Math 490A—Fall 2019
Solutions for Homework due October 8

Exercise 9.6: Prove Theorem 9.4. (Theorem 9.4 says that the ring $K[x]$ of polynomials with coefficients in a field $K$ contains infinitely many irreducible monic polynomials.) You can proceed according to the following outline:

1. Show that $K[x]$ has at least one irreducible monic polynomial. You can do so by exhibiting a specific one.
   Consider the polynomial $x$. To see that it’s irreducible, suppose $f(x)g(x)$ is a factorization of $x$ in $K[x]$. Since $x$ has degree 1, we see that $\deg f(x) + \deg g(x) = 1$, so one of $f(x)$ and $g(x)$ must have degree 0 and hence be a unit. Thus, any factorization of $x$ in $K[x]$ must be trivial. \(\square\)
   (You can take your favorite monic polynomial of degree 1, if you want a different example. Exactly the same argument applies.)

2. We are going to suppose that $K[x]$ has only finitely many irreducible monic polynomials and arrive at a contradiction. Suppose that the distinct polynomials $p_1(x), \ldots, p_k(x)$ make up the entire set of irreducible monic polynomials in $K[x]$.
   OK, suppose that the distinct polynomials $p_1(x), \ldots, p_k(x)$ make up the entire set of irreducible monic polynomials in $K[x]$.

3. Show that none of $p_1(x), \ldots, p_k(x)$ can divide the polynomial $(p_1(x)\cdots p_k(x)) + 1$.
   Suppose $p_i(x)$ divides $f(x) = (p_1(x)\cdots p_k(x)) + 1$, so there is a $g(x)$ such that $p_i(x)g(x) = f(x)$ and we have
   \[
   p_i(x)g(x) = (p_1(x)\cdots p_k(x)) + 1
   = p_i(x)(p_1(x)\cdots p_{i-1}(x)p_{i+1}(x)\cdots p_k(x)) + 1.
   \]
   Then
   \[
   p_i(x)(g(x) - (p_1(x)\cdots p_{i-1}(x)p_{i+1}(x)\cdots p_k(x))) = 1
   \]
   so $p_i(x)$ divides 1. But this says that $p_i(x)$ is a unit (it divides 1), so it’s not irreducible.

4. Observe that $(p_1(x)\cdots p_k(x)) + 1$ has some monic polynomial $p(x)$ in $K[x]$ as a divisor, and that therefore there is a monic irreducible polynomial in $K[x]$ distinct from $p_1(x), \ldots, p_k(x)$.
   We showed that there is at least one monic irreducible in $K[x]$, so our list $p_1(x), \ldots, p_k(x)$ has at least one element in
it and therefore \( f(x) = (p_1(x) \cdots p_k(x)) + 1 \) has positive degree. Theorem 9.2 says that \( f(x) \) (which is obviously monic) is either irreducible or factors as a product of irreducible polynomials, so \( f(x) \) is clearly divisible by an irreducible. But if any \( a(x) \) divides \( b(x) \), so does \( \gamma a(x) \) for any nonzero \( \gamma \in K \), since such a \( \gamma \) is a unit in \( K \). (If \( a(x)c(x) = b(x) \), then \( (\gamma a(x))(\gamma^{-1}c(x)) = b(x) \).) So \( f(x) \) is divisible by a monic irreducible.

5. Deduce that the set \( p_1(x), \ldots, p_k(x) \) could not have been the entire collection of irreducible monic polynomials in \( K[x] \), and that therefore there must be infinitely many irreducible monic polynomials in \( K[x] \).

We have shown that there is a monic irreducible in \( K[x] \) that divides \( f(x) = p_1(x) \cdots p_k(x) + 1 \) and that none of the \( p_i(x) \) divides \( f(x) \). So there is a monic irreducible polynomial that is not one of the \( p_i(x) \).

It might be a little easier to understand the logic of the proof if we restate things as follows. We know there’s at least one monic irreducible. Suppose that there are only finitely many, so there’s some \( k \in \mathbb{N} \) such that \( p_1(x), \ldots, p_k(x) \) is a list of all the monic irreducibles in \( K[x] \). Constructing \( f(x) \) as above, we showed that none of the \( p_i(x) \) divide \( f(x) \), but we have also proved that \( f(x) \) is divisible by a monic irreducible. This is a contradiction, so our assumption that there were finitely many monic irreducibles in \( K[x] \) must be false.

• Exercise 9.7: In \( \mathbb{Q}[x] \), divide \( x^4 - 1 \) by \( x^3 - 2x^2 + x - 2 \) using long division. Determine the quotient and the remainder.

\[
\begin{align*}
  x^3 - 2x^2 + x - 2 & \overline{) x^4 } \\
                   & - x^4 + 2x^3 - x^2 + 2x \\
                   & \underline{- x^4 + 2x^3 - x^2 + 2x} \\
                   & 2x^3 - x^2 + 2x - 1 \\
                   & \underline{- 2x^3 + 4x^2 - 2x + 4} \\
                   & 3x^2 + 3
\end{align*}
\]

So the quotient is \( x + 2 \) and the remainder is \( 3x^2 + 3 \).

• Exercise 9.8: Prove the division theorem. Proceed as follows: (Part 1 says to review how we proved the division theorem for \( \mathbb{Z} \). You don’t have to write anything here for that.)

2. In the polynomial case, we want to mimic the approach for \( \mathbb{Z} \) as best we can. The size of a polynomial is measured in terms of its degree. Thus we can try to do an induction on the degree of \( b(x) \), with \( a(x) \) held fixed. It may be best to do this in three stages. First deal
with the case in which \( b(x) \) has degree less than the degree of \( a(x) \). This should be easy. Then deal with the case in which \( b(x) \) and \( a(x) \) have the same degree. This is a little trickier, but it is still entirely elementary. You are now ready for the general induction step.

Suppose first that \( \deg b(x) < \deg a(x) \). We take \( q(x) = 0 \) and \( r(x) = b(x) \). The condition that \( \deg r(x) < \deg a(x) \) is satisfied by the hypothesis on \( \deg b(x) \).

Now suppose that \( \deg b(x) = \deg a(x) \). Let \( \beta \) be the leading coefficient of \( b(x) \) and \( \alpha \) the leading coefficient of \( a(x) \). Note that both \( \alpha \) and \( \beta \) are nonzero. Consider the polynomial \((\beta/\alpha)a(x)\). Its leading coefficient is \( \beta \) and it has the same degree as \( a(x) \) and \( b(x) \). So the terms of highest degree in \( b(x) - (\beta/\alpha)a(x) \) cancel and \( b(x) - (\beta/\alpha)a(x) \) is a polynomial of degree strictly less than \( \deg a(x) \). So we can take \( q(x) = \beta/\alpha \) and \( r(x) = b(x) - (\beta/\alpha)a(x) \).

3. Assume that \( b(x) \) has degree \( n \) and that \( n \) is larger than the degree of \( a(x) \). Make the appropriate induction assumption about polynomials of degree \( n - 1 \). Taking a hint from the integer case, in which we wrote \( b \) as the sum of the smaller integer \( b - 1 \) and \( 1 \), we want to write \( b(x) \) in terms of a polynomial of degree \( n - 1 \) and a polynomial of degree \( 1 \). Can we write \( b(x) \) as \( xg(x) \) for some polynomial \( g(x) \) of degree \( n - 1 \)? Not necessarily, but we can come close. Observe that you can rewrite \( b(x) \) in the form \( xg(x) + c \) for some constant \( c \). Use the induction assumption to rewrite \( g(x) \) as \( a(x)q'(x) + r'(x) \) for suitable polynomials \( q'(x) \) and \( r'(x) \). What do you know about the degree of \( r'(x) \)? Plug the expression for \( g(x) \) back into \( xg(x) + c \) and look at what you have. The argument at this point is reminiscent of the argument for the division theorem for the integers. You will have two cases, depending on the degree of \( r'(x) \). In one case, it will be obvious what \( q(x) \) and \( r(x) \) should be; in the other, some more work will need to be done.

Recall that our strategy is to fix \( a(x) \) and induct on the degree \( n \) of \( b \). So we’re trying to prove that \( b(x) \) can be written (uniquely) as \( a(x)q(x) + r(x) \) with \( \deg r(x) < \deg a(x) \). We’ve proved that we can do this if \( \deg b(x) \leq \deg a(x) \) and we’re now assuming \( \deg b(x) = n > \deg a(x) \). So our induction hypothesis is that the result holds if we have a polynomial \( b(x) \) of degree less than \( n \).

Suppose \( b(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \). Following the hint, we take \( g(x) = b_nx^{n-1} + b_{n-1}x^{n-2} + \cdots + b_1 \). Then \( b(x) = xg(x) + b_0 \).

By the inductive hypothesis, there exist polynomials \( q'(x) \) and \( r'(x) \) such that \( g(x) = a(x)q'(x) + r'(x) \) and \( \deg r'(x) < \deg a(x) \). So \( b(x) = xg(x) + b_0 = xa(x)q'(x) + xr'(x) + b_0 \).

If \( \deg xr'(x) < \deg a(x) \), we can just take \( q(x) = xq'(x) \) and
\[ r(x) = x r'(x) + b_0; \] the tricky case is when \( \deg x r'(x) = \deg a(x) \) (so \( \deg r'(x) = \deg a(x) - 1 \)).

In that case, we apply the inductive hypothesis again to divide \( x r'(x) + b_0 \) by \( a(x) \). (These two polynomials have the same degree, so this is a case we handled explicitly in the previous part by adjusting the leading coefficients.) So we have polynomials \( q''(x) \) and \( r''(x) \) such that \( x r'(x) + b_0 = q''(x) a(x) + r''(x) \) with \( \deg r''(x) < \deg a(x) \). (Note that \( q''(x) \) has degree 0.) Then

\[
b(x) = x g(x) + b_0 \\
= x q'(x) a(x) + (x r'(x) + b_0) \\
= x q'(x) a(x) + q''(x) a(x) + r''(x) \\
= (x q'(x) + q''(x)) a(x) + r''(x)
\]

where \( \deg r''(x) < \deg a(x) \).

So we take \( q(x) = (x q'(x) + q''(x)) \) and \( r(x) = r''(x) \). This completes the proof of the existence of \( q(x) \) and \( r(x) \). \( \square \)

4. To prove the uniqueness portion of the theorem, suppose there is another pair of polynomials \( s(x) \) and \( t(x) \) with \( b(x) = a(x) s(x) + t(x) \) and with the degree of \( t(x) \) less than the degree of \( a(x) \). Use the degree formula of Theorem 9.1 to show that \( r(x) - t(x) = 0 = q(x) - s(x) \).

So suppose \( b(x) = a(x) q(x) + r(x) = a(x) s(x) + t(x) \) with \( \deg r(x), \deg t(x) < \deg a(x) \). Subtracting, we have \( 0 = a(x) (q(x) - s(x)) + (r(x) - t(x)) \), so

\[
a(x) (s(x) - q(x)) = r(x) - t(x).
\]

Since \( r(x) \) and \( t(x) \) both have degree less than \( \deg a(x) \), so does \( r(x) - t(x) \). Then \( a(x) (s(x) - q(x)) \) also has degree less than \( \deg a(x) \). But the degree of a product of polynomials is the sum of their degrees, so the only way the left side of the equation can have degree less than \( \deg a(x) \) is if \( s(x) - q(x) = 0 \). Then we must also have \( r(x) - t(x) = 0 \). So we have shown that \( s(x) = q(x) \) and \( t(x) = r(x) \). \( \square \)

- Exercise 9.9: Use Theorem 9.6 to prove Theorem 9.7. (Theorem 9.7 says that if \( f(x) \in K[x] \), for a field \( K \), and \( \gamma \in K \) is a root of \( f(x) \), then \( x - \gamma \) divides \( f(x) \) in \( K[x] \).)

Suppose that \( f(x) \in K[x] \) and \( \gamma \in K \) is a root of \( f(x) \). Theorem 9.6 is the special case of the division theorem when the divisor has the form \( x - \gamma \), and it says that there is a polynomial \( q(x) \in K[x] \) and an element \( r \in K \) such that \( f(x) = \).
(x − γ)q(x) + r. Plugging in γ (more technically, evaluating the polynomials at γ), we get 0 = 0q(γ) + r = r. So the remainder r must be 0. This says that f(x) = (x − γ)q(x), so x − γ divides f(x).

Exercise 9.10: Prove Theorem 9.8, which says that, for K a field and

γ ∈ K, if f(x), g(x) ∈ K[x] such that x − γ divides the product f(x)g(x),

then x − γ divides at least one of f(x) and g(x).

1. Use Theorem 9.6 to rewrite f(x) and g(x) in terms of x − γ and multiply the two expressions together to express f(x)g(x) in terms of x − γ and a constant.

By theorem 9.6, we can write f(x) = (x − γ)q_f(x) + r_f

and g(x) = (x − γ)q_g(x) + r_g, where q_f(x), q_g(x) ∈ K[x] and r_f, r_g ∈ K. Then we have

\[ f(x)g(x) = ((x − γ)q_f(x) + r_f)((x − γ)q_g(x) + r_g) \]

\[ = (x − γ)(q_f(x)q_g(x) + q_f(x)r_g + q_g(x)r_f + r_fr_g). \]

2. Use the fact that x − γ divides this product to show that it divides the constant.

(You can’t divide by x − γ; you have to do the same kind of thing we did in Exercise 9.6 part 3.) Since x − γ divides f(x)g(x), there is an h(x) ∈ K[x] such that f(x)g(x) = (x − γ)h(x). So we have

\[ (x − γ)h(x) = (x − γ)(q_f(x)q_g(x) + q_f(x)r_g + q_g(x)r_f + r_fr_g). \]

Subtracting (x − γ)(q_f(x)q_g(x) + q_f(x)r_g + q_g(x)r_f) from both sides gives us

\[ (x − γ)h(x) − (x − γ)(q_f(x)q_g(x) + q_f(x)r_g + q_g(x)r_f) = r_fr_g. \]

In this last equation, x − γ clearly divides the left side, so it must also divide r_fr_g.

[Once you’ve done this kind of thing a few more times, you can get away with just saying something like “Since x − γ divides f(x)g(x), it must divide r_fr_g.” But for now, you need to write out a more complete argument. ]

3. Deduce that the constant is 0, and from this conclude that x − γ divides f(x) or g(x).

But x − γ has degree 1 and r_fr_g has degree at most 0; a polynomial of positive degree can’t divide a nonzero polynomial of lower degree. This tells us that r_fr_g must be 0, so at least one of r_f and r_g is 0. That implies that x − γ divides at least one of f(x) and g(x)
• Exercise 9.11: Prove Theorem 9.9, which says that, for \( f(x) \in K[x] \), if \( \gamma_1, \ldots, \gamma_m \) are distinct roots of \( f(x) \) in \( K \), then \((x-\gamma_1) \cdots (x-\gamma_m)\) divides \( f(x) \) in \( K[x] \).

We prove this by induction on \( m \).

For the base case, \( m = 1 \), Theorem 9.7 tells us that \( x - \gamma_1 \) divides \( f(x) \) in \( K[x] \).

Now assume that we know that if \( \gamma_1, \ldots, \gamma_k \) are distinct roots of some \( f(x) \), then \((x-\gamma_1) \cdots (x-\gamma_k)\) divides \( f(x) \) in \( K[x] \), and let \( \gamma_{k+1} \) be another root of \( f(x) \), not equal to any of the \( \gamma_i \) with \( i \leq k \).

Our assumption means that there is a \( g_k(x) \in K[x] \) with \( f(x) = (x-\gamma_1) \cdots (x-\gamma_k)g_k(x) \), and Theorem 9.7 tells us that \( x - \gamma_{k+1} \) divides \( f(x) \). Then Theorem 9.8 implies that \( x - \gamma_{k+1} \) divides either \((x-\gamma_1) \cdots (x-\gamma_k)\) or \( g_k(x) \). But \( x - \gamma_{k+1} \) obviously doesn’t divide \((x-\gamma_1) \cdots (x-\gamma_k)\); if it did, \( \gamma_{k+1} \) would be a root of \((x-\gamma_1) \cdots (x-\gamma_k)\), but plugging in \( \gamma_{k+1} \) for \( x \) gives us a product of nonzero elements of \( K \), which we know is an integral domain. So that product is nonzero. This says that \( x - \gamma_{k+1} \) must divide \( g_k(x) \). If we call the quotient \( g_{k+1}(x) \), then we have

\[
f(x) = (x-\gamma_1) \cdots (x-\gamma_{k+1})g_{k+1}(x),
\]

so \((x-\gamma_1) \cdots (x-\gamma_{k+1})\) divides \( f(x) \) in \( K[x] \). This completes the induction proof.

• Exercise 9.12: Prove Theorem 9.10, which says that a nonzero polynomial in \( K[x] \) of degree \( n \) has at most \( n \) distinct roots in \( K \). (Hint: If \( f(x) \) has \( n+1 \) distinct roots, what can you say about the degree of \( f(x) \)?)

Suppose that \( f(x) \in K[x] \) is a nonzero polynomial of degree \( n \) with \( n+1 \) distinct roots, \( \gamma_1, \ldots, \gamma_{n+1} \) in \( K \). By Theorem 9.9, the polynomial \( h(x) = (x-\gamma_1) \cdots (x-\gamma_{n+1}) \) divides \( f(x) \) in \( K[x] \). But \( h(x) \) has degree \( n+1 \) and a polynomial of degree \( n+1 \) cannot divide a nonzero polynomial of degree \( n \). So \( f(x) \) can have at most \( n \) distinct roots in \( K \).

• Exercise 9.13: Let \( K \) be a field.

1. Show that a polynomial \( f(x) \) in \( K[x] \) of degree 2 either has a root in \( K \) or is irreducible in \( K[x] \).

If a polynomial of degree 2 has a nontrivial factorization, both factors must have positive degree less than 2, and hence have degree 1. But having a factor of degree 1 is equivalent to having a root in \( K \). If \( f(x) \) has no nontrivial factorization, it’s irreducible.
2. Show that a polynomial \( f(x) \) in \( K[x] \) of degree 3 either has a root in \( K \) or is irreducible in \( K[x] \).

If a polynomial of degree 3 has a nontrivial factorization, one factor must have degree 1 and the other must have degree 2. So the polynomial is divisible by a degree 1 polynomial and hence has a root in \( K \). If \( f(x) \) has no nontrivial factorization, it is irreducible. ☐

3. Give an example of a polynomial \( f(x) \) in \( \mathbb{R}[x] \) of degree 4 that has no roots in \( \mathbb{R} \) yet is not irreducible in \( \mathbb{R}[x] \).

Observe that the polynomial \( x^2 + 1 \) has degree 2 but no roots in \( \mathbb{R} \) (since the square of any real number is non-negative). So \( x^2 + 1 \) must be irreducible in \( \mathbb{R}[x] \). Then \( (x^2 + 1)(x^2 + 1) \) is a polynomial of degree 4 in \( \mathbb{R}[x] \) which obviously has a nontrivial factorization but has no degree 1 factors, and thus no roots in \( \mathbb{R} \).