Solutions to 412 Homework 2

Exercise 11.1. Prove that all numbers of the form $\alpha + \beta i$, for α and β in $\mathbb{Q}$, are algebraic over $\mathbb{Q}$.

Proof. Fixing some $\alpha, \beta \in \mathbb{Q}$, we consider the polynomial

$$\begin{aligned}(x - (\alpha + \beta i))(x - (\alpha - \beta i)) &= x^2 - (\alpha + \beta i)x - (\alpha - \beta i)x + (\alpha + \beta i)(\alpha - \beta i) \\ &= x^2 - 2\alpha x + (\alpha^2 + \beta^2).\end{aligned}$$

By construction it is clear that $\alpha + \beta i$ is a root of this polynomial. Moreover, since α and β are in $\mathbb{Q}$, so is -2α and $\alpha^2 + \beta^2$. We conclude that $\alpha + \beta i$ is algebraic over $\mathbb{Q}$. □

Exercise 11.7. Let n be an integer greater than 1. Prove that $x^n - 2$ is irreducible in $\mathbb{Q}[x]$.

Proof. We will prove this by contradiction. Supposing to the contrary that $x^n - 2$ is reducible in $\mathbb{Q}[x]$, then by Corollary 11.5 it is also reducible in $\mathbb{Z}[x]$. Then there exist polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$, of degrees $k < n$ and $l < n$, such that $x^n - 2 = g(x)h(x)$. It follows that there exist integers $a_0, \ldots, a_k, b_0, \ldots, b_l$ such that

$$g(x) = a_k x^k + \cdots + a_0 \text{ and } h(x) = b_l x^l + \cdots + b_0.$$

Then, as we've seen before,

$$x^n - 2 = \sum_{m=0}^{n} \left(\sum_{i+j=m} a_i b_j x^m \right).$$

Comparing the constant terms, we have that $-2 = a_0 b_0$, so 2 divides exactly one of a_0 or b_0. We without loss of generality suppose 2 divides a_0 but not b_0. Then looking at the degree-one coefficient we see

$$0 = a_0 b_1 + a_1 b_0,$$

then since 2 divides 0 and $a_0 b_1$ it must divide $a_1 b_0$, and therefore a_1. This will serve as a base case for our induction argument.

We now assume that 2 divides the first $m - 1$ terms of $g(x)$, but not b_0, for some $m < k$. Considering the degree-m term, we see

$$0 = a_0 b_m + a_1 b_{m-1} + \cdots + a_{m-1} b_1 + a_m b_0.$$

Since 2 divides 0 and the first m terms on the right hand side, it follows that 2 also divides $a_m b_0$. But since 2 doesn't divide b_0 it must divide a_m. Thus we conclude by induction that 2 divides every term of $g(x)$.

From this we then know that 2 must divide the degree-n terms of $g(x)h(x)$: $a_k b_l$. But we know this term should equal one, giving us a contradiction. Therefore, such $g(x)$ and $h(x)$ cannot exist, and by Corollary 11.5 $x^n - 2$ is irreducible. □

11.12. Use Eisenstein's criterion to show that the following polynomials do not factor in $\mathbb{Z}[x]$ as products of lower-degree polynomials. Deduce that they are irreducible in $\mathbb{Q}[x]$.

Solution.
(1) $x^{22} + 7x^3 + 7$: we use the prime 7.
(2) $x^{35} + 35x^{15} - 90$: we use the prime 5.
(3) $1662x^{384} - 35x^{100} + 625x^{44} + 100x^{10} - 75x + 20$: we use the prime 5.
(4) $6x^{31} + 35x^{21} + 245x^{11} + 175$: we use the prime 7.

Since these don't factor in $\mathbb{Z}[x]$ by Eisenstein's criterion, it follows from Theorem 11.6 or Corollary 11.5 that they are irreducible in $\mathbb{Q}[x]$. □

Exercise 11.14. Prove Theorem 11.7.

Theorem 1 (Theorem 11.7)**.** *For every prime p, the polynomial ring $\mathbb{F}_p[x]$ has irreducible polynomials of arbitrarily high degree; that is, there is no positive integer n such that all the irreducible polynomials of $\mathbb{F}_p[x]$ have degree less than or equal to n.*

Proof. We begin by fixing a positive integer n. Any polynomial of degree less than or equal to n will be of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

with the a_i elements of $\mathbb{F}_p$. However, $\mathbb{F}_p$ consists of only p elements, so there are p^{n+1} choices for our set $\{a_0, \ldots, a_n\}$, and thus p^{n+1} different polynomials of degree less than or equal to n. However, by Theorem 9.4 $\mathbb{F}_p[x]$ contains infinitely many irreducible polynomials. Therefore the set of polynomials of degree $\leq n$ cannot contain all irreducible polynomials. Since n was arbitrary, our result follows. $\square$

Exercise 11.17. Use reduction modulo p to prove that $x^5 + x^2 + 1$ does not factor in $\mathbb{Z}[x]$ as a product of lower-degree polynomials.

Proof. We consider $x^5 + x^2 + 1$ in $\mathbb{F}_2[x]$. We see that

$$0^5 + 0^2 + 1 = 1 \text{ and } 1^5 + 1^2 + 1 = 1,$$

so the polynomial has no roots in $\mathbb{F}_2$, and thus no degree-one factors in $\mathbb{F}_2[x]$. Then, if it were reducible in $\mathbb{F}_2[x]$, then there must exist irreducible polynomials $f(x)$ and $g(x)$ in $\mathbb{F}_2[x]$, of degree 2 and 3 respectively, such that $x^5 + x^2 + 1 = f(x)g(x)$. But we already know that $\mathbb{F}_2[x]$ has only one irreducible degree-two polynomial, so $f(x) = x^2 + x + 1$. We then observe that

$$x^5 + x^2 + 1 = (x^2 + x + 1)(x^3 + x^2) + 1,$$

so such a factorization is impossible. Therefore $x^5 + x^2 + 1$ is irreducible in $\mathbb{F}_2[x]$ and 2 does not divide the leading term, 1, so by Theorem 11.9 the polynomial is also irreducible in $\mathbb{Z}[x]$. $\square$

Exercise 12.3. Use the Euclidean algorithm to find the greatest common divisors of the following pairs of polynomials:

(1) $x^2 + 1$ and $x^5 + 1$ in $\mathbb{Q}[x]$.
(2) $x^2 + 2x + 1$ and $x^3 + 2x^2 + 2$ in $\mathbb{F}_3[x]$.

Solution. (1)

$$\begin{aligned} x^5 + 1 &= (x^2 + 1)(x^3 - x) + (x + 1) \\ x^2 + 1 &= (x + 1)(x - 1) + 2 \\ x + 1 &= 2\left(\frac{x}{2} + \frac{1}{2}\right) + 0. \end{aligned}$$

So 2 is a gcd and 1 is **the** gcd.

(2)

$$\begin{aligned} x^3 + 2x^2 + 2 &= (x^2 + 2x + 1)x + (2x + 2) \\ x^2 + 2x + 1 &= (2x + 2)(2x + 2) + 0. \end{aligned}$$

So $2x + 2$ is a gcd and $x + 1$ is **the** gcd. $\square$

12.5. For the pair of polynomials $a(x)$ and $b(x)$ below, use the Euclidean algorithm to find polynomials $r(x)$ and $s(x)$ such that $a(x)r(x) + b(x)s(x)$ equals a greatest common divisor of $a(x)$ and $b(x)$:

(1) $x^2 + 1$ and $x^5 + 1$ in $\mathbb{Q}[x]$.
(2) $x^2 + 2x + 1$ and $x^3 + 2x^2 + 2$ in $\mathbb{F}_3[x]$.

Solution. We have already worked the Euclidean algorithm for both these pairs in the above exercise.

(1)

$$\begin{aligned} x &= (x^2 + 1) - (x + 1)(x - 1) \\ &= (x^2 + 1) - ((x^5 + 1) - (x^2 + 1)(x^3 - x))(x - 1) \\ &= (x^2 + 1)(x^4 - x^3 - x^2 + x + 1) - (x^5 + 1)(x - 1). \end{aligned}$$

(2)

$$2x + 2 = (x^3 + 2x^2 + 2) - (x^2 + 2x + 1)x.$$

$\square$

Exercise 13.2. Let K be a field with additive identity 0 and multiplicative identity 1. Write 2 for the sum $1+1$ and 4 for 2×2. Assume that $2 \neq 0$ in K, so that also $4 \neq 0$.

Solution. We will go item by item. **We may divide by 2 and 4 because, as established in the problem statement, neither of these are 0 and are therefore units.**

(1) For elements a and b of K, we see that
$$(x+a)^2 = x^2 + 2ax + a^2,$$
and so
$$\left(x + \frac{b}{2}\right)^2 = x^2 + bx + \frac{b^2}{4}.$$

(2) We may rewrite the equation
$$x^2 + bx + c = 0$$
$$x^2 + bx + \frac{b^2}{4} - \left(\frac{b^2}{4} - c\right) = 0$$
$$\left(x + \frac{b}{2}\right)^2 = \frac{b^2}{4} - c = \frac{b^2 - 4c}{4}.$$
Therefore we may solve either equation.

(3) If $b^2 - 4c = 0$, then it follows that
$$x^2 + bx + c = \left(x + \frac{b}{2}\right)^2,$$
and the only root of this polynomial is $x = -\frac{b}{2}$.

(4) If a is a solution to
$$x^2 + bx + c = 0,$$
then it follows from the above that
$$\left(2\left(a + \frac{b}{2}\right)\right)^2 = d.$$
Therefore, if d has no square root in K, then we cannot have a solution to the above equation, and it follows that $x^2 + bx + c$ is irreducible in $K[x]$.

(5) On the other hand, if d is nonzero and does have a square root $\sqrt{b^2 - 4c}$ in K, then we claim that $-\sqrt{b^2 - 4c}$ is the other distinct root. Were they the same then
$$0 = \sqrt{b^2 - 4c} - \sqrt{b^2 - 4c} = 2\sqrt{b^2 - 4c} = 2\sqrt{b^2 - 4c} \times \frac{1}{\sqrt{b^2 - 4c}} = 2,$$
which contradicts our initial hypotheses. With these two roots, we may then solve for
$$2\left(x + \frac{b}{2}\right) = \pm\sqrt{b^2 - 4c}$$
$$x + \frac{b}{2} = \pm\frac{\sqrt{b^2 - 4c}}{2}$$
$$x = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2}.$$

(6) Thus we have established the quadratic formula holds for any field K where $2 \neq 0$.

$\square$

Exercise 13.3. Prove that every complex number $a + bi$ has a complex square root. Deduce that every quadratic polynomial $f(x)$ in $\mathbb{C}[x]$ has a root in $\mathbb{C}$ and that $f(x)$ factors as the product of two degree-one polynomials in $\mathbb{C}[x]$.

Proof. We begin by noticing that every real number contains a root in $\mathbb{C}$, so we may assume that $b \neq 0$. We consider some $r + si$ and consider the requirements for it to be a square root:

$$(r + si)^2 = r^2 + 2rsi - s^2 = (r^2 - s^2) + 2rsi = a + bi.$$

Thus

$$a = r^2 - s^2 \text{ and } b = 2rs.$$

We note that from our second equation and our assumption that $b \neq 0$, we have that bother r and s are nonzero, so we may divide by them if necessary. We rewrite the second equation to see that

$$s = \frac{b}{2r},$$

plugging this into the first equation and then multiplying by r^2 we get

$$\begin{aligned} a &= r^2 - \frac{b^2}{4r} \\ ar^2 &= r^4 - \frac{b^2}{4} \\ 0 &= r^4 - ar^2 - \frac{b^2}{4}. \end{aligned}$$

Viewing this as a quadratic function in r^2, we may use the quadratic formula to see

$$r^2 = \frac{a}{2} \pm \frac{\sqrt{a^2 + b^2}}{2}.$$

The term inside the square root is positive, so our answer is a real number. Moreover, only one possible answer is positive. To ensure that r is a real number, we choose that solution and take the square root of both sides to get

$$r = \sqrt{\frac{a}{2} + \frac{\sqrt{a^2 + b^2}}{2}}.$$

As we have already expressed s in terms of b and r, we have found a square root of $a + bi$.

We now consider a degree-two polynomial $f(x)$, assuming it is monic (otherwise we just factor out a constant). Since $2 \neq 0$ and $4 \neq 0$, we may use our work in Exercise 13.2. If $f(x) = x^2 + bx + c$ and $b^2 - 4c = 0$ then we know we have a solution from the previous exercise. Otherwise, we have shown that $b^2 - 4c$ will always have a root in $\mathbb{C}$, then by the previous exercise there will be two solutions to $f(x)$ in $\mathbb{C}$. In either case we will have at least one solution $\alpha \in \mathbb{C}$, then $x - \alpha$ will divide $f(x)$ in $\mathbb{C}[x]$. As $f(x)$ was a quadratic, it follows that it factors as the product of two degree-one polynomials, completing our proof. □

Exercise 13.5. Use the fact that $\sqrt{n}$ is irrational for every positive integer n that is not the square of an integer to state a criterion describing which polynomials $x^2 + bx + c$ in $\mathbb{Z}[x]$ have roots in $\mathbb{Q}$ and which do not.

Solution. As $2 \neq 0$ and $4 \neq 0$ in $\mathbb{Q}$, we may use the result of Exercise 13.2 to conclude the roots of the polynomial will be of the form

$$x = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2}.$$

We conclude that we will have roots in $\mathbb{Q}$ if and only if $\sqrt{b^2 - 4c}$ is in $\mathbb{Q}$, ie. it is not irrational. But then from above, we know this will occur if and only if $b^2 - 4c$ is positive and is the square of some integer. □

Exercise 13.6.

(1) Show that 1 and 4 have square roots in $\mathbb{F}_5$, but 2 and 3 do not.
(2) Find the solutions to $x^2 + 2x + 2 = 0$ in $\mathbb{F}_5$ using the quadratic formula.
(3) Show that $x^2 + 2x + 3 = 0$ has no solutions in $\mathbb{F}_5$.
(4) Find all solutions to $x^2 + 3x + 1 = 0$.
(5) Find all solutions to $x^2 + 3x + 3 = 0$.

Solution. (1) We can just check all the elements of $\mathbb{F}_5$. We see that

$$0^2 = 0; 1^2 = 1; 2^2 = 4; 3^2 = 9 = 4; 4^2 = 16 = 1.$$

(2) From the quadratic formula we see

$$\begin{aligned} x &= -\frac{2}{2} \pm \frac{\sqrt{4-8}}{2} \\ &= -1 \pm \frac{\sqrt{1}}{2} \\ &= -1 \pm 3 \times 1 \\ &= -4 \text{ and } 2 \\ &= 1 \text{ and } 2. \end{aligned}$$

(3) Again using the quadratic formula, a solution will be of the form

$$x = -1 \pm \frac{\sqrt{-8}}{2}.$$

But we observe that $\sqrt{-8} = \sqrt{2}$, which we know from (1) does not exist in $\mathbb{F}_5$. We conclude from Exercise 13.2 that no solution exists in $\mathbb{F}_5$.

(4)

$$\begin{aligned} x &= -\frac{3}{2} \pm \frac{\sqrt{5}}{2} \\ &= -3 \times 3 \pm 3 \times 0 \\ &= 1. \end{aligned}$$

(5)

$$\begin{aligned} x &= -\frac{3}{2} \pm \frac{\sqrt{-3}}{2} \\ &= 1 \pm 3 \times \sqrt{2}. \end{aligned}$$

Again, $\sqrt{2}$ does not exist in $\mathbb{F}_5$, so the field contains no roots to this polynomial.

$\square$