Sample Homework Solutions for 3.2

Jim Brown

1. Suppose $f(x) \in \mathbb{C}[x]$ is a monic polynomial of degree n with roots $c_1, c_2, \dots c_n$. Prove that the sum of the roots is $-a_{n-1}$ and their product is $(-1)^n a_0$.

Proof: We proceed by induction on the degree of $f(x)$. The case of $n = 2$ is the base case and handled as follows. Let $f(x) = x^2 + a_1 x + a_0 \in \mathbb{C}[x]$ with roots c_1, c_2. Then we can write $f(x) = (x-c_1)(x-c_2) = x^2-(c_1+c_2)x+c_1c_2$. Equating the coefficients we have that $a_1 = -(c_1 + c_2)$ and $a_0 = c_1c_2$, i.e,. $-a_1 =$ the sum of the roots and $(-1)^2 =$ product of the roots. Now suppose there is some positive integer k so that any polynomial of degree k satisfies the conditions we desire. Let $f(x) = x^{k+1} + a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ with roots given by $c_1, \dots, c_{k+1}$. The fact that the c_i's are the roots of $f(x)$ allows one to write

$$f(x) = (x - c_1)(x - c_2) \cdots (x - c_{k+1}). \tag{1}$$

We can apply the induction hypothesis to the polynomial $(x-c_1)\cdots(x-c_k)$ to conclude that

$$(x - c_1) \cdots (x - c_k) = x^k - (c_1 + \cdots + c_k)x^{k-1} + \cdots + (-1)^k c_1 \cdots c_k.$$

Now we multiply this by $(x - c_{k+1})$ on both sides to obtain:

$$\begin{aligned} f(x) &= (x - c_1) \cdots (x - c_k)(x - c_{k+1}) \\ &= (x^k - (c_1 + \cdots + c_k)x^{k-1} + \cdots + (-1)^k c_1 \cdots c_k)(x - c_{k+1}) \\ &= x^{k+1} - (c_1 + \cdots + c_k)x^k + \cdots + (-1)^k c_1 \cdots c_k - c_{k+1}x^k - \cdots - (-1)^k c_1 \cdots c_k c_{k+1} \\ &= x^{k+1} - (c_1 + \cdots + c_{k+1})x^k + \cdots + (-1)^{k+1} c_1 \cdots c_{k+1}, \end{aligned}$$

i.e., $-a_k = c_1 + \cdots + c_{k+1}$ and $(-1)^{k+1} a_0 = c_1 \cdots c_{k+1}$. Thus, the statement is true for all degrees n by induction. ■

2. Prove that

(b) $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, but $\mathbb{Q}[\sqrt{6}] \subsetneq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Proof: It is clear that $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ as $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ contains $\sqrt{2}$ and $\sqrt{3}$ and is closed under addition, thus contains $\sqrt{2} + \sqrt{3}$. Therefore, it contains any polynomial value $p(\sqrt{2}+\sqrt{3})$ for $p(x) \in \mathbb{Q}[x]$. To show that $\mathbb{Q}[\sqrt{2},\sqrt{3}] \subset \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ we need to show that $\sqrt{2}$ and $\sqrt{3}$ are both in $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$. Observe that

$$\sqrt{2} = \frac{1}{2}[(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})] \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$$

and

$$\sqrt{3} = -\frac{1}{2}[(\sqrt{2}+\sqrt{3})^3 - 11(\sqrt{2}+\sqrt{3})] \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$$

and so we have $\mathbb{Q}[\sqrt{2},\sqrt{3}] \subset \mathbb{Q}[\sqrt{2}+\sqrt{3}]$.
It is clear that $\mathbb{Q}[\sqrt{6}] \subset \mathbb{Q}[\sqrt{2},\sqrt{3}]$ as $\sqrt{6} = \sqrt{2}\cdot\sqrt{3} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$. To show the reverse containment does not hold, suppose $\sqrt{2} \in \mathbb{Q}[\sqrt{6}]$. Then there exists $a, b \in \mathbb{Q}$ so that $\sqrt{2} = a + b\sqrt{6}$. Squaring both sides we get $2 = a^2 + 6b^2 + 2ab\sqrt{6}$. Solving this for $\sqrt{6}$ we see that this would imply $\sqrt{6} \in \mathbb{Q}$, a contradiction. The only problem with solving for $\sqrt{6}$ would occur if either a or b was 0. It is easy to see that $b \neq 0$ since $\sqrt{2} \notin \mathbb{Q}$. Similarly, if $a = 0$, then $\sqrt{2} = b\sqrt{6}$, i.e., $\sqrt{3} = \frac{1}{b} \in \mathbb{Q}$, a contradiction. Thus, $\sqrt{2} \notin \mathbb{Q}[\sqrt{6}]$. ■

3. Find the splitting fields of the following polynomials in $\mathbb{Q}[x]$:

(c) $f(x) = x^4 - 9$

The first step is to determine the roots of $f(x)$. As we saw in section 2.3, the roots are given by $\sqrt[4]{9}\omega^j$ for $1 \leq j \leq 3$ with ω the 4th root of unity, which is i. Note that $\sqrt[4]{9} = \sqrt{3}$. Thus, the roots are $\sqrt{3}, \sqrt{3}i, -\sqrt{3}, -\sqrt{3}i$.
Let K be the splitting field of $f(x)$.
<u>Claim</u>: $K = \mathbb{Q}[\sqrt{3}, i]$.
<u>Proof</u>: Observe that $K \subset \mathbb{Q}[\sqrt{3}, i]$ because all of the roots of $f(x)$ are contained in $\mathbb{Q}[\sqrt{3}, i]$ and K is by definition the smallest field containing all of the roots of $f(x)$. Now we must show that $\sqrt{3}$ and i are necessarily in K as well. It is clear that $\sqrt{3} \in K$ as $\sqrt{3}$ is a root of $f(x)$ and K must contain all the roots. Since K contains $\sqrt{3}$, it must also contain $\dfrac{\sqrt{3}}{3}$. Since $\sqrt{3}i$ is a root, it is in K as well. Now using that K is closed under multiplication we have that $i = \dfrac{\sqrt{3}}{3}\sqrt{3} \in K$. Thus, $\mathbb{Q}[\sqrt{3}, i] \subset K$ and the claim is shown. ■

4. Decide whethe each of the following subsets of $\mathbb{R}$ is a ring, a field, or neither.

(a) $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$

This is not a ring as it is not closed under multiplication: $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$, but we claim $\sqrt[3]{4}$ is not in this set. Suppose there exists $a, b \in \mathbb{Q}$ so that $\sqrt[3]{4} = a + b\sqrt[3]{2}$, i.e., $\sqrt[3]{4} - b\sqrt[3]{2} = a$. Squaring both sides we get $2\sqrt[3]{2} - 4b + b^2\sqrt[3]{4} = a^2$, i.e., $2\sqrt[3]{2} - b^2\sqrt[3]{4} = a^2 + 4b$. Now we substitute $a + b\sqrt[3]{2}$ for $\sqrt[3]{4}$ to obtain the equation

$$(2 + b^3)\sqrt[3]{2} = a^2 + 4b - ab^2.$$

Since $b \in \mathbb{Q}$, we know that $b^3 \neq -2$ since $\sqrt[3]{2} \notin \mathbb{Q}$, so we can divide by $(2 + b^3)$ to obtain

$$\sqrt[3]{2} = \frac{a^2 + 4b - ab^2}{2 + b^3} \in \mathbb{Q}$$

a contradiction. Thus $\sqrt[3]{4}$ is not in the set.

7. Let $f(x) \in \mathbb{R}[x]$.

(a) Prove that the complex roots of $f(x)$ come in "conjugate pairs"; i.e., $\alpha \in \mathbb{C}$ is a root of $f(x)$ if and only if $\overline{\alpha}$ is also a root.

Proof: Let α be a root of $f(x) = a_n z^n + \cdots + a_1 z + a_0 \in \mathbb{R}[x]$. Then using that $\overline{\overline{z}} = z$, $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z} \cdot \overline{w}$, and $\overline{x} = x$ for all $z, w \in \mathbb{C}$ and all $x \in \mathbb{R}$ we have

$$\begin{aligned}
0 &= a_n\alpha^n + \cdots + a_1\alpha + a_0 \iff \\
0 &= \overline{a_n\alpha^n + \cdots + a_1\alpha + a_0} \iff \\
0 &= \overline{a_n}\,\overline{\alpha}^n + \cdots + \overline{a_1}\,\overline{\alpha} + \overline{a_0} \iff \\
0 &= a_n\overline{\alpha}^n + \cdots + a_1\overline{\alpha} + a_0.
\end{aligned}$$

Thus we see that $f(\alpha) = 0$ if and only if $f(\overline{\alpha}) = 0$. ■

(b) Prove that the only irreducible polynomials in $\mathbb{R}[x]$ are linear polynomials and quadratic polynomials $ax^2 + bx + c$ with $b^2 - 4ac < 0$.

Proof: The condition $b^2 - 4ac < 0$ is the condition that the quadratic polynomial has no real roots, as one can easily see from the quadratic equation. Therefore, the statement is to prove that we can reduce any polynomial down to just linear factors over $\mathbb{R}[x]$ and quadratic polynomials in $\mathbb{R}[x]$ with complex roots. The statement is clear for polynomials of degree 1 and 2, so we proceed by induction on the degree of the polynomial, taking degree

3 as our base case. Let $f(x) \in \mathbb{R}[x]$ have degree 3. Let α_1, α_2 and α_3 be the roots of $f(x)$. If one of them is complex, say α_1, then necessarily one of the others, say α_2 is the complex conjugate of α_1 by part (a) above. Thus we have that α_3 must be real. So $f(x) = (x - \alpha_3)(x^2 + (\alpha_1 + \overline{\alpha_1})x + \alpha_1\overline{\alpha_1}$. Since $\alpha_1 + \overline{\alpha_1}$ and $\alpha_1\overline{\alpha_1}$ are both real numbers, we have factored our polynomial as claimed. If on the other hand all the α_i are real, then we have $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ are we are done with the base case. Now suppose that any polynomial of degree $j \leq k$ for some positive integer k can be factored into a product of linear and irreducible quadratic terms over $\mathbb{R}[x]$. Let $f(x)$ be a polynomial of degree $k + 1$. Suppose $f(x)$ has a real root α. Then there exists a polynomial $g(x) \in \mathbb{R}[x]$ of degree k so that $f(x) = (x - \alpha)g(x)$. Now we apply the induction hypothesis to $g(x)$ and have that we can factor $f(x)$ into a product of linear terms and irreducible quadratic terms over $\mathbb{R}[x]$. If $f(x)$ does not have a real root, then necessary it has a complex root α. By part (a), $\overline{\alpha}$ is also a root of $f(x)$. Thus there exists a $g(x) \in \mathbb{R}[x]$ of degree $k-1$ so that $f(x) = (x^2 + (\alpha + \overline{\alpha})x + \alpha\overline{\alpha})g(x)$. Applying the induction hypothesis to $g(x)$ again gives our result. Thus, by induction, we have that every polynomial in $\mathbb{R}[x]$ can be factored into irreducible linear and quadratic polynomials, meaning these are the only irreducible polynomials over $\mathbb{R}[x]$. ■