/pR is freely generated of rank n over F, i.e. $R/pR \cong F^n$ as F-vector spaces. By the Chinese remainder theorem and Problem 7,

$$n = \dim_F(R/pR) = \sum_{\mathfrak{p} \in A} \dim_F(R/\mathfrak{p}^{e_\mathfrak{p}}) = \sum_{\mathfrak{p} \in A} \sum_{j=1}^{e_\mathfrak{p}} \dim_F(\mathfrak{p}^{j-1}/\mathfrak{p}^j) = \sum_{\mathfrak{p} \in A} e_\mathfrak{p} \dim_F(R/\mathfrak{p}).$$

Since the sum is finite, each $\dim_F(R/\mathfrak{p})$ is a finite quantity $f_\mathfrak{p}$, so $R/\mathfrak{p}$ is a finite field with $p^{f_\mathfrak{p}}$ elements. With this notation, $n = \sum e_\mathfrak{p} f_\mathfrak{p}$. □

Problem 10. Let $\alpha = (1 + \sqrt{-23})/2$ and let I be the ideal in $\mathbb{Z}[\alpha]$ generated by 2 and α. Prove that I^3 is a principal ideal.

Solution. Observe that if $\overline{I}$ is generated by 2 and $\overline{\alpha} = (1 - \sqrt{-23})/2$, then $I\overline{I} = 2R$, where $R = \mathbb{Z}[\alpha]$. If $K = \mathbb{Q}(\sqrt{-23})$ and $\beta = (3 + \sqrt{-23})/2 \in R$, then $N_{K/\mathbb{Q}}(\beta) = 8 = 2^3$. Since $2 \nmid \beta$ in R, either $\beta R = I^3$ or $\beta R = \overline{I}^3$. In either case, $[I^3] = 1$ in the class group of R, since $[\overline{I}] = [I]^{-1}$. □

HOMEWORK C4 - SOLUTIONS

Problem 1. Let M, M', N be finitely generated modules over a Dedekind ring R with the property that $M \oplus N \cong M' \oplus N$. Prove that $M \cong M'$.

Solution. From the classification of finitely generated torsion modules over R, and in particular the uniqueness statements, it is immediate that $M_{\text{tors}} \cong M'_{\text{tors}}$. For the torsion-free parts, we have $\operatorname{rank}(M \oplus N) = \operatorname{rank}(M' \oplus N)$, so $\operatorname{rank} M = \operatorname{rank} M'$ since rank is additive. We also have $\det(M \oplus N) = \det(M' \oplus N)$, so $\det M = \det M'$ since determinant is multiplicative and gives elements in the class group of R. Since M and M' have the same rank and determinant, their torsion-free parts are isomorphic, again by uniqueness in the classification. □

Problem 2. Let M be a non-zero torsion-free module over a Dedekind ring R and $\mathfrak{a} \subset R$ an ideal. Show that there is an injective R-module homomorphism $\mathfrak{a} \to M$.

Solution. Write $M \cong R^{n-1} \oplus \mathfrak{b}$ for $n \geq 1$ the rank of M and $\mathfrak{b} \subset R$ an ideal. If $n \geq 2$, then we take the inclusion of $\mathfrak{a}$ into one of the copies of R. Otherwise, since $M \neq 0$, we have $\mathfrak{b} \cong M \neq 0$. Left multiplication by any non-zero $\alpha \in \mathfrak{b}\mathfrak{a}^{-1} \subset F$ is an injective R-module homomorphism $\mathfrak{a} \to \mathfrak{b}$. □

Problem 3. Let $\mathfrak{a}$ be a non-zero ideal of a Dedekind ring R. Prove that $\mathfrak{a} \oplus \mathfrak{a}^{-1} \cong R^2$. Deduce that $\mathfrak{a}$ is generated by at most two elements.

Solution. From a result we showed in class,

$$\mathfrak{a} \oplus \mathfrak{a}^{-1} \cong R \oplus \mathfrak{a}\mathfrak{a}^{-1} = R \oplus R.$$

Hence $\mathfrak{a} \cong R^2/\mathfrak{a}^{-1}$ is generated by at most two elements as an R-module. □

Problem 4. Let $\mathfrak{a}$ be a non-zero ideal of a Dedekind ring R. Prove that $\mathfrak{a}^{-1} \cong \operatorname{Hom}_R(\mathfrak{a}, R)$.

Solution. We showed in class that $\operatorname{Hom}_R(\mathfrak{a}, \mathfrak{b}) \cong \mathfrak{b}\mathfrak{a}^{-1}$; take $\mathfrak{b} = R$. □

Problem 5. Let $M_1, \ldots, M_n$ be (left) R-modules and $M = M_1 \oplus \cdots \oplus M_n$. Prove that the ring $\operatorname{End}_R(M)$ is isomorphic to the ring of $n \times n$ matrices (f_{ij}) with $f_{ij} \in \operatorname{Hom}_R(M_j, M_i)$.

Solution. By Homework B4 Problem 5, we have $\operatorname{End}_R(M) \cong (\operatorname{Hom}_R(M_j, M_i))_{ij}$ as R-modules, so in particular as abelian groups. To check isomorphism of rings, we must show that composition corresponds to matrix multiplication. Using Einstein summation convention, if f, g are represented by $F = (f_{ij})$ and $G = (g_{ij})$, we have $(f \circ g)(m_k) = f(g_{jk} m_k) = f_{ij} g_{jk} m_k = (FG)_{ik} m_k$. □

Problem 6. Show that every (left) R-module is free if and only if R is a division ring.

Solution. If R is not a division ring, then let $a \in R$ be non-zero with no left inverse. The left ideal Ra is not all of R, so $R/Ra \neq 0$. This is not a free left R-module, since a annihilates it.

If R is a division ring, then let M be a left R-module and consider a minimal generating set $\{m_i\}$. Suppose $a_1 m_1 + \cdots + a_n m_n = 0$ is a non-trivial linear dependence of shortest length, so that $a_k \neq 0$ for $1 \leq k \leq n$. Then $m_1 = -a_1^{-1}(a_2 m_2 + \cdots + a_n m_n)$, contradicting minimality of the generating set $\{m_i\}$ since we could remove m_1. Hence M is freely generated by $\{m_i\}$, i.e. M is free. □

Problem 7. Let R be a ring, $S = M_n(R)$, and view R^n as a left S-module. Prove that every S-module endomorphism f of R^n is $f(v) = va$ for some $a \in R$. Deduce that $\mathrm{End}_S(R^n) \cong R^{\mathrm{op}}$.

Solution. An S-module endomorphism f of R^n is of the form $f(v) = (v^t A)^t$, with $A \in S$, such that $f(Bv) = Bf(v)$ for all $B \in S$ and $v \in R^n$. This requires that $B(v^t A)^t = ((Bv)^t A)^t$ for all $B \in S$ and $v \in R^n$. By taking suitable combinations of unit vectors v and unit matrices B, we see that this can only be attained for $A = aI$ for some $a \in R$. This gives us $f(v) = (v^t(aI))^t = va$. If $f(v) = va$ and $g(v) = vb$, then $(f \circ g)(v) = vba$, which gives us $\mathrm{End}_S(R^n) \cong R^{\mathrm{op}}$. □

Problem 8. Let V be a finite-dimensional left D-module over a division ring D. Prove that the ring $\mathrm{End}_D(V)$ is simple and semisimple.

Solution. Since V is finite-dimensional, we have $\mathrm{End}_D(V) \cong M_n(D)$ for $n = \dim V$. This is semisimple, and to see that it is simple, let I be a non-zero two-sided ideal of $\mathrm{End}_D(V)$. Let $A \in I$ be non-zero, so then it has a non-zero entry a. Multiplying on the left and right by unit matrices and elementary matrices, it follows that all unit matrices are in I, so then $I = \mathrm{End}_D(V)$. □

Problem 9. Let V be a finite-dimensional left D-module over a division ring D and $W \subset V$ be a submodule. Prove that

$$\mathrm{Hom}_D(V, W) \cong \{f \in \mathrm{End}(V) \mid f(V) \subset W\}$$

is a right ideal in $\mathrm{End}_D(V)$. Prove that every right ideal in $\mathrm{End}_D(V)$ is equal to $\mathrm{Hom}_D(V, W)$ for a unique submodule $W \subset V$.

Solution. Clearly $\mathrm{Hom}_D(V, W)$ is an additive subgroup of $\mathrm{End}_D(V)$. For any $f \in \mathrm{Hom}_D(V, W)$ and $g \in \mathrm{End}_D(V)$, we have $(f \circ g)(V) \subset f(V) \subset W$, so $f \circ g \in \mathrm{Hom}_D(V, W)$.

Let $I \subset \mathrm{End}_D(V)$ be a right ideal and $W = \sum_{f \in I} f(V) \subset V$. Then $I \subset \mathrm{Hom}_D(V, W)$, and we claim that this is equality. Let $v_1, \ldots, v_n$ be a basis for V. It suffices to show for any $w \in W$ that there exists $f \in I$ such that $f(v_1) = w$ and $f(v_i) = 0$ for $2 \leq i \leq n$. For $w \in W$, there exist $u_1, \ldots, u_k \in V$ and $f_1, \ldots, f_k \in I$ such that $\sum f_j(u_j) = w$. We can find $g_j \in \mathrm{End}_D(V)$ such that $g_j(u_j) = e_1$ by transitivity of the action on V by matrices, and then $\tilde{f} = \sum_j f_j \circ g_j \in I$ satisfies $\tilde{f}(v_1) = w$. Letting $g \in \mathrm{End}_D(V)$ be given by $g(v_1) = v_1$ and $g(v_i) = 0$ for $2 \leq i \leq n$, the map $f = \tilde{f} \circ g \in I$ has the required properties. □

Problem 10. Let D be a division ring. Prove that the center of D is a subfield of D.

Solution. It is always the case that $Z(D)$ is a commutative subring of D. If $ab = ba$, then left and right multiplying by a^{-1}, we have $ba^{-1} = a^{-1}b$, so if $a \in Z(D)$, then $a^{-1} \in Z(D)$. □

HOMEWORK C5 - SOLUTIONS

Problem 1. Find a non-zero abelian group A such that $A \oplus A \cong A$. Let $R = \operatorname{End} A$. Prove that the (left) R-modules R and R^2 are isomorphic. Show that $R^n \cong R^m$ for all $n, m > 0$.

Solution. This was Homework B4 Problems 1 and 2. □

Problem 2. Let R be a ring that admits a homomorphism to a division ring. Prove that the (left) R-modules R^n and R^m are isomorphic only if $n = m$.

Solution. We use the characterization that a ring R has this property if and only if for any matrices $A \in M_{m\times n}(R)$ and $B \in M_{n\times m}(R)$, the equalities $AB = I_m$ and $BA = I_n$ together imply $m = n$.

Let $f : R \to D$ be a homomorphism. By the same argument as for finite-dimensional vector spaces over a field, $D^n \cong D^m$ if and only if $n = m$, so the characterization holds for D. Now suppose $A \in M_{m\times n}(R)$ and $B \in M_{n\times m}(R)$ with $AB = I_m$ and $BA = I_n$. Applying f component-wise to A and B, we get $f(A)f(B) = I_m$ and $f(B)f(A) = I_n$ as matrices over D, so $m = n$. □

Problem 3. Let R be a ring with the property that all (left) cyclic R-modules are projective. Prove that R is semisimple.

Solution. In particular, every simple R-module is projective. Let I be the sum of all minimal left ideals of R, and suppose $M \subset R$ is a maximal left ideal containing R. Then R/M is simple, hence projective, so the short exact sequence $0 \to M \to R \to R/M \to 0$ is split. This gives us an injective map $R/M \to R$ whose image is a minimal left ideal of R which is not contained in M, a contradiction. Hence no maximal left ideal contains I, so $I = R$, i.e. R is semisimple. □

Problem 4. Let R be a ring such that any two simple (left) R-modules are isomorphic. Prove that R has no non-trivial central idempotents.

Solution. We show the contrapositive. Let $e \in R$ be a non-trivial central idempotent element. Then $1 - e \in R$ is also a non-trivial central idempotent, and in particular, e and $1 - e$ are non-invertible. If M_1 and M_2 are maximal left ideals containing e and $1 - e$, respectively, then $M_1 \neq M_2$. To see that the simple R-modules R/M_1 and R/M_2 are non-isomorphic, it suffices to show that their annihilators are unequal. For $a + M_1 \in R/M_1$, we have $e(a + M_1) = ae + M_1 = M_1$ since e is central, so $e \in \operatorname{ann}(R/M_1)$. Similarly, $1 - e \in \operatorname{ann}(R/M_2)$, so these two annihilators cannot be equal, as else they would contain $1 = e + (1 - e)$. □

Problem 5. Determine all irreducible representations of the dihedral group of order $2n$ over $\mathbb{C}$.

Solution. Write $D_n = \langle r, s \mid r^n, s^2, srsr\rangle$ and let $\rho : D_n \to \mathbb{C}^\times$ be a one-dimensional representation. Then $\rho(r)^n = \rho(s)^2 = \rho(s)^2\rho(r)^2 = 1$. This gives us $\rho(s) = \pm 1$ and $\rho(r)^n = \rho(r)^2 = 1$. If n is odd, then $\rho(r) = 1$, while if n is even, we have $\rho(r) = \pm 1$.

The two-dimensional representations defined by $\rho(r) = \operatorname{rot}(2\pi k/n)$ and $\rho(s) = \operatorname{diag}(1, -1)$ for $1 \leq k < n/2$ are irreducible, since $\rho(r)$ and $\rho(s)$ do not commute, hence are not simultaneously diagonalizable. Moreover, they are not isomorphic, since isomorphism preserves eigenvalues.

If n is even, then we have 4 one-dimensional representations and $n/2-1$ two-dimensional irreducible representations. The sum of squares of dimensions is $4 \cdot 1^2 + (n/2 - 1) \cdot 2^2 = 2n$, so we have found all of the irreducibles. A similar check shows that we are also done when n is odd. □

Problem 6. Find the dimensions of all irreducible representations of A_5 over $\mathbb{C}$.

Solution. The group A_5 has five conjugacy classes, represented by 1, (12), (12)(34), (12345), (12354). Therefore, there are five irreducible representations, one of which is trivial, and hence has dimension 1. If d_2, d_3, d_4, d_5 are the dimensions of the other irreducibles, then $d_2^2+d_3^2+d_4^2+d_5^2 = 59$. The only solution in integers (up to rearrangements) is $(d_2, d_3, d_4, d_5) = (3, 3, 4, 5)$. □

Problem 7. Determine all irreducible representations of $\mathbb{Z}/n\mathbb{Z}$ over $\mathbb{Q}$.

Solution. In this case, the regular representation is given by circulant matrices, which for the generating element has characteristic polynomial $x^n - 1$. The decomposition $x^n - 1 = \prod_{d|n} \Phi_d$, where $\Phi_d \in \mathbb{Q}[x]$ is the d-th cyclotomic polynomial, shows that the irreducible representations can be given by setting $\rho([1]_n)$ to the companion matrix of Φ_d for some $d \mid n$. The dimensions of these representations are $\varphi(d)$. Conversely, $\rho([1]_n)^n$ must be an identity matrix, which forces $\rho([1]_n)$ to be similar to a direct sum of companion matrices of Φ_d's. □

Problem 8. Determine all irreducible representations of the symmetric group S_3 over $\mathbb{Q}$.

Solution. There are three irreducible representations of S_3 over $\mathbb{C}$, and all of them can be realized over $\mathbb{Q}$. In particular, the trivial and sign representations already take rational values, and the two-dimensional irreducible representation can be given by

$$\rho((123) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad \rho((1,2)) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Any other representation over $\mathbb{Q}$ is also a representation over $\mathbb{C}$, hence isomorphic as a complex representation to a direct sum involving irreducibles. Two rational matrices are similar over $\mathbb{C}$ if and only if they are similar over $\mathbb{Q}$, so we also have isomorphism as rational representations. Therefore, we have found all of the irreducibles. □

Problem 9. A representation $G \to GL_n(F)$ over a field F is called *absolutely irreducible* if the composition $G \to GL_n(F) \to GL_n(\overline{F})$ is irreducible, where $\overline{F}$ is an algebraic closure of F. Prove that if $G \to GL_n(F)$ is absolutely irreducible, then for every field extension L/F, the composition $G \to GL_n(F) \to GL_n(L)$ is irreducible.

Solution. By sending elements transcendental over F to 0, we get a homomorphism $L \to \overline{F}$. Then $G \to GL_n(F) \to GL_n(L) \to GL_n(\overline{F})$ is irreducible, so $G \to GL_n(F) \to GL_n(L)$ is irreducible. □

Problem 10. Let G be a finite group, $H \leq G$ be a subgroup, and V be an H-space. Consider the vector space W of all maps $f : G \to V$ satisfying $f(gh) = hf(g)$ for all $h \in H$ and $g \in G$. Show that the G-action on W given by $(gf)(g') = f(g'g)$ for all $g, g' \in G$ and $f \in W$ makes W a G-space.

Solution. This is an action, since

$$1f(g') = f(g'1) = f(g'), \qquad ((gg')f)(g'') = f(g''gg') = (g'f)(g''g) = (g'(gf))(g'').$$

Each g acts linearly, since

$$(g(f+f'))(g') = (f+f')(g'g) = (gf)(g') + (gf')(g'), \qquad (g(af))(g') = (af)(g'g) = a(gf)(g').$$

□

HOMEWORK C6 - SOLUTIONS

Problem 1. Let G be a finite group and Z be the center of G. Let $\mu : Z \to F^\times$ be a character of Z. Prove that there is an irreducible representation $\rho : G \to GL(V)$ such that $\rho(g)(v) = \mu(g)v$ for all $g \in Z$ and $v \in V$.

Solution. It suffices, since any finite-dimensional G-space is artinian, to show that there is some representation with $\rho(g)(v) = \mu(g)v$, as we can then take a minimal non-trivial G-invariant subspace to obtain an irreducible representation with the same property.

Let $g_1, \dots, g_n$ be representatives for the cosets of Z in G, and consider the induced representation on the vector space V freely generated by $g_1, \dots, g_n$, i.e. for $g \in G$,

$$\rho(g)\left(\sum_{i=1}^n a_i g_i\right) = \sum_{i=1}^n a_i \mu(z_i) g_{j(i)},$$

where $j(i)$ and $z_i \in Z$ are such that $gg_i = g_{j(i)}z_i$. For $z \in Z$, we have $zg_i = g_i z$, so

$$\rho(z)\left(\sum_{i=1}^n a_i g_i\right) = \sum_{i=1}^n a_i \mu(z) g_i = \mu(z)\sum_{i=1}^n a_i g_i.$$

Thus we have the desired representation. □

Problem 2. Let F be a field of characteristic $p > 0$ and G be a finite p-group. Prove that

$$\operatorname{rad}(F[G]) = \left\{ \sum_{g \in G} a_g g \in F[G] \mid \sum_{g \in G} a_g = 0 \right\}.$$

Determine all simple (left) $F[G]$-modules.

Solution. Observe that the augmentation map $\varepsilon : F[G] \to F$ is a ring homomorphism. Therefore, if $\varepsilon(\alpha) = a \neq 0$ for some $\alpha \in F[G]$ and $a \in F$, then $\varepsilon(1 - a^{-1}\alpha) = 0$, so $1 - a^{-1}\alpha$ cannot be left invertible. This shows that $\operatorname{rad}(F[G]) \subset \ker \varepsilon$. To see the other inclusion, it suffices (because the kernel of any ring homomorphism is a two-sided ideal) to show that any $\alpha \in \ker \varepsilon$ has $1 - \alpha$ invertible. For this, if $|G| = p^n$, then

$$\alpha^{p^n} = \left(\sum_{g \in G} a_g g\right)^{p^n} = \sum_{g \in G} a_g^{p^n} g^{p^n} = \sum_{g \in G} a_g^{p^n} = \left(\sum_{g \in G} a_g\right)^{p^n} = 0,$$

so $(1 - \alpha)^{-1} = 1 + \alpha + \cdots + \alpha^{p^n - 1} \in F[G]$, as required.

If M is a simple left $F[G]$-module, then M is finitely generated, and since $\operatorname{rad}(F[G])$ is an ideal, $\operatorname{rad}(F[G])M \subset M$ as a submodule, so $\operatorname{rad}(F[G])M = 0$ or $\operatorname{rad}(F[G])M = M$. In the latter case, by Nakayama's lemma (for non-commutative rings), $M = 0$, so M is not simple. Thus $\operatorname{rad}(F[G])M = 0$, so M is also a simple module over $F[G]/\operatorname{rad}(F[G]) \cong F$. Therefore, $M \cong F$ as an F-vector space, and so the only simple (left) $F[G]$-modules are the one-dimensional ones, whose characterization is well-known. □

Problem 3. Let V be the kernel of $F^n \to F$ taking $(a_1, \ldots, a_n)$ to $\sum_i a_i$. The symmetric group S_n acts on V by permutations of the coordinates. Prove that if the characteristic of F does not divide n, then the corresponding representation is irreducible.

Solution. Let W be a non-trivial S_n-invariant subspace of V and let $(a_1, \ldots, a_n) \in W$ be non-zero. Since $\operatorname{char} F \nmid n$, not all of the a_i are equal, as otherwise we would have $\sum_i a_i = na_1 = 0$, which would give $a_i = 0$ for all i. Therefore, there are some two indices $i \neq j$ with $a_i \neq a_j$. Since W is invariant under permutation of coordinates, we can move these indices to the first and second coordinates, so that $a_1 \neq a_2$. Then

$$(a_1, a_2, a_3, \ldots, a_n) - (a_2, a_1, a_3, \ldots, a_n) = (a_1 - a_2, a_2 - a_1, 0, \ldots, 0) \in W,$$

so $(1, -1, 0, \ldots, 0) \in W$. Further transpositions give that $e_1 - e_i \in W$ for all $i \geq 2$ (where e_i denotes the standard i-th basis vector). These span all of V, so the only non-trivial S_n-invariant subspace of V is V itself. In other words, the corresponding representation of S_n is irreducible. □

Problem 4. Let ρ be a representation of a finite group G and let V be the corresponding G-space. Show that the dual space V^* has the structure of a G-space via $(g\varphi)(v) = \varphi(g^{-1}v)$. Prove that $\chi_{\rho^*}(g) = \chi_\rho(g^{-1})$, where ρ^* is the representation corresponding to the G-space V^*.

Solution. We have that $(1\varphi)(v) = \varphi(1^{-1}v) = \varphi(v)$ and

$$((gh)\varphi)(v) = \varphi((gh)^{-1}v) = \varphi(h^{-1}g^{-1}v) = \varphi(h^{-1}(g^{-1}v)) = (h\varphi)(g^{-1}v) = (g(h\varphi))(v),$$

so we have an action on V^*. Moreover,

$$(g(\alpha\varphi + \beta\psi))(v) = (\alpha\varphi + \beta\psi)(g^{-1}v) = \alpha\varphi(g^{-1}v) + \beta\psi(g^{-1}v) = (\alpha(g\varphi) + \beta(g\varphi))(v),$$

so the action is linear, i.e. V^* is a G-space.

Let $v_1, \ldots, v_n$ be a basis for V and let $\theta_1, \ldots, \theta_n$ be the corresponding dual basis. Then we have $(g\theta_i)_j = (g\theta_i)(v_j) = \theta_i(g^{-1}v_j) = (g^{-1})_{ji}$, so

$$\chi_{\rho^*}(g) = \sum_{i=1}^{n} (g\theta_i)_i = \sum_{i=1}^{n} (g^{-1})_{ii} = \chi_\rho(g^{-1}).$$

□

Problem 5. Show that ρ^* is irreducible if and only if ρ is irreducible.

Solution. Let U be a non-trivial proper G-invariant subspace of V, let $v_1, \ldots, v_k$ be a basis for U, and extend it to a basis $v_1, \ldots, v_n$ of V. Let $\theta_1, \ldots, \theta_n$ be the corresponding dual basis, and let W be the span of $\theta_{k+1}, \ldots, \theta_n$.

For $i > k$ and $j \leq k$, we have $(g\theta_i)_j = \theta_i(g^{-1}v_j) = 0$ since $g^{-1}v_j$ is in the span of $v_1, \ldots, v_k$ by G-invariance of U. Therefore, $g\theta_i$ is in the span of $\theta_{k+1}, \ldots, \theta_n$ whenever $i > k$, so W is G-invariant. By hypothesis, $1 \leq k < n$, so $1 \leq n - k < n$, which shows that W is a non-proper G-invariant subspace of V^*. This shows that if ρ is not irreducible, then ρ^* is not irreducible. The canonical isomorphism of V and V^{**} for finite-dimensional vector spaces gives an isomorphism of ρ and ρ^{**}, so the same argument shows that if ρ^* is not irreducible, then $\rho \cong \rho^{**}$ is not irreducible. □

From now on, suppose that F is an algebraically closed field of characteristic zero.

Problem 6. Let G be a finite group. The abelian group $\operatorname{Rep} G$ is generated by the isomorphism classes $[\rho]$ of representations ρ of G, subject to the relations $[\rho \oplus \rho'] = [\rho] + [\rho']$ for all representations ρ and ρ'. Prove that $\operatorname{Rep} G$ is a free abelian group with basis the set of isomorphism classes of irreducible representations of G. Prove that the tensor product yields the structure of a commutative ring on $\operatorname{Rep} G$.

Solution. Let $\rho_1, \dots, \rho_k$ be the irreducible representations of G. Every representation is isomorphic to a direct sum of irreducible representations, so $\operatorname{Rep} G$ is generated by the isomorphism classes of irreducible representations.

Suppose $\sum_i a_i[\rho_i] = 0$. Applying the map $\operatorname{Rep} G \to \operatorname{Ch} G$ from Problem 7, we have $\sum_i a_i \chi_i = 0$. The characters form a basis for $\operatorname{Ch} G$, so $a_i = 0$ for all i. Thus $\operatorname{Rep} G$ is freely generated by the irreducible representations.

Define a multiplication on $\operatorname{Rep} G$ by extending $[\rho_i][\rho_j] = [\rho_i \otimes \rho_j]$ linearly. If 1 denotes the trivial representation, then $[\rho][1] = [\rho \otimes 1] = [\rho]$, and similarly $[1][\rho] = [\rho]$. Commutativity follows from the commutativity of the tensor product. Finally,

$$[\rho]([\rho_1' + \rho_2']) = [\rho][\rho_1' \oplus \rho_2'] = [\rho \otimes (\rho_1' \oplus \rho_2')] = [\rho \otimes \rho_1'] + [\rho \otimes \rho_2'] = [\rho][\rho_1'] + [\rho][\rho_2'].$$

Therefore, the multiplication gives a commutative ring structure. □

Problem 7. Let G be a finite group. Prove that the map $\operatorname{Rep} G \to \operatorname{Ch} G$ taking the class $[\rho]$ to the character χ_ρ is a well-defined injective ring homomorphism. Write down the multiplication table for $\operatorname{Rep} S_3$.

Solution. Isomorphic representations have the same characters, so the map is well-defined.

Moreover, the character of a direct sum is the sum of the characters, so the map extends linearly.

Finally, the character of a tensor product is the product of the characters, so the map gives a ring homomorphism. The argument from Problem 6 shows that the map is injective.

Letting ρ_1, ρ_2, ρ_3 denote representatives of the irreducible representations of S_3, we can find the character table of S_3, and hence obtain the multiplication table for $\operatorname{Rep} S_3$ from the fact that the character map is an injective ring homomorphism.

	id	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

	$[\rho_1]$	$[\rho_2]$	$[\rho_3]$
$[\rho_1]$	$[\rho_1]$	$[\rho_2]$	$[\rho_3]$
$[\rho_2]$	$[\rho_2]$	$[\rho_1]$	$[\rho_3]$
$[\rho_3]$	$[\rho_3]$	$[\rho_3]$	$[\rho_1] + [\rho_2] + [\rho_3]$

□

Problem 8. Find all groups that have exactly two non-isomorphic representations.

Solution. Any group has infinitely many non-isomorphic representations by acting on F^n trivially. Henceforth, we find (finite) groups with exactly two non-isomorphic irreducible representations.

Let d be the dimension of the non-trivial irreducible representation. Then $d \mid |G| = 1 + d^2$, so $d = 1$ and $|G| = 2$. Hence $G = \mathbb{Z}/2$ (which has the required property). □

Problem 9. Find an irreducible two-dimensional representation of S_4.

Solution. We use the presentation

$$S_4 = \langle a, b, c \mid a^2, b^3, c^4, abc \rangle.$$

Given this, the irreducible two-dimensional representation is (in matrix form)[1]

$$a \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad b \mapsto \begin{pmatrix} -1/2 & 1 \\ -3/4 & -1/2 \end{pmatrix}, \qquad c \mapsto \begin{pmatrix} -1/2 & 1 \\ 3/4 & 1/2 \end{pmatrix}.$$

These satisfy the given relations, so it is a representation. For irreducibility, an invariant subspace would have to be the span of $(1, 0)$ or the span of $(0, 1)$, but neither are eigenvectors for $\rho(c)$. □

Problem 10. Let $C(g)$ be the conjugacy class of an element g in a finite group G and let χ be the character of an irreducible representation ρ. Prove that if $|C(g)|$ is relatively prime to $\dim \rho$ and $\chi(g) \neq 0$, then $\rho(g)$ is multiplication by a scalar.

Solution. Let $d = \dim \rho$. Then $\chi(g)$ and $|C(g)|\chi(g)/d$ are algebraic integers, so $\chi(g)/d$ is an algebraic integer since $|C(g)|$ is relatively prime to d. If $|G| = n$, then since the algebraic integers in the n-th cyclotomic extension are $\mathbb{Z}[\zeta_n]$ by a well-known theorem, we have $\chi(g) = d \sum_k a_k \zeta_n^k$ for some integers a_k. As $\chi(g)$ is a sum of d roots of unity, this requires $a_k = 1$ for some k and $a_l = 0$ for all other l. Therefore, $\chi(g) = d\zeta_n^k$ for some k and $|\chi(g)| = d$, so $\rho(g)$ is a scalar matrix. □

[1] This can be found by lifting the standard representation of $S_4/V_4 \cong S_3$, or by brute force.

HOMEWORK C7 - SOLUTIONS

Throughout, the base field F is algebraically closed of characteristic zero and G is a finite group.

Problem 1. Let χ be an irreducible character of a group G of order n. Prove that $\sum_g \chi(g)^2$ is either equal to 0 or n.

Solution. Suppose ρ is the corresponding irreducible representation for χ. Then ρ^* is irreducible with $\chi_{\rho^*}(g) = \chi(g^{-1})$, so

$$\frac{1}{n}\sum_{g\in G}\chi(g)^2 = \frac{1}{n}\sum_{g\in G}\chi(g)\chi_{\rho^*}(g^{-1}) = \langle \chi, \chi_{\rho^*}\rangle \in \{0,1\}.$$

Therefore, $\sum_g \chi(g)^2 \in \{0, n\}$. □

Problem 2. Let $\rho : G \to GL(V)$ and $\mu : G \to GL(W)$ be two representations. Prove that

$$\dim \mathrm{Hom}_G(V,W) = \langle \chi_\rho, \chi_\mu\rangle.$$

Solution. Consider the representation $\rho^* \otimes \mu$ on $V^* \otimes W$, which is given by

$$(\rho^*\otimes\mu)(g)(f\otimes w) = (v \mapsto f(g^{-1}v))\otimes gw.$$

The isomorphism $V^*\otimes W \to \mathrm{Hom}(V,W)$ given by $\theta\otimes w \mapsto (v\mapsto \theta(v)w)$ induces the representation $(gf)(v) = gf^{-1}(g^{-1}v)$ on $\mathrm{Hom}(V,W)$. For $f \in \mathrm{Hom}_G(V,W) \subset \mathrm{Hom}(V,W)$, we have $gf = f$ for all g, and if $gf = f$ for all g, then $f \in \mathrm{Hom}_G(V,W)$, so $\dim \mathrm{Hom}_G(V,W) = \langle \chi_{\rho^*\otimes\mu}, 1\rangle$. We compute

$$\langle \chi_{\rho^*\otimes\mu}, 1\rangle = \frac{1}{|G|}\sum_{g\in G}\chi_{\rho^*}(g)\chi_\mu(g) = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g^{-1})\chi_\mu(g) = \langle \chi_\mu, \chi_\rho\rangle = \langle \chi_\rho, \chi_\mu\rangle.$$

□

Problem 3. Let V be a simple G-space. Show that there is at most one (up to a scalar multiple) G-invariant non-degenerate bilinear form on V.

Solution. There is an isomorphism $\mathrm{Hom}(V,V^*) \to \mathrm{Bil}(V,V;F)$ given by $f \mapsto ((v,w)\mapsto f(v)(w))$. For the bilinear map to be G-invariant, we require that $f(v)(w) = f(gv)(gw)$ for all $v,w\in V$ and $g\in G$. Replacing w with $g^{-1}w$, we have $f(gv)(w) = f(v)(g^{-1}w)$, so $f(gv) = g(f(v))$, so G-invariant bilinear maps are induced by G-homomorphisms $V \to V^*$. Since V is simple, V^* is simple, so by Schur's lemma, $\dim \mathrm{Hom}_G(V,V^*) \le 1$. □

Problem 4. For an arbitrary G-space V and a 1-dimensional G-space L, show that $V\otimes L$ is simple if and only if V is simple.

Solution. Since L is one-dimensional, $\chi_L : G \to F^\times$ is a group homomorphism, so

$$\langle \chi_{V\otimes L}, \chi_{V\otimes L}\rangle = \langle \chi_V\chi_L, \chi_V\chi_L\rangle = \frac{1}{|G|}\sum_{g\in G}\chi_V(g)\cancel{\chi_L(g)}\chi_V(g^{-1})\cancel{\chi_L(g^{-1})} = \langle \chi_V, \chi_V\rangle.$$

In particular, V is simple if and only if $V\otimes L$ is simple, in which case both sides are 1. □

Problem 5. Prove that the rings $F[G \times H]$ and $F[G] \otimes_F F[H]$ are isomorphic.

Solution. The set function $(g, h) \mapsto g \otimes h$ from the standard basis of $F[G \times H]$ to the standard basis of $F[G] \otimes_F F[H]$ gives an isomorphism of vector spaces over F. Moreover,

$$(g, h)(g', h') = (gg', hh') \mapsto gg' \otimes hh' = (g \otimes g')(h \otimes h'),$$

so the isomorphism is in fact a ring isomorphism. □

Problem 6. Let ρ be a representation on V. Show that ρ yields a representation μ on S^2V, where $S^2V = (V \otimes V)/\langle v \otimes w - w \otimes v\rangle$ is the *symmetric square* of V. Prove that

$$\chi_\mu(g) = \frac{1}{2}(\chi_\rho(g)^2 + \chi_\rho(g^2)).$$

Solution. Since

$$g(\langle v \otimes w - w \otimes v\rangle) = \langle gv \otimes gw - gw \otimes gv\rangle \subset \langle v \otimes w - w \otimes v\rangle,$$

the quotient S^2V has a well-defined G-space structure inherited from $V \otimes V$.

For $g \in G$, let $v_1, \ldots, v_n$ be a basis of eigenvectors of g, and let $gv_i = \lambda_i v_i$. Then $v_i \otimes v_j + v_i \otimes v_j$ with $1 \le i \le j \le n$ is a basis for S^2V, with eigenvalues $\lambda_i\lambda_j$, so

$$\chi_\mu(g) = \sum_{i \le j} \lambda_i\lambda_j = \frac{1}{2}(\chi_\rho(g)^2 + \chi_\rho(g^2)),$$

where we note that $\chi_\rho(g^2) = \sum_i \lambda_i^2$. □

Problem 7. Let $\rho : S_n \to GL_n$ be the natural representation of the symmetric group S_n by permutations of the coordinates. Determine $\langle \chi_\rho, \chi_\rho \rangle$.

Solution. From Homework C6 Problem 3, together with S_n acting trivially on $(1, \ldots, 1)$, it follows that $\chi_\rho = 1 + \chi$ for some irreducible character $\chi \neq 1$ if $n \ge 2$. Therefore, $\langle \chi_\rho, \chi_\rho \rangle = 2$.

For $n = 1$, we just have $\chi_\rho = 1$, so $\langle \chi_\rho, \chi_\rho \rangle = 1$. □

Problem 8. A representation $\rho : G \to GL(V)$ is called *faithful* if ρ is injective. Find a faithful representation of the quaternion group Q_8 of the smallest dimension.

Solution. Since Q_8 is not abelian, it has no faithful representation of dimension one. On the other hand, Q_8 admits the two-dimensional faithful representation

$$\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \right\}.$$

□

Problem 9. Let G be a p-group and H be the subgroup of all central elements g with $g^p = 1$. Let ρ be a representation of G. Prove that if the restriction $\rho|_H$ of ρ on H is faithful, then ρ is faithful.

Solution. We show the contrapositive. Suppose ρ is not faithful, so then $\ker \rho$ is non-trivial. As it is a normal subgroup, the p-group G acts on $\ker \rho$ by conjugation, and since $p \mid |\ker \rho|$, the number of fixed points $|Z \cap \ker \rho|$ is divisible by p. Since $1 \in Z \cap \ker \rho$, there is a non-trivial element $g \in Z \cap \ker \rho$. If the order of g in G is p^k, then $h = g^{p^{k-1}} \in Z \cap \ker \rho$ is non-trivial with $h^p = 1$, so $h \in H \cap \ker \rho = \ker \rho|_H$ is non-trivial. Thus $\rho|_H$ is not faithful. □

Problem 10. Let $\rho : G \to GL(V)$ be a faithful representation of G. Prove that every simple G-space W is a direct summand of the tensor product of several copies of V.

Solution. Since W is simple, it suffices to show that $\langle \chi_\rho^k, \chi_W \rangle \neq 0$ for some k.

Let $\dim \rho = d$ and $|G| = n$, then let H be the subgroup of all $g \in G$ such that g acts as scalar multiplication. Since ρ is faithful, H is a finite group embedding into $\mathbb{C}^\times$, so H is cyclic, generated by some $h \in H$. Moreover, if $|H| = m$, then $\chi_\rho(h^j) = d\zeta^j$, where ζ is a primitive m-th root of unity. For $g \notin H$, we have $|\chi_\rho(g)| < d$. Therefore, for each $0 \leq r < m$,

$$L_r = \lim_{k\to\infty} \frac{\langle \chi_\rho^{km+r}, \chi_W \rangle}{d^{kn+r}} = \frac{1}{n} \sum_{g\in H} \chi_W(g^{-1}) \left(\frac{\chi_\rho(g)}{d} \right)^{km+r} = \frac{1}{n} \sum_{j=0}^{m-1} \zeta^{jr} \chi_W(h^{-j}).$$

The only way to have $L_r = 0$ for all r is to have $\chi_W(h^{-j}) = 0$ for all j, but $\chi_W(1) = \dim W > 0$. Hence for some r, we have $L_r \neq 0$, and so for k sufficiently large, $\langle \chi_\rho^{km+r}, \chi_W \rangle \neq 0$. □

HOMEWORK C8 - SOLUTIONS

Problem 1. Let $A = (a, b)$ be a quaternion algebra over a field F of characteristic different from 2. Prove that $A \cong M_2(F)$ if and only if the equation $ax^2 + by^2 = z^2$ has a non-zero solution in F.

Solution. If $ax^2 + by^2 = z^2$ for $x, y, z \in F$ not all zero, then

$$(z + x\mathbf{i} + y\mathbf{j})(z - x\mathbf{i} - y\mathbf{j}) = (z - x\mathbf{i} - y\mathbf{j})(z + x\mathbf{i} + y\mathbf{j}) = z^2 - ax^2 - by^2 = 0 \qquad (*)$$

by direct expansion, so A is not a division algebra. Therefore, $A \cong M_2(F)$.

On the other hand, suppose $ax^2 + by^2 = z^2$ has no non-zero solution. From $(*)$, it follows after dividing through by $z^2 - ax^2 - by^2$ that $z + x\mathbf{i} + y\mathbf{j}$ is invertible for x, y, z not all zero. For an element $\alpha = w + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ of A with $z \neq 0$, we can write

$$w + x\mathbf{i} + y\mathbf{j} + z\mathbf{k} = (y + z\mathbf{i})(u + v\mathbf{i} + \mathbf{j})$$

with $(y + z\mathbf{i})(u + v\mathbf{i}) = w + x\mathbf{i}$. Since $y + z\mathbf{i}$ is invertible as $z \neq 0$, there exist u, v satisfying this condition. Hence we can write α as a product of two invertible elements, so α is invertible. We have thus shown that A is a division algebra, so $A \ncong M_2(F)$. □

Problem 2. Let $A_1 = (a, b_1)$ and $A_2 = (a, b_2)$ be two quaternion algebras over a field F of characteristic different from 2. Prove that $A_3 = (a, b_1b_2)$ is isomorphic to a subalgebra of $A_1 \otimes A_2$.

Solution. We seek an injective homomorphism $f : A_3 \to A_1 \otimes A_2$. For this, we define

$$\mathbf{i} \overset{f}{\mapsto} \mathbf{i} \otimes 1 \qquad \text{and} \qquad \mathbf{j} \overset{f}{\mapsto} \mathbf{j} \otimes \mathbf{j}$$

and extend it to a ring homomorphism. This respects the relations, as

$$\begin{aligned} f(\mathbf{i}^2) &= (\mathbf{i} \otimes 1)(\mathbf{i} \otimes 1) = \mathbf{i}^2 \otimes 1 = a(1 \otimes 1) = f(a), \\ f(\mathbf{j}^2) &= (\mathbf{j} \otimes \mathbf{j})(\mathbf{j} \otimes \mathbf{j}) = \mathbf{j}^2 \otimes \mathbf{j}^2 = b_1b_2(1 \otimes 1) = f(b_1b_2), \\ f(\mathbf{ij}) &= (\mathbf{i} \otimes 1)(\mathbf{j} \otimes \mathbf{j}) = (\mathbf{ij} \otimes \mathbf{j}) = -(\mathbf{ji} \otimes \mathbf{j}) = f(-\mathbf{ji}), \end{aligned}$$

so it is well-defined. For injectivity,

$$0 = f(w + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}) = w(1 \otimes 1) + x(\mathbf{i} \otimes 1) + y(\mathbf{j} \otimes \mathbf{j}) + z(\mathbf{k} \otimes \mathbf{j})$$

implies that $w = x = y = z = 0$. □

Problem 3. In the conditions of Problem 2, compute the centralizer of A_3 in $A_1 \otimes A_2$. Deduce that $[A_3] = [A_1][A_2]$ in $\mathrm{Br}(F)$.

Solution. It suffices to compute the centralizer of the basis $\{1 \otimes 1, \mathbf{i} \otimes 1, \mathbf{j} \otimes \mathbf{j}, \mathbf{k} \otimes \mathbf{j}\}$. By inspection, this contains $\{1 \otimes 1, 1 \otimes \mathbf{j}, \mathbf{i} \otimes \mathbf{i}, \mathbf{i} \otimes \mathbf{k}\}$. By the double centralizer theorem and counting dimensions, we have found a basis for the entire centralizer. Note also that this is the quaternion algebra (a^2, b_2), which by Problem 1 is isomorphic to $M_2(F)$. Hence by the double centralizer theorem again,

$$[A_1][A_2] = [A_1 \otimes_F A_2] = [A_3 \otimes_F C_{A_1 \otimes_F A_2}(A_3)] = [A_3][C_{A_1 \otimes_F A_2}(A_3)] = [A_3].$$

□

Problem 4. Prove that the endomorphism σ of the quaternion algebra $A = (a, b)$ (over a field F of characteristic different from 2) given by

$$\sigma(w + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}) = w - x\mathbf{i} - y\mathbf{j} - z\mathbf{k}$$

is an *involution* of A, i.e. $\sigma(uv) = \sigma(v)\sigma(u)$ for all $u, v \in A$ and $\sigma \circ \sigma = \mathrm{id}_A$.

Solution. That $\sigma \circ \sigma = \mathrm{id}_A$ is trivial. To see that $\sigma(uv) = \sigma(v)\sigma(u)$ for all $u, v \in A$, by linearity, it suffices to check this on the basis elements $\{1, \mathbf{i}, \mathbf{j}, \mathbf{z}\}$.

When $u = 1$, we have $\sigma(u) = 1$, so the result holds. Similarly, we are done if $v = 1$.

Otherwise, both u and v are imaginary basis vectors, so $\sigma(u) = -u$ and $\sigma(v) = -v$. If $u = v$, then $uv = u^2 \in F^\times$, so $\sigma(u^2) = u^2 = \sigma(u)^2$. If $u \neq v$, then uv is also an imaginary basis vector and $uv = -vu$, so $\sigma(uv) = -uv = vu = (-v)(-u) = \sigma(v)\sigma(u)$. □

Problem 5. In the setup of Problem 4, prove that every element $u \in A$ is a root of the quadratic polynomial $t^2 - (u + \sigma(u))t + u\sigma(u)$ over F.

Solution. For $u = w + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$, we can compute

$$u + \sigma(u) = 2w \in F \qquad \text{and} \qquad u\sigma(u) = \sigma(u)u = w^2 + ax^2 + by^2 - abz^2 \in F.$$

Substitution of $t = u$ gives

$$u^2 - (u + \sigma(u))u + u\sigma(u) = u^2 - u^2 - \sigma(u)u + u\sigma(u) = 0.$$

□

Problem 6. Let A be an F-algebra. Prove that A is isomorphic to the algebra $M_n(B)$ for some n and F-algebra B if and only if there are elements $e_{ij} \in A$ for $i, j = 1, \ldots, n$ satisfying $\sum_i e_{ii} = 1$ and $e_{ij}e_{kl} = \delta_{jk}e_{il}$.

Solution. If $A \cong M_n(B)$, let e_{ij} correspond to the matrix with 1 in position i, j and 0 elsewhere.

Conversely, observe that the e_{ij}'s are linearly independent over F, as if $\sum_{i',j'} \lambda_{i'j'}e_{i'j'} = 0$, then multiplying on the left by e_{ii} and on the right by e_{jj} gives $\lambda_{ij} = 0$ for any i, j. From this and the relations given, the F-linear span of the e_{ij}'s is isomorphic to $M_n(F)$ as F-algebras.

Next, consider the set

$$B = \left\{ \sum_{k=1}^{n} e_{ki}ae_{jk} \mid a \in A \text{ and } 1 \leq i, j \leq n \right\} = \left\{ \sum_{k=1}^{n} e_{k1}ae_{1k} \mid a \in A \right\} \subset A.$$

We claim that this is in fact an F-subalgebra. By letting $a = 0$ and $i = j = 1$, we get $0 \in B$. By letting $a = 1$ and $i = j = 1$, we get

$$\sum_{k=1}^{n} e_{k1}e_{1k} = \sum_{k=1}^{n} e_{kk} = 1 \in B.$$

To see that B is an F-vector space, we write

$$B = \left\{ \sum_{k=1}^{n} e_{ki} a e_{jk} \right\} = \left\{ \sum_{k=1}^{n} e_{k1} a' e_{1k} \mid a' \in A \right\}$$

by setting $a' = e_{1i} a e_{j1}$ to get the non-trivial inclusion and noting that the latter set is an F-vector space. Finally, for closure under multiplication, we multiply

$$\left(\sum_{k=1}^{n} e_{ki} a e_{jk} \right) \left(\sum_{k'=1}^{n} e_{k'i'} b e_{j'k'} \right) = \sum_{k=1}^{n} e_{ki} a e_{ji'} b e_{i'k} \in B.$$

Define the map $f : A \to B \otimes_F \operatorname{span}(e_{ij}) \cong B \otimes_F M_n(F) \cong M_n(B)$ by

$$f(a) = \sum_{i,j=1}^{n} \left(\sum_{k=1}^{n} e_{ki} a e_{jk} \right) \otimes e_{ij}.$$

This is clearly F-linear, while

$$f(1) = \sum_{i,j=1}^{n} \left(\sum_{k=1}^{n} e_{ki} e_{jk} \right) \otimes e_{ij} = \sum_{i=1}^{n} \sum_{k=1}^{n} e_{kk} \otimes e_{ii} = 1 \otimes 1.$$

For multiplicativity,

$$\begin{aligned} f(a)f(b) &= \left(\sum_{i,j=1}^{n} \left(\sum_{k=1}^{n} e_{ki} a e_{jk} \right) \otimes e_{ij} \right) \left(\sum_{i',j'=1}^{n} \left(\sum_{k'=1}^{n} e_{k'i'} b e_{j'k'} \right) \otimes e_{i'j'} \right) \\ &= \sum_{i,j,j'=1}^{n} \left(\sum_{k,k'=1}^{n} e_{ki} a e_{jk} e_{k'j} b e_{j'k'} \right) \otimes e_{ij'} \\ &= \sum_{i,j,j'=1}^{n} \left(\sum_{k=1}^{n} e_{ki} a e_{jj} b e_{j'k} \right) \otimes e_{ij'} \\ &= \sum_{i,j'=1}^{n} \left(\sum_{k=1}^{n} e_{ki} a b e_{j'k} \right) \otimes e_{ij'} = f(ab). \end{aligned}$$

Hence f is an F-algebra homomorphism.

To see that f is injective, suppose $f(a) = 0$. Then $\sum_k e_{ki} a e_{jk} = 0$ for all i, j since the e_{ij} form a basis for $M_n(F)$, and multiplying on the left by e_{ii} and on the right by e_{jj} gives $e_{ii} a e_{jj} = 0$ for all i, j. Summing over i and j gives $a = 0$.

To see that f is surjective, consider an arbitrary element $\sum_{i,j} b_{ij} \otimes e_{ij}$ in $B \otimes_F M_n(F)$, with $b_{ij} = \sum_k e_{ki} a_{ij} e_{jk}$ for some $a_{ij} \in A$. If $a = \sum_{i,j} e_{ii} a_{ij} e_{jj}$, then the same types of calculations give that $f(a) = \sum_{i,j} b_{ij} \otimes e_{ij}$. Thus we have the required isomorphism of F-algebras. $\square$

Problem 7. Let L/F be a field extension of degree n. Prove that L is isomorphic to a subalgebra of $M_n(F)$.

Solution. Fix a basis of L/F. For any $\alpha \in L$, multiplication by α induces an F-linear map, which gives a matrix in $M_n(F)$ with respect to the chosen basis. Since L is a field and an F-algebra, the set of all matrices obtained in this way forms an F-subalgebra of $M_n(F)$. □

Problem 8. Let A and B be two F-algebras such that B is simple and $M_n(A)$ is isomorphic to a subalgebra of $M_n(B)$. Prove that A is isomorphic to a subalgebra of B.

Solution. To be written. □

Problem 9. Let A be a central simple F-algebra of degree n and L/F be a field extension of degree kn such that L is isomorphic to a subalgebra of $M_k(A)$. Prove that L is a splitting field of A.

Solution. The central simple F-algebra $M_k(A)$ has degree $kn = [L : F]$, so by a theorem from class, L is a splitting field of $M_k(A)$. Therefore, $[M_k(A)] = [M_k(F)][A]$ is in the kernel of the homomorphism of Brauer groups induced by extension by scalars. Since $[M_k(F)] = 1 \in Br(F)$, it follows that $[A]$ is in this kernel, so L is a splitting field of A. □

Problem 10. Let A be a central division F-algebra of degree n and L/F be a splitting field of degree s. Prove that n divides s and L is isomorphic to a subalgebra of $M_{s/n}(A)$.

Solution. To be written. □