Math 490A—Fall 2019
Review Sheet for Final Exam

December 8, 2019

The final exam will be given as a take-home. I expect to make it available on the course website on the last day of classes, Wednesday, December 11. It will be due at the end of the final exam period scheduled for the course, 12:30 pm on Wednesday, December 18. For the take-home exam, you are allowed to use the textbook and notes, handouts, and solutions from the class. You can consult me about questions, but you are not to use any other sources. That includes textbooks, the internet, or other people. I will schedule a few office hours during the week you have to work on the exam, but you can also send me email if you have a question or want to set up a meeting.

You should be able to use the axioms, definitions, and results from the textbook and class in answering questions and doing proofs. I won’t ask you to state definitions or theorems (since you have access to the book), but I may ask you to explain the connection between two definitions or two versions of a theorem (e.g., Bézout’s theorem in different settings). You should be able to use most of the techniques used in proofs from the textbook. The homework is a good general guide to the kind of problems you’ll see. So make sure you have gone through the posted solutions to homework problems.

For proofs, you can use results from the book, homework problems, or discussion in class, but you need to cite those results. You don’t need to cite theorems by the number in the book (though you can, since you’ll have access to the book), but you should at least say “A theorem in the book says that . . . ” or something like that which makes it clear exactly what result your referring to.

In addition to the homework (and solutions), I think it will be very helpful for you to go through the handouts on “Key Ideas” I’ve put on the web page. But here’s a brief discussion about the topics since the midterm exam (though the fact that something is listed here doesn’t mean it will necessarily be on the exam and the fact that something isn’t mentioned here doesn’t mean it won’t be on the exam). Note that the material is fairly cumulative, so an exam question that involves a topic we considered recently might also test you on your understanding of earlier material. You should also go over the review sheet for the midterm exam for a discussion of what you are expected to know about that material.
**Chapter 11:** Chapter 11 studies the irreducibility of polynomials in $\mathbb{Q}[x]$. The key ideas are the connection between irreducibility in $\mathbb{Q}[x]$ and factorization in $\mathbb{Z}[x]$. Of course, you can multiply any polynomial $f(x)$ in $\mathbb{Q}[x]$ by a nonzero integer $d$ (e.g., the lcm of the denominators of the coefficients) to get a polynomial in $\mathbb{Z}[x]$. From the standpoint of $\mathbb{Q}[x]$, you’ve multiplied the polynomial by a unit and so haven’t made any significant change in its factorization properties. But in $\mathbb{Z}[x]$, the only units are 1 and $-1$ and multiplying by some $d \neq \pm 1$ gives a new polynomial $df(x)$ that’s definitely not irreducible in $\mathbb{Z}[x]$ (unless $f(x) = \pm 1$), since $df(x)$ is a nontrivial factorization. So to study irreducibility in $\mathbb{Q}[x]$ in terms of $\mathbb{Z}[x]$, we need to look at polynomials that can’t be factored into products of lower-degree polynomials, and we need to work with primitive polynomials and use Gauss’s Lemma to control factorizations that involve common factors of the coefficients. But then we can prove that a polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if it’s irreducible in $\mathbb{Q}[x]$. (It’s this result that tells us, for instance, that if a polynomial with integer coefficients has roots in $\mathbb{Q}$, those roots are actually in $\mathbb{Z}$ and so must divide the constant term in $\mathbb{Z}$.)

**Chapter 12:** Chapter 12 proves the analog of the Fundamental Arithmetic for polynomial rings over a field. The key thing you should observe is that, replacing absolute value as the notion of “size” for integers (in the division theorem) with degree for polynomials, not only the theorems but also their proofs carry over to this new setting. We do change our terminology a bit and talk about irreducible polynomials instead of primes, but that’s partly because the school mathematics definition of a prime in terms of factorization is really the definition of irreducible in a general ring. In rings like $\mathbb{Z}$ and $K[x]$, primes (in the sense of Euclid’s lemma about dividing a product) and irreducibles (in the sense of not having any nontrivial factorizations) are the same elements; an element has one property if and only if it has the other property. So you should go back through Chapter 12 and Chapters 3 and 5 and make sure that the parallels are clear to you. The results in this chapter are key to understanding how factorization works in polynomial rings.

**Chapter 13 and Chapter 14:** Chapters 13 and 14 consider an irreducible polynomial $m(x) \in F[x]$ for some field $F$ (typically $\mathbb{Q}$ or some $\mathbb{F}_p$ in the examples, but that’s not really critical). If $m(x)$ has degree greater than 1, it doesn’t have any roots in $F$ and, to study the roots, we need to go to a larger field. So the problem is how to construct this larger field. These two chapters give two
approaches that end up doing the same thing.

One approach is to simply create a symbol $\gamma$ representing a root of $m(x)$ and take $F$-linear combinations of powers of $\gamma$ ("polynomial-like expressions in $\gamma$). Then we use the fact that $\gamma$ is supposed to be a solution to $m(x) = 0$ to (a) show that we only need to consider powers of $\gamma$ up to $\deg m(x) - 1$, and (b) properly define a multiplication on these linear combinations. (In particular, if $m(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1x - a_0$, then we have $\gamma^n = a_{n-1}\gamma^{n-1} + \cdots + a_1\gamma + a_0$) and we can use this as a "rewrite rule" to convert any linear combination of powers of $\gamma$ to one that only involves powers up to $n - 1$. We then use ad hoc techniques to show that the set $K$ of these linear combinations of $\gamma$ is a field containing (a copy of) $F$ and a root ($\gamma$) of $m(x)$. This approach is concrete and is essentially what we do when we create $\mathbb{C}$ from $\mathbb{R}$ by introducing a symbol $i$ for a root of the irreducible polynomial $x^2 + 1$, so it’s at least somewhat familiar.

So you can regard most of Chapter 13 and the first section of Chapter 14 as exploring different examples of this approach.

The second approach is to look at $F[x]_{m(x)}$, the set of congruence classes of polynomials in $F[x]$ modulo the irreducible polynomial $m(x)$, where congruence is the exact analog of what it meant for $\mathbb{Z}$: two polynomials in $F[x]$ are congruent modulo $m(x)$ if and only if their difference is a multiple of $m(x)$. We show that $F[x]_{m(x)}$ is a ring with operations coming from the operations of $F[x]$ just as we showed $\mathbb{Z}_m$ is a ring: to add two congruence classes in $F[x]_{m(x)}$, for instance, we take one polynomial from each congruence class, add those polynomials in $F[x]$ and take the congruence class of this sum, and similarly for multiplication. (As for $\mathbb{Z}_m$, we have to show that these operations are well-defined, meaning that you end up with the same congruence class for the sum/product no matter which polynomials you choose from the classes you start with.) We show that each congruence class contains exactly one element of degree less than $n = \deg m(x)$, and that the units in $F[x]_{m(x)}$ are just the classes that contain polynomials of degree 0, so we end up with (a copy of) $F$ living in $F[x]_{m(x)}$. Next, we show that the fact that $m(x)$ is irreducible makes $F[x]_{m(x)}$ a field. In this field, $[m(x)]_{m(x)} = 0$, so $[x]_{m(x)}$ is a root of $m(x)$.

We went through the properties of $\mathbb{Z}_m$ pretty quickly, since you should all have seen this in Math 300 or the equivalent. But it would probably be helpful to look back through the book’s discussion of congruences in Chapter 4 (which we didn’t really cover in class) and congruence rings in Chapter 6 (which we did quickly) to see that the construction of the ring $F[x]_{m(x)}$ is an exact parallel with the construction of $\mathbb{Z}_m$ and that the proof that $F[x]_{m(x)}$ is a field when $m(x)$ is irreducible is an exact parallel to the proof that that $\mathbb{Z}_m$ is a field when $m$ is a prime (which is the same as being irreducible in $\mathbb{Z}$).

At the end of the discussion, the book asks you to show that the two approaches to constructing a field extension of $F$ in which $m(x)$ has a root give the same thing, just writing $\gamma$ for $[x]_{m(x)}$ in $F[x]_{m(x)}$. (Showing that the multiplications really match is up is technically a little tricky, given the machinery we have in hand, but it’s pretty straightforward to see how the basic idea works.) As we discussed in class on Thursday, the idea of starting with the concrete construction with the symbol $\gamma$ sounds good, but maybe it’s not really so helpful in
practice, and I think if I teach this course again, I might skip the first approach and just go through the second approach more carefully, filling in a bit more of the details in class. So it’s ok if you focus more on the second approach.

One really important thing to take away from this construction is the following. Suppose $E$ is a field containing $F$ and $\alpha$ is an element of $E$ that is algebraic over $F$. (Recall that this means that $\alpha$ is a root of some polynomial $m(x) \in F[x]$, and we can assume without loss of generality that $m(x)$ is irreducible.) Then the smallest field that contains both $F$ and the element $\alpha$ consists of the set of $F$-linear combinations of the powers of $\alpha$ up to (but not including) the degree of $m(x)$. (These are the “polynomial-like expressions in $\alpha$”). So by taking $\alpha$ and its positive powers, we actually get the multiplicative inverse of $\alpha$ and all its powers (together with all the combinations of the powers and elements of $F$ using addition and multiplication). So we get all the positive and negative powers of $\alpha$ “for free” from the positive powers up to the degree of $m(x)$. This is not true if we take an element $\beta$ of $E$ that is transcendental (not algebraic) over $F$: taking all the $F$-linear combinations of positive powers of $\beta$ does not give us, for instance, a multiplicative inverse of $\beta$, and the polynomial-like (or just polynomial) expressions in $\beta$ do not form a field. So we can find a field containing $\mathbb{Q}$ and, say $\sqrt[14]{-3}$ pretty easily, but describing the smallest field containing $\mathbb{Q}$ and $\pi$ is much more complicated.

**Compass and straightedge constructions and solvability by radicals:**

This material was really just for your general edification as students and teachers of algebra and I won’t expect you to do anything with it on the final exam. You should take away a couple of insights from the stuff on compass and straightedge constructions. One is that it gives a significant example of the connectedness of mathematics and the fact that ideas from one part of mathematics are often needed to solve problems in another, apparently unconnected, part. These are geometry problems but we solve them by translating them into algebra problems, describing the points that we can construct with compass and straightedge in terms of a specific kind of field extension whose dimension is a power of 2. The other is an illustration of the power of these ideas of field extensions constructed using roots of polynomials.

Obviously, presenting the full details of the theorem about solvability by radicals would require developing a lot more mathematical machinery, about groups and solvable groups (and even defining solvability for groups depends on some deep ideas about special kinds of subgroups, etc.), the elementary symmetric functions, and so on. So I certainly don’t expect you to have really “understood” that theorem from the presentation I gave in class. But you at least have an idea of some of the ingredients that go into it, and can see how it involves almost all the ideas we’ve discussed in the course: factorization and irreducibility of polynomials, building a field where an irreducible polynomial has a root, and so on. And I hope that having an idea of what’s involved in that theorem (and maybe seeing one specific, not very complicated polynomial that’s not solvable by radicals) enriches your view of solving polynomials and
“algebra” in general, and, through that, on how you’ll teach those things.