Algebra II Homework 4 Commentary

Zachary Gardner

Problem 1

(a) A subtle but important point here is that invariant factors are **required** to be monic. If we were to remove this requirement then rational canonical form would not be unique and it would be possible for a degree 1 polynomial to divide another degree 1 polynomial with a different constant coefficient.

(b) Even though $\mathbb{Z}/n\mathbb{Z}$ is not a PID it is true that every ideal is principal. In fact, every quotient of a PID has this property (can you see why?).

(c) The key to prime elements in a general commutative ring R not being irreducible is the presence of (nonzero) zero divisors. We can rule this out by requiring R to be an integral domain.

(d) The only way to get full points for this one is to give an explicit counterexample. Note that it's not immediately obvious that the union of two ideals is an ideal if and only if one ideal contains the other (though it is true!).

Problem 2

- Checking commutativity under addition is overkill since this is automatic from the ring structure of R.
- The problem does not specify that R is commutative but it's fine if you assumed this. Regardless, the result remains true for non-commutative R as we long as we specify that each ideal in the chain is a left, right, or two-sided ideal.
- Once you are closed under addition and scaling by R then you are automatically closed under subtraction and contain 0 (be sure to distinguish between the additive and multiplicative identity).
- It is not true that a finite union of ideals is an ideal (hence the same is true for infinite unions).
- It is true that a finite union of a chain of ideals is an ideal, since the union is just the ideal at the end of the chain.
- Induction does not allow us to deduce that an infinite union of a chain of ideals is an ideal from the finite case. The problem is that a chain of arbitrarily large finite length is not the same thing as a chain of infinite length.

Problem 3

Don't forget about the zero matrix! Rational canonical form is something that only works for nonzero matrices.

Problem 4

Part (a)

- This is not just trivial! The key is proving that if $a(x), b(x) \in k[x]$ with $a(x) \mid b(x)$ in $L[x]$ then $a(x) \mid b(x)$ in $k[x]$. We will sketch two proofs of this for clarity.
- Here's the first proof. By assumption we have $b(x) = a(x)p(x)$ for some $p(x) \in L[x]$ (crucially this may not a priori be an element of $k[x]$). Using the division algorithm for $k[x]$ we may choose $q(x), r(x) \in k[x]$ such that $\deg r(x) < \deg a(x)$ and $b(x) = a(x)q(x) + r(x)$. Then, $r(x) = a(x)(p(x) - q(x))$ and the degree condition forces $p(x) - q(x) = 0 \implies p(x) = q(x)$.
- Here's the second proof. Once again by assumption we have $b(x) = a(x)p(x)$ for some $p(x) \in L[x]$. We may write

  $$\begin{aligned} a(x) &= \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0 \in k[x] \\ p(x) &= \beta_m x^m + \beta_{m-1} x^{m-1} + \cdots + \beta_0 \in L[x] \\ b(x) &= \gamma_{m+n} x^{m+n} + \gamma_{m+n-1} x^{m+n-1} + \cdots + \gamma_0 \in k[x]. \end{aligned}$$

  We then have

  $$\begin{aligned} &\gamma_0 = \alpha_0\beta_0 \implies \beta_0 = \alpha_0^{-1}\gamma_0 \in k \\ &\gamma_1 = \alpha_0\beta_1 + \alpha_1\beta_0 \implies \beta_1 = \alpha_0^{-1}(\gamma_1 - \alpha_1\beta_0) \in k \\ &\vdots \end{aligned}$$

  and so we see by induction that $p(x) \in k[x]$. There is of course a slight difficulty if $\alpha_0 = 0$ but this can be dealt with without too much work by writing $a(x) = x^v a'(x)$ for $v > 0$ sufficiently large and $a'(x)$ having nonzero constant coefficient.
- An abstract way of viewing all of this is that the inclusion map $k[x] \hookrightarrow L[x]$ induces a well-defined injective homomorphism $k[x]/(a(x)) \hookrightarrow L[x]/(a(x))$.

Parts (b) and (c)

- For part (b), one way of viewing things is in terms of the function $\mathrm{RCF}_F : M_n(F) \to M_n(F)$ that takes a matrix defined over F to its rational canonical form. For $k \subseteq L$ a field extension, the statement of part (b) is equivalent to the statement that RCF_k is the restriction of RCF_L to $M_n(k) \subseteq M_n(L)$.
- For part (c) stuff with rational canonical form technically doesn't cover the case of the zero matrix (but this is easily dealt with).

Problem 5

Part (b) $\implies$ Part (c)

You still need to provide some explanation even though the hint says this is trivial. Mentioning the factoring triangle is sufficient. In general, the rule of thumb for hints on problem sets is that they are sketchy on purpose and so you should justify whatever claims are made in the hint.

Part (c) $\implies$ Part (a)

The main point is to note that there is some subtlety when generalizing from the $n = 2$ to the $n > 2$ case. Letting

$$\varphi : R \twoheadrightarrow R/I_1 \times \cdots \times R/I_n, \qquad r \mapsto (r + I_1, \dots, r + I_n),$$

suppose we choose $r_1, \dots, r_n \in R$ such that

$$\varphi(r_1) + (1 + I_1, I_2, \dots, I_n), \dots, \varphi(r_n) = (I_1, I_2, \dots, 1 + I_n).$$

Then, $r := r_1 + \cdots + r_n$ satisfies

$$\varphi(r - 1) = 0 \implies r - 1 \in \ker \varphi = \bigcap_{i=1}^{n} I_i$$

and so we have $r + a = 1$ for some a contained in every I_i. By construction we have $r_i \in \bigcap_{j \neq i} I_j$ and so for $i \neq j$ we have

$$\underbrace{\textstyle\sum_{k \neq i} r_k}_{\in I_i} + \underbrace{(r_i + a)}_{\in I_j} = r + a = 1.$$

This shows that I_i, I_j are relatively prime. The end result can be checked more simply by considering each r_i separately, but the advantage of the above approach is that we *uniformly* get coprime elements that work for all $i \neq j$. This is a stronger result.

Problem 6

- Not that the k-pairs $V_x \times V_x$ and V_{x^2} are **not** isomorphic as k-pairs even though they are isomorphic as k-vector spaces (since both have dimension 2 over k). This is because multiplication by x is the zero map on V_x (hence induces the zero map on $V_x \times V_x$) but not on V_{x^2}.
- In line with the above comment, it's worth unpacking precisely what the problem statement means. The problem asks us to prove that every k-pair is isomorphic to

  $$k[x]/(q_1(x)^{r_1}) \times \cdots \times k[x]/(q_t(x)^{r_t}) \tag{1}$$

  for $q_1(x), \dots, q_t(x) \in k[x]$ monic irreducible and $r_1, \dots, r_t \in \mathbb{Z}^{\geq 1}$ such that the set

  $$\{q_1(x)^{r_1}, \dots, q_t(x)^{r_t}\}$$

  is unique up to permutation. Here, set should be understood to mean multi-set – i.e., we allow duplicate entries. This way $k[x]/(x) \times k[x]/(x)$ is a valid k-pair distinct from both $k[x]/(x)$ and $k[x]/(x^2)$.

- Suppose that $f_1(x) \mid \cdots \mid f_m(x)$ are the invariant factors of a given k-pair. Then, the polynomials $f_i(x)$ and $f_j(x)$ are **not** relatively prime since one divides the other by construction. For the same reason it is common for at least one invariant factor to not be irreducible. Indeed, if invariant factors were always irreducible then over $\mathbb{C}$ minimal polynomials could only be linear (degree 1)!
- Proving uniqueness of the expression in (1) requires both uniqueness of invariant factors **and** uniqueness of prime factorization for non-constant polynomials in $k[x]$. The Chinese Remainder Theorem (CRT for short) tells us how to connect the two, giving us a way to "collapse down" and "expand" k-pairs.
- This problem shows that we have a well-defined and unique elementary divisor decomposition for k-pairs. This is closely related to but not the same as the invariant factor decomposition, which itself exists and is unique. Note that the invariant factor decomposition is a special case of the so-called Smith normal form (which is defined even for non-square matrices).

Problems 7 and 8

- Be careful to distinguish between rational canonical form and Jordan canonical form. In particular, take heed that every diagonal matrix is in Jordan canonical form but diagonal matrices are rarely in rational canonical form (this only happens if all diagonal entries are the same).
- Some people worked with minimal and characteristic polynomials using different definitions than the ones given on this problem set. For us, the minimal polynomial is defined to be the largest invariant factor while the characteristic polynomial is defined to be the product of all of the invariant factors. For a perhaps more familiar perspective on these notions look at Problems 4 and 5 on Homework 5.
- Problem 7 can be proven using Problem 8.
- Some students misinterpreted the statement of Homework 3 Problem 6, which says that a matrix $A \in M_n(k)$ is diagonalizable if and only if there is an isomorphism of k-pairs $V_A \cong V_{x-\alpha_1} \times \cdots \times V_{x-\alpha_n}$ for some $\alpha_1, \ldots, \alpha_n \in k$. The key here is that the scalars α_i don't have to be distinct. This is because diagonal matrices can have repeated diagonal entries (which correspond to eigenvalues with algebraic multiplicity greater than 1).
- Let's say $A \in M_n(k)$ is diagonalizable, so $V_A \cong V_{x-\alpha_1} \times \cdots \times V_{x-\alpha_n}$ for some $\alpha_1, \ldots, \alpha_n \in k$. By regrouping as necessary we get

  $$V_A \cong V_{x-\lambda_1}^{c_1} \times \cdots \times V_{x-\lambda_r}^{c_r}$$

  for $\lambda_1, \ldots, \lambda_r \in k$ **distinct** and $c_1, \ldots, c_r \in \mathbb{Z}^{\geq 1}$. Using the argument of Problem 6 we get from this $\min_A(x) = (x-\lambda_1)^{e_1} \cdots (x-\lambda_r)^{e_r}$ for some $e_1, \ldots, e_r \in \mathbb{Z}^{\geq 1}$. How do we know each $e_i = 1$? While it's certainly true that $\min_A(x)$ divides the characteristic polynomial $\mathrm{ch}_A(x) = (x-\lambda_1)^{c_1} \cdots (x-\lambda_r)^{c_r}$, the latter may not be square-free and so we need to work a little harder. The key is that $V_{\min_A(x)}$ must appear as a product factor of V_A by virtue of the invariant factor decomposition. Having some $e_i > 1$ would violate the uniqueness part of Problem 6 since $V_{(x-\lambda_i)^{e_i}}$ and $V_{x-\lambda_i}^{e_i}$ are not isomorphic as k-pairs.

Problem 9

- Remember that you can't divide by 0 in the division algorithm. This is a missing condition in the definition of norm given on this problem set.
- Note that the usual division algorithm for $\mathbb{Z}$ you are probably familiar with only deals with positive integers. I was looking for some justification as to why the general (potentially negative) case follows from the positive case.
- The word "norm" is unfortunately one of those math words that has a thousand different meanings. We don't require a Euclidean norm to satisfy the triangle inequality.
- The degree-sum formula $\deg(fg) = \deg(f) + \deg(g)$ does work for all $f, g \in k[x]$ (even 0) under the conventions that $\deg(0) = -\infty$ and $-\infty + a = -\infty$ for every $a \in \mathbb{Z}$.
- Some people lost points for failing to give some explanation for why the division algorithm works for $k[x]$. Saying to "just do polynomial long-division" won't work since that's just another name for the division algorithm. Note that a choice of remainder won't be unique unless you specify that it has to be monic.
- The well-ordering principle (affectionately termed WOP) is the statement that any nonempty set of positive integers has a least element. This is useful for proving any division algorithm, whether for $\mathbb{Z}$, $k[x]$, or $\mathbb{Z}[i]$.
- One subtle point that makes the division algorithm work for $\mathbb{Z}[i]$ is the fact that the function $N : \mathbb{Z}[i] \to \mathbb{Z}^{\geq 0}$ given by $a + bi \mapsto a^2 + b^2$ extends to a function $N : \mathbb{C} \to \mathbb{Z}^{\geq 0}$ such that $N(\alpha) = 0 \iff \alpha = 0$ and $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{C}$.
- There are several ways to view the geometry of this problem. Keerthi's solution thinks about how far a point inside the unit square can be from one of the corners. Another way to think about the problem is to note that the square root of $N : \mathbb{C} \to \mathbb{Z}^{\geq 0}$ gives us the Euclidean distance function if we think of $\mathbb{C}$ as $\mathbb{R}^2$. More specifically, the distance between points (a, b) and (c, d) in $\mathbb{R}^2$ is

  $$\sqrt{(a-c)^2 + (b-d)^2} = \sqrt{N((a+bi) - (c+di))}.$$

  Given $\beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, the ideal $\beta\mathbb{Z}[i]$ forms a lattice in $\mathbb{C}$ if we once again view $\mathbb{C}$ as $\mathbb{R}^2$. Geometrically, the division algorithm says that, given any point α on the square lattice $\mathbb{Z}[i]$, we can find a point βq on the lattice $\beta\mathbb{Z}[i]$ such that α is contained within the disc of radius $\sqrt{N(\alpha)}$ centered at βq.
- Summarizing the above, the division algorithm for $\mathbb{Z}[i]$ allows us to cover the lattice $\mathbb{Z}[i]$ by circular discs centered at points of some smaller lattice. One could imagine trying to do something similar for $\mathbb{Z}[\sqrt{d}]$ with $d \in \mathbb{Z}$ square-free. It turns out then that the picture involves trying to cover points of a lattice by elliptical discs or even the interiors of hyperbolae. This is a simple manifestation of something called the geometry of numbers or Minkowski theory.

Problem 10

- It's important to state things clearly! For example, "Let a be an element in I with minimal positive norm." Symbolically this can be written as $\min\{N(i) \neq 0 : i \in I\}$. You should not define this as $\min\{N(i) : 0 \neq i \in I\}$ even though the two are technically equal by the first property of Euclidean norms. Along the same line, note that we automatically have $a \neq 0$ and so we can actually perform the division algorithm with respect to a.

- When doing division with respect to a and getting a remainder $r \in I$ with $N(r) < N(a)$, the right way to go is not to say $N(r) \geq N(a)$ and call contradiction. Instead, since $N(a)$ is minimal positive we must have $N(r) = 0$ which in turns forces $r = 0$.