**THE UNIVERSITY OF BRITISH COLUMBIA**
**SESSIONAL EXAMINATIONS – APRIL 2013**
**MATHEMATICS 323**

**Time:** 2 hours 30 minutes

**Instructions:** You can use the statements we proved in class, or the theorems proved in the textbook, without proof (except the question 4e); but you need to provide complete statements of all the results you quote. Write your name and student number at the top of each booklet you use, and please number the booklets (e.g. “booklet 2 of 5”) if you use more than one.

1. [10 points] Determine whether the following statements are true or false (you have to include proofs/counterexamples):
   (a) Let $R$ be an integral domain, $F$ – a free $R$-module of finite rank, and $M$ – a torsion $R$-module. Then there is no injective homomorphism from $F$ to $M$.

   **Solution:** True. Suppose there was an injective homomorphism $\varphi : F \to M$. Then let $N = \varphi(F)$; $N$ is a submodule of $M$, and therefore is also a torsion module. On the other hand, $N$ is isomorphic to $F$ (since $\varphi$ is injective, it is an isomorphism from $F$ onto $N$), hence free. We proved in class that a free module over an integral domain has to be torsion-free. Hence, $\text{Tor}(N) = 0$; but we also have $\text{Tor}(N) = N$, so $N = 0$. Thus, $\varphi$ is a zero homomorphism, and therefore not injective – a contradiction (we are assuming $F \neq \{0\}$, i.e. the set of generators of $F$ is non-empty).

   (b) Over an arbitrary integral domain, any submodule of a free module is free.

   **Solution:** This is false. For example, take a non-principal ideal, e.g. $(2, x)$ in $\mathbb{Z}[x]$. It is a submodule of the free $\mathbb{Z}[x]$-module $M = \mathbb{Z}[x]$, but it is not free.

2. [8 points] Recall that for a module $M$, 
   \[ \text{Ann}(M) = \{ r \in R \mid rm = 0 \ \forall m \in M \}, \]

   and for an ideal $I \subset R$, 
   \[ \text{Ann}(I) = \{ m \in M \mid rm = 0 \ \forall r \in I \}. \]

   Let $R$ be an integral domain, let $M$ be an $R$-module, and suppose that $\text{Ann}(M) = IJ$, where $I$ and $J$ are co-maximal ideals in $R$. Prove that $M \cong M_1 \oplus M_2$, where $M_1 = \text{Ann}(I)$, and $M_2 = \text{Ann}(J)$.

   **Solution:** Since $I$ and $J$ are co-maximal, there exist $a_0 \in I$, $b_0 \in J$ such that $1 = a_0 + b_0$. Now, let $x \in M$. Then $x = 1 \cdot x = (a_0 + b_0)x = a_0x + b_0x$. Now, note that $a_0x \in M_2$, since $M$ is annihilated by $IJ$, and therefore $IM$ is annihilated by $J$, and $a_0x \in IM$. Similarly, $b_0x \in M_1$. Thus we have proved that $M = M_1 + M_2$.

   Now we need to check that the sum is direct, that is, $M_1 \cap M_2 = \{0\}$. Suppose that $x \in M_1 \cap M_2$. As above, we have $x = a_0x + b_0x$. Note that since $x \in M_1$, $a_0x = 0$, because $a_0 \in I$, and $I$ annihilates $M_1$. Similarly, $b_0x = 0$; but then we have $x = 0$. 


3. [22 points] In each question, factor the given element into irreducibles in
the given ring (or show that it is irreducible). (Include complete proofs of
irreducibility of the factors). If the factorization is unique, indicate why; if
not unique, please give two.
(a) \( x^4 - x^2 + 4 \) in \( \mathbb{F}_5[x] \).
This polynomial is reducible. We first look for roots in \( \mathbb{F}_5 \), (there are
none), and then look for quadratic factors. Note that the polynomial
\( y^2 - y + 4 = 0 \) has the double root \( y = 3 \), so our polynomial factors as
\( (x^2 - 3)^2 \). (Check: \( (x^2 - 3)^2 = x^4 - 6x^2 + 9 = x^4 - x^2 + 4 \) (remember
that all the calculations are in \( \mathbb{F}_5 \) !) The polynomial \( x^2 - 3 \) is irre-
ducible, since it clearly does not have a root in \( \mathbb{F}_5 \) (remember that for
polynomials of degree not greater than 3 this is a sufficient condition
of irreducibility). The factorization is unique, since the polynomial
ring over a field is a PID.
(b) \( 12 \) in \( \mathbb{Z} \{\sqrt{-3}\} \).
There are two factorizations (up to associates):
\( 12 = -2 \cdot 2 \cdot \sqrt{-3}^2 = -(1 + \sqrt{-3})(1 - \sqrt{-3})\sqrt{-3}^2 \).
One shows that all the factors listed above are irreducible using the
norm. Recall that the norm of an element is the square of its complex
absolute value. For example, let us show that \( 1 + \sqrt{-3} \) is irreducible
in this ring. Suppose we had \( 1 + \sqrt{-3} = \alpha \beta \). Then we’d have \( N(1 + \sqrt{-3}) = N(\alpha)N(\beta) \), so \( 4 = N(\alpha)N(\beta) \). Then, since we need \( \alpha \) and
\( \beta \) to be not units, the only possibility is \( N(\alpha) = N(\beta) = 2, \) but that
is impossible since one cannot write \( 2 = a^2 + 3b^2 \) for integers \( a, b \).
Irreducibility of the other factors is proved similarly.
(c) \( 12 \) in \( \mathbb{Z} \{\sqrt{-3} + 1\} \). Explain the relationship with part (c).
This ring is Euclidean, and hence a PID and a UFD. All the elements
in the factorizations from (b) are still irreducible, but now the two
factorizations are associate, since \( 2 = \frac{1 + \sqrt{-3}}{2}(1 - \sqrt{-3}) \), and \( \frac{1 + \sqrt{-3}}{2} \) is a
unit.
(d) \( 3x^4 - 6x^3 + 12x^2 - 18x + 6 \) in \( \mathbb{Q}[x] \), and in \( \mathbb{Z}[x] \).
In \( \mathbb{Z}[x] \), this polynomial factors as \( f(x) = 3(x^4 - 2x^3 + 4x^2 - 6x + 2) \),
and the factor \( g(x) = (x^4 - 2x^3 + 4x^2 - 6x + 2) \) is irreducible by
Eisenstein’s criterion (use \( p = 2 \)).
In \( \mathbb{Q}[x] \), \( f \) and \( g \) are associate, and \( g \) is irreducible by Gauss’ Lemma,
since it is monic and irreducible over \( \mathbb{Z} \).
(e) \( x^{p-2} + x^{p-3} + \ldots + 1 \) in \( \mathbb{F}_p[x] \), where \( p \) is a prime.
Note that the multiplicative group \( \mathbb{F}_p^\times \) of \( \mathbb{F}_p \) has order \( p - 1 \); hence
\( x^{p-1} = 1 \) in \( \mathbb{F}_p^\times \) for all \( x \in \mathbb{F}_p \), \( x \neq 0 \). Thus, every non-zero element
of \( \mathbb{F}_p \) is a root of the polynomial \( x^{p-1} - 1 \). Therefore, \( x^{p-1} = (x - 1)(x - 2)\ldots(x - (p - 1)) \), where we think of \( \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \) as the set
\( \{0, 1, \ldots, p-1\} \). Now note that \( x^{p-1} = (x - 1)(x^{p-2} + \ldots + x + 1) =
(x - 1) f(x) \). Therefore, our polynomial \( f(x) \) factors into linear factors
over \( \mathbb{F}_p \):
\[ f(x) = (x - 2)(x - 3)\ldots(x - (p - 1)). \]
4. [22 points]
(a) Is the ideal \( I = \{a + bi \mid a, b \text{ are both even}\} \) a maximal ideal in \( \mathbb{Z}[i] \)?

No (see part (b) below for a better proof).

One can compute the quotient \( \mathbb{Z}[i]/I \) and see that it has 4 elements:

- the classes of 0, 1, \( i \), and \( 1 + i \). (Note that it is not isomorphic to any
- nice and familiar ring of 4 elements: it is not \( \mathbb{Z}/4\mathbb{Z} \) or \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \),
- and definitely not the field \( \mathbb{F}_4 \). Note that the element \( 1 + i \in \mathbb{Z}[i]/I \)
- is nilpotent: \((1 + i)^2 = 2i \in I\), and hence \( 1 + i^2 = 0 \). Thus \( \mathbb{Z}[i]/I \) is
- not a field, and so \( I \) is not maximal.

(b) Prove that the ideal \( I \) from part (a) is principal, and find the generator
- of \( I \).

\( I \) has to be principal since \( \mathbb{Z}[i] \) is Euclidean; it is easy to check that
\( I = \langle 2 \rangle \). Now, since \( \mathbb{Z}[i] \) is a PID, an ideal is maximal if and only
if it is prime, and that happens iff it is generated by an irreducible
- element. The element 2 is not irreducible: \( 2 = (1 + i)(1 - i) \), so \( I \) is
- not maximal.

(c) Prove that \( (7) \) is a prime ideal in \( \mathbb{Z}[i] \). Describe the quotient \( \mathbb{Z}[i]/(7) \).

The element 7 is irreducible (as usual, using the norm: if it factored,
both factors would have to be units or have the norm 7, but it is
impossible to have norm 7: \( a^2 + b^2 = 7 \) has no solutions with integers
\( a, b \). Hence, \( (7) \) is prime, and therefore maximal (all this works since
\( \mathbb{Z}[i] \) is a PID). Then the quotient is a field; so it is the field of 49
- elements.

(d) Let \( p > 2 \) be a prime such that the field \( \mathbb{F}_p \) contains an element \( a \) such
- that \( a^2 = -1 \) (in \( \mathbb{F}_p \)). Prove that then \( (p) \) is not a maximal ideal in
\( \mathbb{Z}[i] \).

Existence of \( a \) such that \( a^2 = -1 \) in \( \mathbb{F}_p \) is equivalent to saying that
the polynomial \( x^2 + 1 \) is reducible over \( \mathbb{F}_p \), which is equivalent to
\( \mathbb{F}_p[x]/(x^2 + 1) \) being not a field. We have:

\[
\mathbb{F}_p[x]/(x^2 + 1) = (\mathbb{Z}/p\mathbb{Z})[x]/(x^2 + 1) \cong (\mathbb{Z}[x]/(x^2 + 1))/(p) \cong \mathbb{Z}[i]/(p),
\]

where the next-to-last isomorphism follows from the fact that \( R[x]/IR[x] \cong
(R/I)[x] \) that we proved in class. Thus we proved that \( \mathbb{Z}[i]/(p) \) is not
- a field (i.e. \( p \) is not a maximal ideal) iff there exists \( a \in \mathbb{F}_p \) such that
\( a^2 = -1 \).

(e) Prove that every prime number \( p \) that is congruent to 1 mod 4 can be
- represented as a sum of two squares.

Continuing the argument of Part (c), an element \( p \) is not prime in
\( \mathbb{Z}[i] \) iff it is reducible, and being reducible means that it factors as a
product of two elements of norm \( p \), which means that \( p = a^2 + b^2 \)
for some \( a, b \in \mathbb{Z} \). Thus we have proved the following: \( p \) can be
represented as a sum of two squares iff it is a reducible element of
\( \mathbb{Z}[i] \), which happens iff the ideal \( (p) \) is not maximal in \( \mathbb{Z}[i] \), which is
equivalent to the existence of an element \( a \in \mathbb{F}_p \) such that \( a^2 = -1 \)
(I will call such an element a "square root of \(-1\)").

It remains to prove that for every prime \( p \) such that \( p \equiv 1 \mod 4 \),
there exists a square root of \(-1\) in \( \mathbb{F}_p \). Note that a square root of
\(-1 \) is an element of order 4 in the multiplicative group \( \mathbb{F}_p^\times \). Such an
element exists iff the order of the group (i.e. \( p - 1 \)) is divisible by 4.
Note: This was a deliberately hard problem; it is also discussed in Section 8.3 "Factorization in the Gaussian Integers" in DF.

5. [7 points] Let $N$ be the submodule of $\mathbb{Z}^3$ generated by the elements $(1, 2, 3)$ and $(4, 5, 6)$. Describe the quotient $\mathbb{Z}^3/N$ (as a $\mathbb{Z}$-module).

Solution: Let us write the relations matrix for the generators of the module $N$, and use the row and column operations to diagonalize it. Then the diagonal elements will be the invariant factors of the module $\mathbb{Z}^3/N$.

We have:

\[
\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.
\]

Thus $\mathbb{Z}^3/N \simeq (\mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}$.

6. [12 points] Let $T : \mathbb{C}^4 \rightarrow \mathbb{C}^4$ be the linear operator defined by $(x_1, x_2, x_3, x_4) \mapsto (x_2, x_3, x_4, ax_1)$ (with respect to the standard basis), where $a \neq 0$ is a complex number.

(a) Find the minimal polynomial of $T$.
(b) Find the characteristic polynomial of $T$.
(c) Decompose $\mathbb{C}^4$ with the $\mathbb{C}[x]$-module structure given by $T$ as a direct sum of cyclic $\mathbb{C}[x]$-submodules.

Hint: No heavy computation is required in this problem.

Solution sketch: The trick is that the matrix of this linear operator is already in the rational canonical form, and all the rest can be easily read off from here.

7. [7 points] Classify abelian groups of order 600 up to isomorphism.

Solution: Let us use the classification of finitely generated modules over $\mathbb{Z}$. Such an abelian group is a module annihilated by the ideal $(600)$. Factor 600 into primes: $600 = 2^3 \cdot 3 \cdot 5^2$. For every prime, the elementary divisors that are powers of this prime, multiplied together, have to give the power of our prime in the decomposition of 600. This means, the elementary divisors that are powers of 2 can be 2, 2, 2 or 2, 4 or 8. The elementary divisors that are powers of 5 can be 5, 5 or 25. The elementary divisor 3 always has to be present. Thus, there are 6 options for the set of elementary divisors, and 6 such groups: $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$, etc.

8. [12 points] Let $T : V \rightarrow V$ be a linear operator. The subspace $W \subseteq V$ is called invariant if $T(W) \subseteq W$.

(a) Give an example of a linear operator on a real vector space of dimension greater than 1 that does not have a 1-dimensional invariant subspace.
(b) Prove that any linear operator on a complex finite-dimensional vector space has at least one 1-dimensional invariant subspace.

Solution sketch: (a) Any rotation in the plane.

(b) Any linear operator has Jordan canonical form, which consists of at least one Jordan block. Each Jordan block corresponds to an invariant
subspace, and in that subspace there is exactly one eigenvector – namely, the first vector of the Jordan canonical basis.