Math146 - Review solutions for midterm 1

George McNinch

2025-02-19

I. The exam will cover what is (currently) in sections 1 - 7 of the course lecture notes.

II. You should be able to give careful statements for the definitions of the following terms:

Solution: I'm not going to write detailed solutions for these since I believe they can all be found in the lecture notes. If you can't locate a definition in the notes, let me know (e.g. by email).

a a *commutative ring* R, a *field* F, an *integral domain* R, a *ring homomorphism* $f : R \to S$, an *ideal* I of a commutative ring R,a *principal ideal* of a commutative ring R, a *principal ideal domain*, the *quotient ring* R/I where I is an ideal of a commutative ring,

b an *irreducible element* of a commutative ring R, the greatest common divisor $\gcd(a, b)$ for elements $a, b \in R$ of a principal ideal domain R, a *unit* of a commutative ring, an *associate* of an element of a commutative ring, a 0-divisor of a commutative ring R

c the *field of fractions* F of an integral domain R, the *polynomial ring* $R[T]$ for a commutative ring R

III. You should know the statements of the following results.

a. The *first isomorphism theorem for rings*

Solution: Let R and S be rings and let $\phi : R \to S$ be a *surjective* ring homomorphism. Then ϕ induces an isomorphism of rings $\overline{\phi} : R/K \to S$ where $K = \ker \phi$ is the kernel of ϕ. The mapping $\overline{\phi}$ is defined by $\overline{\phi}(r + K) = \phi(r)$ for $r \in R$.

b. the result that the *unique factorization property* holds in a PID

Solution: Let R be a PID and let $a \in R$ be non-zero and suppose that $a \notin R^\times$. Then

(i) There are irreducible elements $p_1, p_2, \cdots, p_n \in R$ such that $a = p_1 p_2 \cdots p_n$.

(ii) If $q_1, q_2, \cdots, q_m \in R$ are irreducibles and if $a = q_1 q_2 \cdots q_m$ then $n = m$ and – after possibly re-ordering the q_j – p_i and q_i are *associate* for $1 \le n$.

c. The *division algorithm* for the polynomial ring $F[T]$ where F is a field.

Solution: Let $f, g \in F[T]$ with $0 \neq g$. Then there are elements $q, r \in F[T]$ such that
(i) $f = qg + r$
(ii) $\deg r < \deg g$ (where we recall that $\deg 0 = -\infty$).

d. Eisenstein's irreducibility criterion

Solution: Let R be a PID with field of fractions F, let $p \in R$ be irreducible, and let $f \in R[T]$ be a polynomial of degree $n \geq 1$. Write $f = \sum_{i=0}^{n} a_i T^i$ with $a_i \in R$.
Assume the following:
(i) $p \nmid a_n$
(ii) $p \mid a_i$ for each $0 \leq i \leq n-1$
(iii) $p^2 \nmid a_0$.
Then f is irreducible in the polynomial ring $F[T]$.

e. the Gauss Lemma and consequences

Solution: Let R be a PID with field of fractions F. For $0 \neq f \in R$, let $\text{content}(f) \in R$ be the gcd of the coefficients of f.
The *Gauss Lemma* is the statement that $\text{content}(fg) = \text{content}(f) \cdot \text{content}(g)$ for non-zero polynomials $f, g \in R[T]$.
An important consquence is that if f is primitive – i.e. $\text{content}(f) = 1$ – and if $f = gh$ for $g, h \in F[T]$ then there are polynomials $g_0, h_0 \in R[T]$ such that $\deg(g) = \deg(g_0)$, $\deg(h) = \deg(h_0)$ and $f = g_0 h_0$.

IV. Be able to give examples of the following:

a. an *integral domain* that is not a *principal ideal domain*

Solution: The polynomial ring $F[T, S]$ in two variables is not a PID, since the ideal $\langle T, S \rangle$ is not principal.
(For a similar example, the polynomial ring $\mathbf{Z}[T]$ is not a PID, since the ideal $\langle 2, T \rangle$ is not principal.)

b. a field F and a polynomial $f \in F[T]$ such that f has no root in F but f is *reducible.*

Solution: Let $F = \mathbf{R}$ and let $f = (T^2+1)^2 = T^4 + 2T^2 + 1 \in \mathbf{R}[T]$. The roots of f in $\mathbf{C}$ are $\pm i$ (each with multiplicity two). Since these roots are not real, f has no roots in $\mathbf{R}$. But f is reducible in $\mathbf{R}[T]$ since $f = (T^2+1) \cdot (T^2+1)$ is the product of two polynomials each of degree 2.

c. A finite field F with exactly 9 elements. (**Hint:** Consider the field $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z}$ of order 3, and find a polynomial of the form $p = T^2 - a \in \mathbf{F}_3[T]$ that is *irreducible.* How many elements are in the quotient $F[T]/\langle p \rangle$?)

Solution: The squares of elements of $\mathbf{F}_3$ are $0 = 0^2, 1 = 1^2, 1 = 2^2$. Since 2 is not a square, the polynomial $T^2 - 2 \in \mathbf{F}_3[T]$ has no root in $\mathbf{F}_3$; since this polynomial has degree 2, we know it to be *irreducible.*

Now form the field $F = \mathbf{F}_3[T]/\langle T^2 - 2 \rangle$. Write $t = T + \langle T^2 - 2 \rangle \in F$. The division algorithm implies that every element of F may be written uniquely in the form $a + bt$ with $a, b \in \mathbf{F}_3$. Put another way, we know that $1, t$ is a basis for the $\mathbf{F}_3$-vector space F.

In the expression $a + bt$ there are 3 choices for a and 3 choices for b; thus there are precisely $3 \times 3 = 9$ elements in F.

V. You should be able to write careful solutions to problems similar to the following:

1. Let F be a field and let $f, g \in F[T]$ be polynomials for which $\gcd(f, g) = 1$. Consider the mapping

$$\phi : F[T] \to F[T]/\langle f \rangle \times F[T]/\langle g \rangle$$

given by the rule $\phi(h) = (h + \langle f \rangle, h + \langle g \rangle)$.

a. Show that $\ker \phi = \langle fg \rangle$ and that ϕ induces an isomorphism

$$\overline{\phi} : F[T]/\langle fg \rangle \xrightarrow{\sim} F[T]/\langle f \rangle \times F[T]/\langle g \rangle$$

Solution: Let $K = \ker \phi$. Clearly $fg \in K$ since

$$\phi(fg) = (fg + \langle f \rangle, fg + \langle g \rangle) = (0, 0).$$

To prove that $K = \langle fg \rangle$, suppose that $h \in K = \ker \phi$. We know see that

$$0 = \phi(h) = (h + \langle f \rangle, h + \langle g \rangle),$$

so we conclude that $f \mid h$ and $g \mid h$. Let's write $h = fx$ for a polynomial $x \in F[T]$.

We need to argue that $g \mid x$; indeed, if we show that $x = gy$ then $h = fx = fgy$ so that $h \in \langle fg \rangle$ as required.

Since $\gcd(f, g) = 1$ we know that $1 = af + bg$ for polynomials $a, b \in F[T]$. We now notice that

$$x = x \cdot 1 = x \cdot (af + bg) = xaf + xbg = ah + xbg;$$

since $g \mid ah$ and $g \mid xbg$, it follows that $g \mid x$ as required. This completes the proof that $\ker \phi = \langle fg \rangle$.

Now the first isomorphism theorem implies that ϕ induces an isomorphism from $F[T]/\langle fg \rangle$ to the image of ϕ, so to finish the proof we need to argue that ϕ is surjective. Since $1 = af + bg$ we know that

$$bg \equiv 1 \pmod{f}$$

and

$$af \equiv 1 \pmod g$$

Thus $\phi(bg) = (1 + \langle f \rangle, 0)$ and $\phi(af) = (0, 1 + \langle g \rangle)$.
It is now easy to see that ϕ is surjective. Indeed, let

$$(s + \langle f \rangle, t + \langle g \rangle) \in F[T]/\langle f \rangle \times F[T]/\langle g \rangle$$

be an arbitrary element. Then

$$\phi(sbg + taf) = (s + \langle f \rangle, 0) + (0, t + \langle g \rangle) = (s + \langle f \rangle, t + \langle g \rangle)$$

which confirms that ϕ is surjective.

b. As a consequence, show that $\mathbf{Q}[T]/\langle T^7 - 1 \rangle$ is isomorphic to the direct product of two fields.

Solution: Set $f = T^6 + T^5 + T^4 + T^3 + T^2 + T + 1 = \dfrac{T^7 - 1}{T - 1}$; since 7 is prime, we have seen that $f \in \mathbf{Q}[T]$ is *irreducible.*
Now, $T^7 - 1 = f(T - 1)$. Since f and $T - 1$ are non-associate irreducible polynomials, we know that $\gcd(f, T - 1) = 1$.
Now part (a) shows that

$$\mathbf{Q}[T]/\langle T^7 - 1 \rangle \simeq \mathbf{Q}[T]/\langle f \rangle \times \mathbf{Q}[T]/\langle T - 1 \rangle \simeq \mathbf{Q}[T]/\langle f \rangle \times \mathbf{Q} \quad (\clubsuit).$$

Since f is irreducible, $\mathbf{Q}[T]/\langle f \rangle$ is a field, and thus wee see that $(\clubsuit)$ is the direct product of two fields.

2. Let R be a PID, let $a_1, a_2, \cdots, a_n \in R$ not all 0, and let $d = \gcd(a_1, a_2, \cdots, a_n)$. Note that $\dfrac{a_i}{d} \in R$ for each i. Prove that $\gcd\left(\dfrac{a_1}{d}, \dfrac{a_2}{d}, \cdots, \dfrac{a_n}{d}\right) = 1$

Solution: We know that there are elements $x_i \in R$ for which

$$d = \gcd(a_1, a_2, \cdots, a_n) = \sum_{i=1}^{n} x_i a_i (\heartsuit).$$

Since d is a gcd of the a_i, it is in particular a divisor of each a_i; thus for each $1 \le i \le n$ we may write $a_i = db_i$ for elements $b_i = \dfrac{a_i}{d} \in R$.
Thus we may rewrite $(\heartsuit)$ in the form

$$d \cdot 1 = \sum_{i=1}^{n} x_i d b_i = d \sum_{i=1}^{n} x_i b_i.$$

Now, cancellation in the integral domain R implies that

$$1 = \sum_{i=1}^{n} x_i b_i.$$

This shows that $1 \in \langle b_1, b_2, \cdots, b_n\rangle$ so that

$$R = \langle 1\rangle \subseteq \langle b_1, b_2, \cdots, b_n\rangle.$$

Thus $R = \langle 1\rangle = \langle b_1, b_2, \cdots, b_n\rangle$ (since the reverse inclusion $\langle b_1, b_2, \cdots, b_n\rangle \subseteq R$ trivially holds) and it follows that $\gcd(b_1, b_2, \cdots, b_n) = 1$ as required.

3. Show that $u = 2 + T + \langle T^3\rangle$ is a unit in the quotient ring $\mathbf{Q}[T]/\langle T^3\rangle$.

Solution: Write $R = \mathbf{Q}[T]/\langle T^3\rangle$ and let $x = T + \langle T^3\rangle \in R$. Thus we are asked to show that $u = 2 + x$ is a unit.
We first observe that $x^3 = T^3 + \langle T^3\rangle = 0$ in R.
Now, notice

$$u(2 - x) = (2 + x)(2 - x) = 4 - x^2$$

Similarly,

$$(4 - x^2)(4 + x^2) = 16 - x^4 = 16$$

It follows that $u \cdot \frac{1}{16}(2 - x)(4 + x^2) = 1$ so that $v = \frac{1}{16}(2 - x)(4 + x^2) \in R$ is a multiplicative inverse for u. Thus $u \in R^\times$ as required.
One can of course check/observe that v may be "simplified" as

$$v = \frac{8 - 4x + 2x^2}{16} = \frac{4 - 2x + x^2}{8}$$

4. Let F be a field. Prove that $\sqrt{T}$ is not in $F(T)$. (**Hint:** Suppose the contrary, namely that $\sqrt{T} = \frac{f}{g}$ for $f, g \in F[T]$. Explain why we find an equation $g^2T = f^2$ in $F[T]$. Now apply unique factorization in the PID to deduce a contradiction).

Solution: Suppose as in the hint that $\sqrt{T} = \frac{f}{g}$ for $f, g \in F[T]$. Thus $g^2T = f^2 \quad (\diamondsuit)$
Using unique factorization, we may write $g = p_1p_2\cdots p_m$ and $f = q_1q_2\cdots q_n$ for irreducible polynomials $p_i, q_j \in F[T]$.
Thus by $(\diamondsuit)$ we have the equation

$$p_1^2p_2^2\cdots p_m^2 \cdot T = q_1^2q_2^2\cdots q_m^2$$

in R. The irreducible element $T \in F[T]$ appears on the LHS of this equation with odd multiplicity, while every irreducible on the RHS appears with even multiplicity. According to unique factorization in the polynomial ring $F[T]$ we know this to be impossible; this contradiction proves that $\sqrt{T} \notin F(T)$.

5. If R is a PID and $p, q \in R$ are non-associate irreducible elements, compute $\gcd(p^2q, pq^2)$?

Solution: We claim that $\gcd(p^2q, pq^2) = pq$.

Well, pq is a divisor of p^2q and of pq^2 so it is a common divisor. Suppose that e is any common divisor of p^2q and pq^2. Unique factorization shows that the only possible irreducible factors are p and q. Since $e \mid p^2q$, the multiplicity of q in e can be at most 1; since $e \mid pq^2$, the multiplicity of p in e can be at most 1. This shows that $e \mid pq$. Thus indeed pq is the required gcd.

6. Consider the field $\mathbf{F}_5$ with 5 elements.
   - Prove that $T^2 - 3 \in \mathbf{F}_5[T]$ is irreducible.

   Solution: The squares in $\mathbf{F}_5$ are $0 = 0^2, 1 = 1^2, 4 = 2^2, 4 = 3^2, 1 = 4^2$. Since 3 is not a square in $\mathbf{F}_5$, the polynomial $T^2 - 3$ has no root in $\mathbf{F}_5$. Since this polynomial has degree 2 and no root, we deduce that $T^2 - 3$ is irreducible in $\mathbf{F}_5[T]$.

   - Let $\gamma = T + \langle T^2 - 3 \rangle \in \mathbf{F}_5[T]/\langle T^2 - 3 \rangle$; thus $\mathbf{F}_5(\gamma) = \mathbf{F}_5[T]/\langle T^2 - 3 \rangle$. Find $s, t \in \mathbf{F}_5$ so that $(s + t\gamma) \cdot (1 + \gamma) = 1$.

   Solution: We calculate, using the fact that $\gamma^2 = 3$:

$$\begin{aligned}(s + t\gamma)(1 + \gamma) &= s + s\gamma + t\gamma + t\gamma^2 \\ &= (s + 3t) + (s + t)\gamma\end{aligned}$$

   Thus we need to solve the system of linear equations

$$\begin{cases} s + 3t &= 1 \\ s + t &= 0 \end{cases}$$

   or the equivalent of matrix equation

$$(\dagger) \quad \begin{bmatrix} 1 & 3 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} s \\ t \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

   We notice that $A = \begin{bmatrix} 1 & 3 \\ 1 & 1 \end{bmatrix}$ has determinant $\det A = 1 - 3 = -2 = 3 \in \mathbf{F}_5$. Thus

$$A^{-1} = \frac{1}{3} \begin{bmatrix} 1 & -3 \\ -1 & 1 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 1 & 2 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 3 & 2 \end{bmatrix}$$

   The solution to $(\dagger)$ is therefore given by

$$\begin{bmatrix} s \\ t \end{bmatrix} = A^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$$

   In other words $\dfrac{1}{1 + \gamma} = 2 + 3\gamma$ in $\mathbf{F}_5(\gamma)$

7. Be able to give the proof of the following results (taken from the notes).

   Let R be a PID and let $p \in R$ irreducible.

- If $p \mid ab$ for $a, b \in R$ then $p \mid a$ or $p \mid b$.

  Solution: This is Proposition 5.1.3 in the lecture notes.

- The quotient ring $R/\langle p \rangle$ is a field.

  Solution: This is Proposition 7.1.1 in the lecture notes.