MATH 4803/8803
MIDTERM EXAMINATION

Name	

1	2	3	4	5	Total

- Solve **four** of the five problems on this exam. **Circle** which problems you'd like to be graded in the grid above.
- Each problem is worth 10 points. The maximum score on this exam is 40 points.
- You have 50 minutes to complete this exam.
- There are no aids of any kind (notes, text, etc.) allowed.
- All answers must be justified unless otherwise noted, and all proofs must be written in clear and grammatical English.
- You may cite any theorem, lemma, proposition, etc. proved in class or in the sections we covered in the text.
- Good luck!

Problem 1.

Let A be an integral domain and M an A-module. The *torsion submodule* of M is the subset of all torsion elements:

$$M_{\text{tors}} := \{x \in M \mid \exists a \in A \setminus \{0\} \text{ such that } ax = 0\}.$$

i. Prove that M_{tors} is a submodule of M.

ii. Prove that M/M_{tors} is torsionfree, i.e. that $(M/M_{\text{tors}})_{\text{tors}} = 0$.

iii. If A is a PID and $M \cong A/(a_1) \times \cdots \times A/(a_n) \times A^r$ as in the classification theorem, what are M_{tors} and M/M_{tors}? What is the annihilator of M?

Solution.

i. Clearly $0 \in M_{\text{tors}}$. For $x, y \in M_{\text{tors}}$ there exist $a, b \in A \setminus \{0\}$ such that $ax = by = 0$. Since A is a domain, $ab \neq 0$. We have $ab(x - y) = 0$, so $x - y \in M_{\text{tors}}$, and thus M_{tors} is a subgroup of M. Also for $r \in A$ we have $a(rx) = r(ax) = r \cdot 0 = 0$, so M_{tors} is a submodule.

ii. Let $\overline{x} = x + M_{\text{tors}} \in M/M_{\text{tors}}$, and suppose that there exists $a \in A \setminus \{0\}$ such that $a\overline{x} = 0$. Then $ax \in M_{\text{tors}}$, so there exists $b \in A \setminus \{0\}$ such that $abx = 0$. As above $ab \neq 0$, so $x \in M_{\text{tors}}$, and therefore $\overline{x} = 0$.

iii. Let

$$x = (x_1, \ldots, x_n, y) \in A/(a_1) \times \cdots \times A/(a_n) \times A^r,$$

and suppose that $ax = 0$ for some $a \in A \setminus \{0\}$. Then $ax_i \in (a_i)$ for all i, and $ay = 0$. This latter is only possible when $y = 0$, so $M_{\text{tors}} \subset A/(a_1) \times \cdots \times A/(a_n)$. On the other hand, if $y = 0$ then $a_n x = 0$ (since $a_i \mid a_n$ for all i), so this inclusion is an equality. Define $\varphi \colon M \twoheadrightarrow A^r$ by $(x_1, \ldots, x_n, y) \mapsto y$. Then $\ker(\varphi) = M_{\text{tors}}$, so $M/M_{\text{tors}} \cong A^r$.

If $r = 0$ then $a \in \operatorname{Ann}(M)$ if and only if

$$0 = a(1, 0, \ldots, 0) = a(0, 1, 0, \ldots, 0) = \cdots = a(0, 0, \ldots, 1),$$

which holds precisely when $a \in (a_1) \cap \cdots \cap (a_n) = (a_n)$. Hence $\operatorname{Ann}(M) = (a_n)$. If $r \neq 0$ then $\operatorname{Ann}(M) = 0$ since no element kills all of A^r.

Problem 2.

Give an example of an integral domain which is not integrally closed. Justify your answer.

Solution.

The ring $\mathbf{Z}[\sqrt{-3}]$ is not integrally closed: its fraction field is $\mathbf{Q}(\sqrt{-3})$, and $\zeta_3 \notin \mathbf{Z}[\sqrt{-3}]$ is integral over $\mathbf{Z}[\sqrt{-3}]$ because it satisfies the equation $\zeta_3^2 + \zeta_3 + 1 = 0$.

Problem 3.

Let A be a subring of B, with B integral over A. Prove that $B^\times \cap A = A^\times$. Show this is false in general without the integrality hypothesis.

Solution.

Clearly $A^\times \subset B^\times$. Let $x \in B^\times \cap A$. Then x has an inverse $x^{-1} \in B$. As B is integral over A, the inverse satisfies an equation of integral dependence

$$x^{-n} + a_{n-1}x^{-(n-1)} + a_{n-2}x^{-(n-2)} + \cdots + a_1 x^{-1} + a_0 = 0$$

for $a_0, a_1, \ldots, a_{n-1} \in A$. Multiplying by x^{n-1} and rearranging, we have

$$x^{-1} = -\big(a_{n-1} + a_{n-2}x + \cdots + a_1 x^{n-2} + a_0 x^{n-1}\big) \in A.$$

Without the integrality hypothesis, we have $\mathbf{Z} \subset \mathbf{Q}$, and $\mathbf{Q}^\times \cap \mathbf{Z} = \mathbf{Z} \setminus \{0\}$, whereas $\mathbf{Z}^\times = \{\pm 1\}$.

Problem 4.

Let x be a cube root of 2 and let $K = \mathbf{Q}(x)$. This is a cubic extension of $\mathbf{Q}$.

i. Let $z = a + bx + cx^2 \in K$ for $a, b, c \in \mathbf{Q}$. Find the conjugates of z in $\mathbf{C}$. Calculate the trace, norm, and characteristic polynomial of z over $\mathbf{Q}$.

ii. Show that $\mathbf{Z}[x] \subset \mathscr{O}_K$, find a basis for $\mathbf{Z}[x]$ as a $\mathbf{Z}$-module, and show that $\mathrm{Frac}(\mathbf{Z}[x]) = K$.

iii. Show that $6\mathscr{O}_K \subset \mathbf{Z}[x]$. [Let $z = a+bx+cx^2 \in \mathscr{O}_K$ for $a, b, c \in \mathbf{Q}$. Calculate the traces of z, xz, and x^2z.]

Solution.

i. The conjugates of z are the images of z under the three $\mathbf{Q}$-embeddings $\sigma_1, \sigma_2, \sigma_3$ of K into $\mathbf{C}$. We may take $\sigma_1(x) = x$, $\sigma_2(x) = \zeta_3 x$, and $\sigma_3(x) = \zeta_3^2 x$, the roots of the minimal polynomial $X^3 - 2$ of x. Therefore the conjugates of z are

$$z, \quad a + bx\zeta_3 + cx\zeta_3^2, \quad a + bx\zeta_3^2 + cx^2\zeta_3.$$

Note that these are the same number if and only if $z \in \mathbf{Q}$. The matrix for multiplication by z is given in the basis $1, x, x^2$ by

$$m_z = \begin{bmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix}.$$

Hence

$$\mathrm{Tr}(z) = \mathrm{Tr}(m_z) = 3a \quad \text{and} \quad N(z) = \det(m_z) = a^3 + 2b^3 + 4c^3 - 6abc.$$

The characteristic polynomial is

$$\det(XI_3 - m_z) = X^3 - \mathrm{Tr}(z)X^2 + (3a^2 - 6bc)X + N(z).$$

ii. Since x satisfies $x^3 - 2 = 0$, we have $x \in \mathscr{O}_K$; clearly $\mathbf{Z} \subset \mathscr{O}_K$, so $\mathbf{Z}[x] \subset \mathscr{O}_K$. Repeatedly substituting $x^3 = 2$ into any integer polynomial in x shows that $1, x, x^2$ span $\mathbf{Z}[x]$. As $1, x, x^2$ are linearly independent in K, they are linearly independent in $\mathbf{Z}[x]$, so they are a basis. Since $\mathbf{Z}[x] \subset K$ we have $\mathrm{Frac}(\mathbf{Z}[x]) \subset K$. Any element of K has the form $z = a+bx+cx^2$ for $a, b, c \in \mathbf{Q}$; if $n \in \mathbf{Z}$ clears the denominators of a, b, c, then $nz \in \mathbf{Z}[x]$. Hence $z = (nz)/n \in \mathrm{Frac}(\mathbf{Z}[x])$, so $K \subset \mathrm{Frac}(\mathbf{Z}[x])$.

iii. Let $z = a + bx + cx^2 \in \mathscr{O}_K$ for $a, b, c \in \mathbf{Q}$. Then $\mathrm{Tr}(z) = 3a$, $\mathrm{Tr}(xz) = 6c$, and $\mathrm{Tr}(x^2z) = 6b$. On the other hand, $z, xz, x^2z \in \mathscr{O}_K$, so their traces are integers. Thus $6z \in \mathbf{Z}[x]$.

Problem 5.

Let A be a subring of a ring C such that $C \cong A^n$ as A-modules, and let $B \subset C$ be a subring containing A, so $A \subset B \subset C$. Suppose that A is a principal ideal domain.

i. Show that B is a finitely generated free A-module.

ii. Suppose that B also has rank n. Let $x_1, \ldots, x_n \in B$ and $y_1, \ldots, y_n \in C$ be bases. Prove that

$$D(x_1, \ldots, x_n) = D(y_1, \ldots, y_n) \cdot d^2$$

for some $d \in A$.

iii. Conclude that if $D(x_1, \ldots, x_n)$ is nonzero and squarefree then $B = C$.

Solution.

i. First note that B is a submodule of the finitely generated free A-module C. Since A is noetherian, B is itself finitely generated, so there exists a surjection $A^m \twoheadrightarrow B$. Let M be the matrix for the composition $\varphi\colon A^m \to B \hookrightarrow C \cong A^n$. Since M has a Smith normal form, there exist bases $x_1, \ldots, x_m$ for A^m and $y_1, \ldots, y_n$ for A^n such that $\varphi(x_i) = a_i y_i$ for $1 \le i \le \min\{n, m\}$ and $a_i \in A$, and such that $\varphi(x_i) = 0$ for $i > n$. It follows that B is free and that some subset of $x_1, \ldots, x_m$ map to a basis for B.

ii. When B has rank n, the argument in (i) shows that there exist bases $x_1, \ldots, x_n$ for B and $y_1, \ldots, y_n$ for C and scalars $a_1, \ldots, a_n \in A$ such that $a_i y_i = x_i$ for all i. Hence

$$\begin{aligned}
D(x_1, \ldots, x_n) &= \det(\mathrm{Tr}(x_i x_j)) = \det(a_i a_j \, \mathrm{Tr}(y_i y_j)) \\
&= \det \begin{bmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{bmatrix} \det(\mathrm{Tr}(y_i y_j)) \det \begin{bmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{bmatrix} \\
&= D(y_1, \ldots, y_n) \cdot (a_1 \cdots a_n)^2.
\end{aligned}$$

We showed in class that if $y_1', \ldots, y_n'$ (resp. $x_1', \ldots, x_n'$) is another basis for C (resp. B), then $D(y_1', \ldots, y_n')$ (resp. $D(x_1', \ldots, x_n')$) differs from $D(y_1, \ldots, y_n)$ (resp. $D(x_1, \ldots, x_n)$) by the square of a unit in A, so

$$D(x_1', \ldots, x_n') = D(y_1', \ldots, y_n') \cdot (a_1 \cdots a_n)^2 u^2$$

for $u \in A^\times$.

iii. If $D(x_1, \ldots, x_n)$ is nonzero and squarefree then $d \in A^\times$ since $d^2 \mid D(x_1, \ldots, x_n)$. Hence each a_i is a unit, so $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ have the same span. It follows that $B = C$.

[Scratch work]