Math 461 Homework 5 — Spring 2020, Drew Armstrong

Problem 1. Use the Rational Root Test to split the following polynomial:

$$f(x) = 8x^3 + 4x^2 - 2x - 1 \in \mathbb{Q}[x].$$

If $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, then the Rational Root Test tells us that $a|1$ and $b|8$, so there are eight potential rational roots:

$$\frac{a}{b} \in \left\{ \pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8} \right\}.$$

By direct checking we find that $\pm 1/2$ are roots. Thus by Descartes' Theorem we have

$$f(x) = (x - 1/2)(x + 1/2)g(x) = (x^2 - 1/4)g(x)$$

for some $g(x) \in \mathbb{Q}[x]$ of degree 1, and by long division we find that $g(x) = 8x + 4$:

$$\begin{array}{r|l}
 & 8x + 4 \\
\hline
x^2 - \frac{1}{4} & 8x^3 + 4x^2 - 2x - 1 \\
 & -\,8x^3 \qquad\quad + 2x \\
\hline
 & \qquad 4x^2 \qquad\ - 1 \\
 & \qquad -\,4x^2 \qquad + 1 \\
\hline
 & \qquad\qquad\qquad\quad 0
\end{array}$$

Finally, we conclude that

$$\begin{aligned}
f(x) &= (x - 1/2)(x + 1/2)(8x + 4) \\
&= 8(x - 1/2)(x + 1/2)^2 \\
&= (2x - 1)(2x + 1)^2.
\end{aligned}$$

Notice that the form of the solution is not unique.

[Remark: It turned out that $-1/2$ is actually a double root of $f(x)$. We could see this more quickly by observing that $-1/2$ is also a root of the derivative polynomial $f'(x) = 24x^2 + 8x - 2$. In general, one can show that a root of $f(x)$ has multiplicity greater than one if and only if it also a root of the derivative $f'(x)$.]

Problem 2. Symmetric Polynomials. Suppose that the polynomial $x^3 + x^2 + 2x + 3$ has the roots r, s, t (in some field). Find some integer coefficients $a, b, c \in \mathbb{Z}$ such that the polynomial $x^3 + ax^2 + bx + c$ has the roots rs, rt, st.

If the polynomial $x^3 + x^2 + 2x + 3$ has roots r, s, t (in some field), then Descartes says

$$\begin{aligned}
x^3 + x^2 + 2x + 3 &= (x - r)(x - s)(x - t) \\
&= x^3 - (r + s + t)x^2 + (rs + rt + st)x - rst,
\end{aligned}$$

and comparing coefficients gives

$$\begin{cases}
-1 &= r + s + t, \\
\ \ 2 &= rs + rt + st, \\
-3 &= rst.
\end{cases}$$

Now suppose that the polynomial $x^3 + ax^2 + bx + c$ has roots rs, rt, st (in the same field). Again, by Descartes' Theorem we have

$$\begin{aligned} x^3 + ax^2 + bx + c &= (x - rs)(x - rt)(x - st) \\ &= x^3 - (rs + rt + st)x^2 + [(rs)(rt) + (rs)(st) + (rt)(st)]x - (rs)(rt)(st), \\ &= x^3 - (rs + rt + st)x^2 + rst(r + s + t)x - (rst)^2, \end{aligned}$$

and then comparing coefficients gives

$$\begin{cases} a &= -(rs + rt + st) = -2, \\ b &= rst(r + s + t) = 3, \\ c &= -(rst)^2 = -9. \end{cases}$$

We conclude that the polynomial $x^3 - 2x^2 + 3x - 9$ has roots rs, rt, st, and we found this without even knowing the values of r, s, t. It doesn't even matter where these roots live, only that they exist in some field somewhere.

[Remark: This problem is based on Laplace's Proof of the Fundamental Theorem of Algebra. If the real polynomial $f(x) \in \mathbb{R}[x]$ has roots α_i $(1 \leq i \leq n)$, recall that for each real number $\lambda \in \mathbb{R}$ we defined the auxiliary polynomial $g_\lambda(x)$ with roots $\beta_{ij\lambda} = \alpha_i + \alpha_j + \lambda\alpha_i\alpha_j$ $(1 \leq i < j \leq n)$. By using the same method as above, we could express each coefficient of $g_\lambda(x)$ as a symmetric function of the roots $\beta_{ij\lambda}$, which is necessarily also a symmetric function of the roots α_i of $f(x)$, hence is some real function of the coefficients of $f(x)$, hence is a real number. Thus it follows that $g_\lambda(x)$ has real coefficients.

If I wanted to make the problem slightly more relevant (and much harder) I would have asked you to find the coefficients of the polynomial with roots $r+s+\lambda rs, r+t+\lambda rt, s+t+\lambda st$. P.S. The answer is $x^3 - (2\lambda - 2)x^2 + (3\lambda^2 - 11\lambda + 3)x - (9\lambda^3 - 12\lambda^2 + 7\lambda + 1)$.]

Problem 3. Some Specific Cyclotomic Polynomials. Let $\omega = e^{2\pi i/n}$ and recall the definition of the nth cyclotomic polynomial:

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \omega^k).$$

(a) If p is prime, show that $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$. [Hint: In this case we have $\gcd(k, p) = 1$ for all $1 \leq k < p$ and hence $\Phi_p(x) = (x - \omega)(x - \omega^2)\cdots(x - \omega^{p-1})$ for $\omega = e^{2\pi i/p}$. On the other hand, we know that $x^p - 1 = (x - 1)(x - \omega)\cdots(x - \omega^{p-1})$.]

(b) If $n = 2^m$ for some $m \geq 1$, show that $\Phi_n(x) = 1 + x^{n/2}$. [Hint: Show that the roots of $\Phi_n(x)$ are precisely the $(n/2)$th roots of -1. First, observe that $\gcd(k, n) = 1$ if and only if k is odd, hence the roots of $\Phi_n(x)$ are $(e^{2\pi i/n})^{\text{odd}}$. Second, observe that $\alpha^{n/2} = -1 = e^{i(\pi+2\pi k)}$ implies $\alpha = e^{i(\pi+2\pi k)/(n/2)} = (e^{2\pi i/n})^{1+2k}$ for all $k \in \mathbb{Z}$.]

(a): Let p be prime and let $\omega = e^{2\pi i/p}$. Then since $\gcd(k, p) = 1$ for all $1 \leq k < p$ we have

$$\Phi_p(x) = (x - \omega^1)(x - \omega^2)\cdots(x - \omega^{p-1}).$$

On the other hand, we know the following two factorizations of $x^p - 1$:

$$x^p - 1 = (x - 1)(1 + x + x^2 + \cdots + x^{p-1})$$

$$x^p - 1 = (x - 1)(x - \omega)\cdots(x - \omega^{p-1}).$$

By comparing these three formulas we obtain

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}.$$

(b): Let $n = 2^m$ be a power of 2 with $m \geq 1$ and let $\omega = e^{2\pi i/n}$. Then I claim that $\Phi_n(x) = 1 + x^{n/2}$. To see this, we first note that $\gcd(k, n) = 1$ if and only if k is odd. Hence

$$\Phi_n(x) = (x - \omega)(x - \omega^3)(x - \omega^5) \cdots (x - \omega^{n-1}).$$

On the other hand, we will compute the $(n/2)$th (i.e., 2^{m-1}th) roots of -1. To do this we note that -1 can be expressed in polar form as $e^{i\pi}$, more generally as $e^{i(\pi+2\pi k)}$ for any $k \in \mathbb{Z}$. If α is an $(n/2)$th root of -1 then we must have

$$\begin{aligned}
\alpha^{n/2} &= -1 \\
\alpha^{n/2} &= e^{i(\pi+2\pi k)} \\
\alpha &= e^{i(\pi+2\pi k)/(n/2)} \\
&= e^{2\pi i(1+2k)/n} \\
&= (e^{2\pi i/n})^{1+2k} \\
&= \omega^{1+2k}
\end{aligned}$$

for some integer $k \in \mathbb{Z}$. It follows that $(n/2)$th roots of -1 are $\omega^1, \omega^3, \omega^5, \cdots, \omega^{n-1}$, and hence

$$\begin{aligned}
x^{n/2} + 1 &= x^{n/2} - (-1) \\
&= (x - \omega)(x - \omega^3)(x - \omega^5) \cdots (x - \omega^{n-1}) \\
&= \Phi_n(x).
\end{aligned}$$

[Remark: In both of these cases we found that $\Phi_n(x)$ has integer coefficients. In Problem 5 below we will prove that this always happens.]

Problem 4. Uniqueness of Quotient and Remainder. Let $\mathbb{F}$ be a field and consider polynomials $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0(x)$.

(a) Suppose that we have $q_1(x), r_1(x), q_2(x), r_2(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = q_1(x)g(x) + r_1(x), \\ \deg(r_1) < \deg(g), \end{cases} \qquad \begin{cases} f(x) = q_2(x)g(x) + r_2(x), \\ \deg(r_2) < \deg(g). \end{cases}$$

In this case, prove that $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. [Hint: First note that $(q_1 - q_2)g = (r_2 - r_1)$. If $q_1 \neq q_2$ then this implies that $\deg(r_2 - r_1) \geq \deg(g)$. On the other hand, we have $\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\}$.]

(b) Now let $R \subseteq \mathbb{F}$ be a subring. Suppose that we have $f(x), g(x) \in R[x]$ where $g(x)$ has leading coefficient 1, and suppose that $f(x) = g(x)q(x)$ for some $q(x) \in \mathbb{F}[x]$. In this case, use part (a) to show that we must actually have $q(x) \in R[x]$. [Hint: Since $g(x) \in R[x]$ has leading coefficient 1, we may apply long division to obtain $f(x) = g(x)q'(x) + r'(x)$ for some $q'(x), r'(x) \in R[x]$ with $\deg(r') < \deg(g')$. On the other hand, we have assumed that $f(x) = g(x)q(x) + 0$ for some $q(x) \in \mathbb{F}[x]$. Apply (a) to show that $q(x) = q'(x)$, and hence $q(x) \in R[x]$.]

(a): Suppose that we have $q_1(x), r_1(x), q_2(x), r_2(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = q_1(x)g(x) + r_1(x), \\ \deg(r_1) < \deg(g), \end{cases} \qquad \begin{cases} f(x) = q_2(x)g(x) + r_2(x), \\ \deg(r_2) < \deg(g). \end{cases}$$

By equating the two formulas for $f(x)$ this implies that

$$\begin{aligned}
q_1(x)g(x) + r_1(x) &= q_2(x)g(x) + r_2(x) \\
[q_1(x) - q_2(x)]g(x) &= [r_2(x) - r_1(x)].
\end{aligned}$$

Now **assume for contradiction** that $q_1(x) \neq q_2(x)$, and hence $q_1(x) - q_2(x) \neq 0(x)$. Since we also have $g(x) \neq 0(x)$, it follows from the above formula that

$$\deg(r_2 - r_1) = \deg((q_1 - q_2)g) = \deg(q_1 - q_2) + \deg(g) \geq \deg(g).$$

On the other hand, since $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$ we must have

$$\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\} < \deg(g).$$

This contradiction shows that $q_1(x) = q_2(x)$. Finally, we conclude that

$$[r_2(x) - r_1(x)] = [q_1(x) - q_2(x)]g(x) = 0(x)g(x) = 0(x),$$

and hence $r_1(x) = r_2(x)$. $\square$

(b): Let $R \subseteq \mathbb{F}$ be a subring of a field and suppose that we have $f(x) = g(x)q(x)$ for some $f(x), g(x) \in R[x]$ and $q(x) \in \mathbb{F}[x]$, where $g(x)$ has leading coefficient 1.[1] In this case I claim that we must have $q(x) \in R[x]$.

To see this, we first apply long division to divide $f(x)$ by $g(x)$. Since $f(x), g(x) \in R[x]$ and since the leading coefficient of $g(x)$ is 1 we are guaranteed that the quotient and remainder are also in the ring $R[x]$. In other words, there exist some $q'(x), r'(x) \in R[x]$ satisfying $f(x) = g(x)q'(x) + r'(x)$ and $\deg(r') < \deg(g)$. On the other hand, we also have $f(x) = g(x)q(x) + 0(x)$ and $\deg(0) < \deg(g)$. But now it follows from part (a) that $q(x) = q'(x)$, hence $q(x)$ has coefficients in R. $\square$

Problem 5. Cyclotomic Polynomials Have Integer Coefficients. We will prove in class that cyclotomic polynomials satisfy the following identity:

$$x^n - 1 = \prod_{\substack{1 \leq d \leq n \\ d|n}} \Phi_d(x).$$

Use this identity and Problem 4(b) to prove by induction that $\Phi_n(x) \in \mathbb{Z}[x]$ for all $n \geq 1$. [Hint: Suppose that we have $x^n - 1 = \Phi_n(x)q(x)$ for some polynomial $q(x) \in \mathbb{Z}[x]$. Then since $\Phi_n(x) \in \mathbb{C}[x]$ has leading coefficient 1, we can apply Problem 4(b) with $R = \mathbb{Z}$ and $\mathbb{F} = \mathbb{C}$.]

We will prove by induction that $\Phi_n(x) \in \mathbb{Z}[x]$ for all $n \geq 1$. The base case is $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Now fix some $n \geq 2$ and **assume for induction** that we have $\Phi_k(x) \in \mathbb{Z}[x]$ for all $1 \leq k < n$. In this case we will show that $\Phi_n(x)$.

To see this we isolate the factor $\Phi_n(x)$ from the right hand side of the given identity:

$$x^n - 1 = \Phi_n(x) \prod_{\substack{1 \leq d < n \\ d|n}} \Phi_d(x).$$

Define the polynomials $f(x) = x^n - 1$, $q(x) = \Phi_n(x)$ and $g(x) = \prod_d \Phi_d(x)$, where this product runs over all $d|n$ such that $1 \leq d < n$. By induction, each factor in this product has integer coefficients, hence $g(x)$ has integer coefficients. (Furthermore, since cyclotomic polynomials have leading coefficient 1 by definition, the product $g(x)$ also has leading coefficient 1.) In summary, we have $f(x) = g(x)q(x)$ where $f(x), g(x) \in \mathbb{Z}[x]$ and $q(x) \in \mathbb{C}[x]$, and where $g(x)$ has leading coefficient 1. Thus it follows from Problem 4(b) that $q(x) \in \mathbb{Z}[x]$ as desired. $\square$

[1]More generally, we can allow the leading coefficient of $g(x)$ be any invertible element of the ring R.

Problem 6. A Property of Quadratic Field Extensions. The construction of $\mathbb{C}$ from $\mathbb{R}$ can be generalized as follows. Let $\mathbb{E} \supseteq \mathbb{F}$ be fields and let $\iota \in \mathbb{E}$ be some element satisfying $\iota \notin \mathbb{F}$ and $\iota^2 \in \mathbb{F}$. Then I claim that the following set is a **subfield** of $\mathbb{E}$:

$$\mathbb{F}(\iota) := \{a + b\iota : a, b \in \mathbb{F}\}.$$

Furthermore, the conjugation operator $(a + b\iota)^* = (a - b\iota)$ behaves exactly like complex conjugation. Jargon: We say that $\mathbb{F}(\iota) \supseteq \mathbb{F}$ is a *quadratic field extension.* The following Lemma will be useful in our discussion of impossible constructions:

> *Consider a polynomial $f(x) \in \mathbb{F}[x]$ of degree 3. If $f(x)$ has some root $\alpha \in \mathbb{F}(\iota)$ in a quadratic field extension then I claim that $f(x)$ also has a root in $\mathbb{F}$.*

Prove the Lemma. [Hint: Let $\alpha \in \mathbb{F}(\iota)$ be a root of $f(x)$. If $\alpha \in \mathbb{F}$ then we are done. Otherwise, the conjugate $\alpha^* \in \mathbb{F}(\iota)$ is another root of $f(x)$, hence by Descartes' Factor Theorem we have

$$f(x) = (x - \alpha)(x - \alpha^*)g(x) \quad \text{for some } g(x) \in \mathbb{F}(\iota)[x] \text{ of degree 1.}$$

Use Problem 4(b) to show that $g(x) \in \mathbb{F}[x]$, hence $g(x)$ has a root in $\mathbb{F}$.]

Proof. Let $\mathbb{F}(\iota) \supseteq \mathbb{F}$ be a quadratic field extension and let $f(x) \in \mathbb{F}[x]$ have degree 3. Then

$$\left(\begin{array}{c} f(x) \text{ has a root} \\ \text{in the field } \mathbb{F}(\iota) \end{array}\right) \quad \Rightarrow \quad \left(\begin{array}{c} f(x) \text{ has a root} \\ \text{in the field } \mathbb{F} \end{array}\right).$$

To prove this, suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}(\iota)$. If $\alpha \in \mathbb{F}$ then we are done, so let us suppose that $\alpha \notin \mathbb{F}$, and hence $\alpha^* \neq \alpha$. Since the coefficients of f are in $\mathbb{F}$ we have

$$f(\alpha) = 0 \quad \Rightarrow \quad [f(\alpha)]^* = 0 \quad \Rightarrow \quad f^*(\alpha^*) = 0 \quad \Rightarrow \quad f(\alpha^*) = 0,$$

and hence α^* is another root of $f(x)$. By applying Descartes' Factor Theorem twice we obtain

$$f(x) = (x - \alpha)(x - \alpha^*)q(x)$$

for some polynomial $q(x) \in \mathbb{F}(\iota)[x]$ of degree 1. But I claim that $q(x)$ actually has coefficients in $\mathbb{F}$. To see this, we define $g(x) = (x - \alpha)(x - \alpha^*)$ and note that

$$g(x) = x^2 - (\alpha + \alpha^*)x + \alpha\alpha^*$$

has coefficients in $\mathbb{F}$ because $(\alpha + \alpha^*)^* = \alpha + \alpha^*$ and $(\alpha\alpha^*)^* = \alpha\alpha^*$. Thus we have $f(x) = g(x)q(x)$ with $f(x), g(x) \in \mathbb{F}[x]$ and $q(x) \in \mathbb{F}(\iota)[x]$, where $g(x)$ has leading coefficient 1.[2] It follows from Problem 4(b) that $q(x) \in \mathbb{F}[x]$ and since $\deg(q) = 1$ this implies that $q(x) = ax+b$ for some $a, b \in \mathbb{F}$ with $a \neq 0$. Finally, we observe that

$$f(-b/a) = g(-b/q)q(-b/a) = g(-b/a)0 = 0,$$

hence $f(x)$ has the root $-b/a \in \mathbb{F}$ as desired. $\square$

[Remark: Why do we care? In class we will use this lemma to prove that a polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3 with no rational roots, also has no constructible roots.[3] It will follow that the numbers $\sqrt[3]{2}$, $\cos(2\pi/9)$, and $\cos(2\pi/7)$ are not constructible, hence the classical problems of doubling the cube, trisecting the angle, and constructing the regular heptagon are impossible.]

---

[2] Actually, the leading coefficient of g doesn't matter this time because $\mathbb{F}$ is a field.

[3] Recall that a "constructible number" is a coordinate of a point that can be constructed from the points $(0, 0)$ and $(1, 0)$ using straightedge and compass.