MAT 3143 – Fall 2020

Final Exam – Solutions

Professor: Alistair Savage

Your solutions should be submitted through Brightspace as a ***single pdf file****. It is your responsibility to make sure that your handwriting is legible and that your scan is of high enough quality that it can be easily read. You should always justify your answer, unless otherwise specified.*

This exam ends at 12:30pm. You may not write anything on your pages after this time. You will then have until 12:40pm to scan and submit your solutions on Brightspace.

If you wish to leave the exam early, you must request permission in the Zoom chat. Once permission is granted, you may not write anything further on your pages, and you have 10 minutes to scan and submit your solutions.

QUESTION 1 **(6 pts)**. For this question, you do *not* need to justify your answers.

(a) Give an example of a field F and a finitely-generated $F[x]$-module that is not finitely generated as an F-module.

Solution: Let $F = \mathbb{R}$, and consider $\mathbb{R}[x]$ as a module over itself (i.e. the left regular module). Then, as an $\mathbb{R}[x]$-module, $\mathbb{R}[x]$ is generated by 1. However, it is not finitely generated as an $\mathbb{R}$-module since it is infinite dimensional.

(b) Give an example of a field F and reducible polynomial $f(x) \in F[x]$ with no roots in F.

Solution: Let $F = \mathbb{R}$. Then $f(x) = (x^2+1)^2$ is a reducible polynomial with no real roots.

(c) State the *structure theorem for finitely-generated modules over a principle ideal domain.*

Solution: Let R be a principle ideal domain, and let M be a nonzero finitely-generated R-module.

(i) The module M is a direct sum of cyclic modules,

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k) \oplus R^n,$$

where the a_i are nonzero, nonunit elements of R, and a_i divides a_j for $i \leq j$.

(ii) The decomposition in part (i) is unique in the following sense: Suppose

$$M \cong R/(b_1) \oplus R/(b_2) \oplus \cdots \oplus R/(b_l) \oplus R^m,$$

where the b_i are nonzero, nonunit elements of R, and b_i divides b_j for $i \leq j$. Then $k = l$, $m = n$, and $(a_i) = (b_i)$ for all i.

(d) State the *modular irreducibility test* for polynomials.

Solution: Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, $n \geq 1$, $a_n \neq 0$. Suppose that there exists a prime number p such that

- $p \nmid a_n$ and
- the reduction of $f(x)$ modulo p is irreducible in $\mathbb{Z}_p[x]$.

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

QUESTION 2 **(4 pts)**. Let I and J be ideals of a ring R.

(a) Prove that $I \cap J$ is an ideal of R.

Solution: Since $0 \in I$ and $0 \in J$, we have $0 \in I \cap J$. Furthermore, if $r, s \in I \cap J$, then $r, s \in I$ and $r, s \in J$. Thus $r - s \in I$ and $r - s \in J$. Hence $r - s \in I \cap J$. So $I \cap J$ is an additive subgroup of R.

Now suppose $s \in I \cap J$ and $r \in R$. Then $s \in I$ and $s \in J$. Hence $rs, sr \in I$ and $rs, sr \in J$. Thus $rs, sr \in I \cap J$.

(b) Is it necessarily true that $I \cup J$ is an ideal of R? Remember to justify your answer.

Solution: No, this is not necessarily true. For example, if $R = \mathbb{R}[x]$, $I = \langle x \rangle$, and $J = \langle x + 1 \rangle$, then $x, x + 1 \in I \cup J$, but $1 = (x + 1) - x \notin I \cup J$. So $I \cup J$ is not an additive subgroup.

QUESTION 3 **(4 pts)**.

(a) State the *Chinese Remainder Theorem*.

Solution: Let R be a ring and let A, B be two ideals of R such that $A + B = R$. Then $R/(A \cap B) \cong (R/A) \times (R/B)$.

(b) Gemma is trying to pack chocolates into boxes. When he tries to put them evenly into three boxes, one is left over. When she tries to put them evenly into seven boxes, two are left over. What are the possibilities for the number of chocolates that Gemma has?

Solution: Let x be the number of chocolates. Then we have

$$\bar{x} = \bar{1} \text{ in } \mathbb{Z}_3 \quad \text{and} \quad \bar{x} = \bar{2} \text{ in } \mathbb{Z}_7.$$

By the Chinese Remainder Theorem, we have $\mathbb{Z}_3 \times \mathbb{Z}_7 \cong \mathbb{Z}_{21}$. The elements of $\mathbb{Z}_{21}$ mapping to $\bar{2} \in \mathbb{Z}_7$ are $\bar{2}$, $\bar{9}$, and $\overline{16}$. Since $\bar{2} \in \mathbb{Z}_{21}$ maps to $\bar{2} \in \mathbb{Z}_3$, $\bar{9} \in \mathbb{Z}_{21}$ maps to $\bar{0} \in \mathbb{Z}_3$, and $\overline{16} \in \mathbb{Z}_{21}$ maps to $\bar{1} \in \mathbb{Z}_3$, we see that $\bar{x} = \overline{16}$ in $\mathbb{Z}_{21}$. Thus, Gemma has $16 + 21k$, $k \in \mathbb{Z}_{\geq 0}$, chocolates.

QUESTION 4 **(4 pts)**. Prove that $\mathbb{R}[x]/\big(\mathbb{R}[x](x^2 + 1)\big) \cong \mathbb{C}$ as rings.

Solution: Consider the map

$$\varphi \colon \mathbb{R}[x] \to \mathbb{C}, \quad \varphi(f(x)) = f(i).$$

Since φ is the composition of the inclusion $\mathbb{R}[x] \to \mathbb{C}[x]$ and the evaluation map $\mathbb{C}[x] \to \mathbb{C}$, $f(x) \mapsto f(i)$, it is a ring homomorphism. It surjective, since

$$\varphi(a + bx) = a + bi \quad \text{for all } a, b \in \mathbb{R}.$$

Since $\varphi(x^2 + 1) = 0$, we have $\mathbb{R}[x](x^2 + 1) \subseteq \ker(\varphi)$. Because $x^2 + 1$ is of degree 2 and has no roots in $\mathbb{R}$, it is irreducible in $\mathbb{R}[x]$. Thus, the ideal $\mathbb{R}[x](x^2 + 1)$ of $\mathbb{R}[x]$ is maximal. Since $\ker(\varphi) \neq \mathbb{R}[x]$, this implies that $\ker(\varphi) = \mathbb{R}[x](x^2 + 1)$. It then follows from the first isomorphism theorem for rings that

$$\mathbb{R}[x]/\big(\mathbb{R}[x](x^2 + 1)\big) \cong \mathbb{C}.$$

QUESTION 5 **(3 pts)**.

(a) State the *Rational Roots Theorem*.

Solution: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ with $a_0 \neq 0$, $a_n \neq 0$. If $r \in \mathbb{Q}$ and $f(r) = 0$, then $r = \frac{c}{d}$ with $c|a_0$ and $d|a_n$.

(b) Prove that $f(x) = x^3 + x^2 + 5x + 3$ is irreducible in $\mathbb{Q}[x]$.

Solution: Since $\deg f(x) = 3$, the polynomial $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if it has no rational roots. By the Rational Roots Theorem, the only possible rational roots are $\pm 1, \pm 3$. We compute

$$f(1) = 10, \quad f(-1) = -2, \quad f(3) = 54, \quad f(-3) = -30.$$

Thus $f(x)$ has no rational roots.

QUESTION 6 **(3 pts)**. Construct a field with 27 elements. Remember to justify that your ring is a field.

Solution: Consider the polynomial $f(x) = x^3 + x^2 - x + 1 \in \mathbb{Z}_3[x]$. Since

$$f(0) = 1, \quad f(1) = 2, \quad f(-1) = 2,$$

we see that $f(x)$ has no roots in $\mathbb{Z}_3$. Since $\deg f(x) = 3$, this implies that $f(x)$ is irreducible. Thus, the ideal $\langle f(x) \rangle$ is maximal, and so $\mathbb{Z}_3[x]/\langle f(x) \rangle$ is a field. Since is has a basis given by $ax^2 + bx + c + \langle f(x) \rangle$, $a, b, c \in \mathbb{Z}^3$, it has $3^3 = 27$ elements.

QUESTION 7 **(4 pts)**.

(a) State the *ascending chain condition on principal ideals* (ACCP).

Solution: We say an integral domain R satisfies the ascending chain condition on principal ideals if R contains no strictly increasing infinite chain

$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \cdots$$

of principal ideals.

(b) Prove that every principal ideal domain satisfies the ACCP.

Solution: Suppose R is a principal ideal domain and, towards a contradiction, that

$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$$

is a chain of principal ideals. Let $A = \bigcup_{i=1}^{\infty} \langle a_i \rangle$. Then A is an ideal of R. Thus, since R is a PID, we have $A = \langle a \rangle$ for some $a \in R$. Then $a \in \langle a_i \rangle$ for some i. Hence $\langle a_i \rangle = \langle a \rangle = A$ and so $\langle a_n \rangle = A$ for $n \geq i$, which is a contradiction. So R satisfies the ACCP.

QUESTION 8 **(7 pts)**.

(a) Find all the units in $\mathbb{Z}(\sqrt{-7}) := \{a + b\sqrt{-7} : a, b \in \mathbb{Z}\}$.

Solution: Note that

$$\left|a + b\sqrt{-7}\right|^2 = a^2 + 7b^2.$$

Suppose $a + b\sqrt{-7}$ is a unit. Then it has an inverse $c + d\sqrt{-7}$, and we have

$$\begin{aligned}(a + b\sqrt{-7})(c + d\sqrt{-7}) = 1 &\implies \left|a + b\sqrt{-7}\right|^2 \left|c + d\sqrt{-7}\right|^2 = |1|^2 \\ &\implies (a^2 + 7b^2)(c^2 + 7d^2) = 1.\end{aligned}$$

Since $a^2 + 7b^2$ and $c^2 + 7d^2$ are both nonnegative integers, this implies that $a^2 + 7b^2 = 1$, which implies that $a = \pm 1$, $b = 0$. Since 1 and -1 are clearly units, we have that $\mathbb{Z}(\sqrt{-7})^\times = \{\pm 1\}$.

(b) Show that $1 + \sqrt{-7}$ is an irreducible element of $\mathbb{Z}(\sqrt{-7})$ but is not prime.

Solution: Let $p = 1 + \sqrt{-7}$ and suppose $p = xy$. Then we have

$$|x|^2|y|^2 = |p|^2 = 8.$$

Since there are no $a, b \in \mathbb{Z}$ such that $a^2 + 7b^2 = 2$, this implies that $|x|^2 \neq 2$ and $|y|^2 \neq 2$. Therefore $|x|^2 = 1$ or $|y|^2 = 1$. Hence $x = \pm 1$ or $y = \pm 1$. So p is irreducible.

Suppose p is prime. Since

$$2^3 = 8 = (1 + \sqrt{-7})(1 - \sqrt{-7}),$$

we have $p|2$. So there exists some $r \in \mathbb{Z}(\sqrt{-7})$ such that $2 = pr$. Then

$$4 = |2|^2 = |p|^2|r|^2 = 8|r|^2.$$

Since $|r|^2 \in \mathbb{Z}_{\geq 0}$, this is a contradiction. Hence p is not prime.

QUESTION 9 **(4 pts)**.

(a) Suppose R is a ring. Define the *annihilator* $\operatorname{ann}(M)$ of an R-module M.

Solution: We have

$$\operatorname{ann}(M) = \{r \in R : ru = 0 \text{ for all } u \in M\}.$$

(b) Let V be a vector space over the field $\mathbb{R}$ of real numbers. Define the linear map

$$T \colon V \to V, \quad Tv = 2v,$$

and consider the associated $\mathbb{R}[x]$-module structure on V. Find a polynomial $p(x) \in \mathbb{R}[x]$ such that $\langle p(x) \rangle = \operatorname{ann}(V)$. Remember to justify your answer.

Solution: For all $v \in V$, we have

$$(x - 2)v = (T - 2)v = Tv - 2v = 0.$$

Thus $p(x) := x - 2 \in \operatorname{ann}(V)$, and so $\langle p(x) \rangle \subseteq \operatorname{ann}(V)$. Since $p(x)$ is linear, it is irreducible. Hence $\langle p(x) \rangle$ is a maximal ideal. It is clear that $\operatorname{ann}(V) \neq \mathbb{R}[x]$ since, for instance, $1 \notin \operatorname{ann}(V)$. Thus $\langle p(x) \rangle = \operatorname{ann}(V)$.

QUESTION 10 **(3 pts)**. Suppose M is a finite module over an infinite ring R. Prove that M is a free R-module if and only if $M = \{0\}$.

Solution: Since the zero module $\{0\}$ is free with the empty set as basis, it remains to prove the other implication. Suppose, towards a contradiction, that $M \neq \{0\}$ is free. Then M has a nonempty basis B. Let $u \in B$ and consider the function

$$\varphi\colon R \to M, \quad r \mapsto ru.$$

Since M is finite but R is infinite, this function cannot be injective. Thus there exist $r, s \in R$, $r \neq s$, such that $ru = su$. Hence $r - s \neq 0$ and $(r - s)u = 0$. This contradicts the assumption that B is linearly independent.

QUESTION 11 **(5 pts)**. Let R be an arbitrary ring.

(a) Define the *left regular module* of R.

Solution: The left regular module of R is R itself, considered as an R-module with its addition law and the action

$$R \times R \to R, \quad (r, v) \mapsto rv,$$

given by the product in R.

(b) Let $s \in R$. Prove that the map

$$\rho_s\colon R \to R, \quad \rho_s(r) = rs.$$

is a homomorphism of R-modules.

Solution: For $r, u, v \in R$, we have

$$\rho_s(u + v) = (u + v)s = us + vs = \rho_s(u) + \rho_s(v)$$

and

$$\rho_s(ru) = (ru)s = r(us) = r\rho_s(u).$$

(c) Prove that every homomorphism of R-modules $\varphi\colon R \to R$ is equal to ρ_s for a unique element $s \in R$.

Solution: Suppose $\varphi\colon R \to R$ is a homomorphism of R-modules. Let $s = \varphi(1)$. Then, for all $u \in R$, we have

$$\varphi(u) = \varphi(u \cdot 1) = u\varphi(1) = us = \rho_s(u).$$

Hence $\varphi = \rho_s$. Since $s = \varphi(1)$, we also see that the choice of s is unique.

QUESTION 12 **(3 pts)**. Suppose R is a commutative ring and $e \in R$ is an idempotent element. Furthermore, suppose that M is an R-module. For $r \in R$, define

$$rM := \{ru : u \in M\}.$$

Prove that $M = eM \oplus (1 - e)M$.

Solution: For $u \in M$, we have

$$u = 1 \cdot u = (e + 1 - e)u = eu + (1 - e)u.$$

Hence $eM + (1 - e)M = M$. Now suppose that $u \in eM \cap (1 - e)M$. Then there exist $v, w \in M$ such that

$$u = ev = (1 - e)w.$$

Thus

$$u = ev = e^2v = eu = e(1 - e)w = (e - e^2)w = (e - e)w = 0w = 0.$$

Hence $eM \cap (1 - e)M = \{0\}$. It follows that $M = eM \oplus (1 - e)M$.