Modern Algebra I Section 1 · Assignment 6

JOHN PERRY

Exercise 1. *(pg. 64 Warm Up a) Why is a linear polynomial in* $\mathbb{Q}[x]$ *always irreducible?*

Solution:

If the linear polynomial p was not irreducible, then there would be two polynomials $a, b \in \mathbb{Q}[x]$ such that $ab = p$ and $\deg a, \deg b \geq 1$. But then $1 = \deg p = \deg a + \deg b \geq 2$ by Theorem 4.1, which is a contradiction. $\Diamond$

Exercise 2. *(pg. 64 Warm Up b) Why is a polynomial of the form* $x^2 + a \in \mathbb{Q}[x]$, *where* $a > 0$, *always irreducible?*

Solution:

If the polynomial were not irreducible, then there would be two polynomials $a, b \in \mathbb{Q}[x]$ such that $x^2 + a = ab$ and $\deg a, \deg b \geq 1$. By Theorem 4.1, $\deg a = \deg b = 1$. So a and b are linear polynomials, say $px - q$ and $rx - s$ say, for $p, q, r, s \in \mathbb{Q}$. By the Root Theorem (4.3), that means $(q/p)^2 + a = 0$ and $(s/r)^2 + a = 0$. But it is easy to see that $b^2 + a \geq a > 0$ and $c^2 + a \geq a > 0$, a contradiction. $\Diamond$

Exercise 3. *(pg. 65 Warm Up c) Determine a factorization of* $x^4 - 5x^2 + 4$ *into irreducibles in* $\mathbb{Q}[x]$.

Solution:

Using the Rational Root Theorem (5.6), we know that all rational roots of the polynomial are of the form

$$\pm\frac{4}{1} = \pm 4 \quad \pm\frac{2}{1} = \pm 2 \quad \pm\frac{1}{1} = \pm 1.$$

If we apply the Root Theorem (4.3) and substitute these into the polynomial, we find that 1, -1, 2, and -2 are roots of the polynomial. Thus it factors as

$$(x+1)(x-1)(x+2)(x-2).$$

$\Diamond$

Exercise 4. *(pg. 65 Warm Up e) We know that 7 is an irreducible integer, but is 7 an irreducible polynomial?*

Solution:

The definition of an irreducible polynomial p includes the requirement that $\deg p > 0$. Since $\deg 7 = 0$, 7 is not an irreducible polynomial. $\Diamond$

Exercise 5. *(pg. 65 Warm Up g) Factor* $2x^3 + 7x^2 - 2x - 1$ *completely into irreducibles in* $\mathbb{Q}[x]$, *using Gauss' Lemma and the Root Theorem. Adjust your factorization (if necessary) so that all factors belong to* $\mathbb{Z}[x]$.

Solution:

We will also use the Rational Root Theorem (5.6)—I have no idea why the book didn't suggest that.

By the Rational Root Theorem, we know that all rational roots of the polynomial are of the form
$$\pm\frac{1}{2} \quad \pm\frac{1}{1}.$$
If we apply the Root Theorem (4.3) and substitute these into the polynomial, we find that 1/2 is the only rational root. We can use long division or synthetic division to show that
$$2x^3+7x^2-2x-1=\left(x-\frac{1}{2}\right)\left(2x^2+8x+2\right).$$
We can adjust the factorization using associates: factor the scalar 2 from the quadratic polynomial and distribute it into the linear polynomial. Thus
$$2x^3+7x^2-2x-1=(2x-1)\left(x^2+4x+1\right).$$
It is easy to use the Rational Root Theorem (5.6) and the Root Theorem (4.3) to show that this polynomial has no roots in $\mathbb{Z}$. By Gauss' Lemma (5.5) the quadratic polynomial is thus irreducible over $\mathbb{Q}$. $\Diamond$

Exercise 6. *(pg. 65 Exercise 1) Prove Theorem 5.1: A polynomial in $\mathbb{Q}[x]$ of degree greater than zero is either irreducible or the product of irreducibles.*

Solution:

Let $f\in\mathbb{Q}[x]$ be arbitrary, but fixed. Assume $\deg f>0$. We proceed by induction on $n=\deg f$.

For the inductive base, let $n=1$. Then f is irreducible by Exercise 1 (Warm Up a).

We have shown that the assertion is true for $n=1$.

Assume that $n>1$. For the inductive hypothesis, assume that every polynomial of degree i is either irreducible or the product of irreducibles, for all $i:1\leq i<n$.

If f is irreducible, then we are done.

Otherwise, we can write $f=pq$ for some $p,q\in\mathbb{Q}[x]$ where $\deg p,\deg q>0$. Recall from Theorem 4.1 that $\deg f=\deg p+\deg q$. Thus $\deg p=\deg f-\deg q<\deg f$. Similarly $\deg q<\deg f$. By the inductive hypothesis, p is either irreducible or the product of irreducibles. So we can write $p=p_1p_2\cdots p_r$ for some $r\in\mathbb{N}$ and for some irreducible $p_i\in\mathbb{Q}[x]$, for all $i:1\leq i\leq r$. By similar reasoning, we can write $q=q_1q_2\cdots q_s$ for some $s\in\mathbb{N}$ and for some irreducible $q_j\in\mathbb{Q}[x]$, for all $j:1\leq j\leq s$. Hence $f=\left(p_1p_2\cdots p_r\right)\left(q_1q_2\cdots q_s\right)$ where $r,s\in\mathbb{N}$ and p_i,q_j are irreducible for all $i:1\leq i\leq r$ and for all $j:1\leq j\leq s$. So f is the product of irreducibles.

We have shown that f is either irreducible or the product of irreducibles. Since n is arbitrary, this is true regardless of the degree of f. Since f is arbitrary, it is true for all $f\in\mathbb{Q}[x]$. $\Diamond$

Exercise 7. *(pg. 65 Exercise 4) Use Gauss's Lemma to determine which of the following are irreducible in $\mathbb{Q}[x]$:*
$$4x^3+x-2,\quad 3x^3-6x^2+x-2,\quad x^3+x^2+x-1.$$

Solution:

It is fairly easy to use factoring by grouping and see that the second polynomial is not irreducible in $\mathbb{Z}[x]$, since
$$\begin{aligned}3x^3-6x^2+x-2&=3x^2(x-2)+(x-2)\\&=(x-2)\left(3x^2-2\right).\end{aligned}$$

By Gauss's Lemma (5.5), the polynomial is also not irreducible in $\mathbb{Q}[x]$.

If the other two polynomials factor, then one of the factors is linear. (See the discussion in the text on page 62.) For the third polynomial, the Root Theorem (4.3) and the Rational Root Theorem (5.6) tell us that any linear factor has the form $x \pm 1$. Since neither 1 nor -1 are roots of the polynomial, it must be irreducible. For the first polynomial, the same theorems tell us that any linear factor has one of the forms $x \pm 1, x \pm 2, 2x \pm 1, 4x \pm 1$. Exhaustive inspection (via synthetic division) shows that none of these factors the polynomial, so it is also irreducible. $\Diamond$

Exercise 8. *(pg. 65 Exercise 5) Show that $x^4 + 2x^2 + 4$ is irreducible in $\mathbb{Q}[x]$.*

Solution:

For convenience, we denote the polynomial as p.

For any rational number a/b, then

$$(a/b)^4 + 2(a/b)^2 + 4 \geq 0 + 2 \cdot 0 + 4 = 4 > 0,$$

so p has no rational roots. By the Root Theorem (4.3), it has no linear factors in $\mathbb{Q}[x]$. This would exclude cubic factors as well, since if $p = qr$ for some $q, r \in \mathbb{Q}[x]$, and if $\deg q = 3$, then by Theorem 4.1 $\deg r = \deg p - \deg q = 4 - 3 = 1$. Since p has no linear factors, r cannot have degree 1, so q cannot have degree 3.

It remains to show that the polynomial has no quadratic factors. Assume to the contrary that $p = x^4 + 2x^2 + 4$ has quadratic factors $p = qr$. So $q = ax^2 + bx + c$ and $r = dx^2 + ex + f$ where $a, b, c, d, e, f \in \mathbb{Q}$. By Gauss' Lemma (5.5), we can assume $q, r \in \mathbb{Z}[x]$, so that $a, b, c, d, e, f \in \mathbb{Z}$. If we multiply q, r, we can collect like terms to obtain

$$p = qr = adx^4 + (ae + bd)x^3 + (af + be + cd)x^2 + (bf + ce)x + cf.$$

Two polynomials are equal iff their coefficients are equal, so

$$\begin{aligned} 1 &= ad \\ 0 &= ae + bd \\ 2 &= af + be + cd \\ 0 &= bf + ce \\ 4 &= cf. \end{aligned}$$

Since a, d are integers and $ad = 1$, it must be that $a = d = 1$. The system now becomes

$$\begin{aligned} 0 &= e + b \\ 2 &= f + be + c \\ 0 &= bf + ce \\ 4 &= cf. \end{aligned}$$

Observe that $b = -e$, so we have

$$2 = f - b^2 + c \tag{1}$$

$$0 = bf - bc \tag{2}$$

$$4 = cf. \tag{3}$$

From equation (2), we know that $b = 0$ or $f = c$. We consider two cases.

Case 1: If $f = c$, equation (3) tells us that $c = \pm 2$. Substituting this into equation (1) we see that $b^2 = 2$ or $b^2 = -4$, neither of which has an integer solution. Since b must be an integer, $f \neq c$.

Case 2: If $b = 0$, equation (1) tells us that $f + c = 2$, or $f = 2 - c$. Substituting into equation (3), we have

$$\begin{aligned} 4 &= c(2-c) \\ 4 &= 2c - c^2 \\ c^2 - 2c + 4 &= 0. \end{aligned}$$

The quadratic formula shows that this has no integer solution for c. Since c must be an integer, $b \neq 0$.

Neither case gives a solution for the coefficients. Hence f cannot factor as the product of two quadratic polynomials. Thus f is irreducible in $\mathbb{Z}[x]$. By Gauss' Lemma (5.5), f is irreducible in $\mathbb{Q}[x]$. $\lozenge$

Exercise 9. *(pg. 65 Exercise 7) Use the Rational Root Theorem 5.6 to factor*

$$2x^3 - 17x^2 - 10x + 9.$$

Solution:

By the rational root theorem, the only roots of the polynomial possible are

$$\pm\frac{9}{1} = \pm 9,\ \pm\frac{9}{2},\ \pm\frac{3}{1} = \pm 3,\ \pm\frac{3}{2},\ \pm\frac{1}{1} = \pm 1,\ \pm\frac{1}{2}.$$

Using substitution (or division), we find that the roots are 9, -1, and 1/2. The polynomial factors as

$$2\left(x - \frac{1}{2}\right)(x+1)(x-9).$$

(You may obtain a different expression; I'm trying to emphasize that $1/2$, -1, and 9 are all roots. $\lozenge$

Exercise 10. *(pg. 66 Exercise 8) Use the Rational Root Theorem 5.6 to argue that*

$$x^3 + x + 7$$

is irreducible over $\mathbb{Q}[x]$. *Use elementary calculus to argue that this polynomial does have exactly one* real *root.*

Solution:

If the polynomial factors as pq, then by Theorem 4.1, $3 = \deg p + \deg q$. Since this is a sum of integers, either $\deg p = 1$ or $\deg q = 1$. By the Rational Root Theorem (5.6), all roots would be of the form

$$\pm\frac{1}{1} = \pm 1, \quad \pm\frac{7}{1} = \pm 7.$$

However, none of those are roots. By the Root Theorem (4.3), the polynomial has no linear factors. Since the polynomial has no linear factors, $\deg p \neq 1$ and $\deg q \neq 1$. So the polynomial cannot factor. $\lozenge$

Exercise 11. *(pg. 66 Exercise 13) (a) Prove that the equation $a^2 = 2$ has no rational solution; that is, prove that $\sqrt{2}$ is irrational. (This part is a repeat of Exercise 2.14.)*

(b) Generalize part a, by proving that $a^n = 2$ has no rational solutions, for all positive integers $n \geq 2$.

Solution:

(a) If $a^2 = 2$ has a rational solution, then $a^2 - 2$ has a rational root. By the Rational Root Theorem (5.6), any such root has the form

$$\pm\frac{1}{1} = \pm 1, \qquad \pm\frac{2}{1} = \pm 2.$$

Since neither of those is a root of $a^2 - 2$, it follows that $a^2 = 2$ has no rational solution.

(b) If $a^n = 2$ has a rational solution, then $a^n - 2 = 0$ has a rational solution, so the polynomial $a^n - 2$ has a rational root. By the Rational Root Theorem (5.6), any such root is of the form

$$\pm\frac{1}{1} = \pm 1, \qquad \pm\frac{2}{1} = \pm 2.$$

Is either a root of $a^n - 2$? Substitute and see:

$$\begin{aligned}
1^n - 2 &= 1 - 2 = -1 \neq 0\\
2^n - 2 &\geq 2^2 - 2 = 2 \neq 0\\
(\text{if } n \text{ is even})\ (-1)^n - 2 &= 1 - 2 = -1 \neq 0\\
(-2)^n - 2 &\geq 2^2 - 2 = 2 \neq 0\\
(\text{if } n \text{ is odd})\ (-1)^n - 2 &= -1 - 2 = -3 \neq 0\\
(-2)^n - 2 &\leq -8 - 2 = -10 \neq 0.
\end{aligned}$$

Since none of the possibilities is a root of $a^n - 2$, it follows that $a^n = 2$ has no rational solution. ◊