ABSTRACT ALGEBRA AND FAMOUS IMPOSSIBILITIES EXERCISES

BRANDO MORA

Contents

Chapter 1: Algebraic Preliminaries

Section 1.1: Fields, Rings, and Vector Spaces.

Exercise 1.1.1.

(a) Which of the following are meaningful?
- (i) the vector space $\mathbb{C}$ over $\mathbb{R}$? Meaningful.
- (ii) the vector space $\mathbb{R}$ over $\mathbb{R}$? Meaningful.
- (iii) the vector space $\mathbb{R}$ over $\mathbb{C}$? Not.
- (iv) the vector space $\mathbb{C}$ over $\mathbb{Q}$? Meaningful.
- (v) the vector space $\mathbb{C}$ over $\mathbb{C}$? Meaningful.
- (vi) the vector space $\mathbb{Q}$ over $\mathbb{Q}$? Meaningful.
- (vii) the vector space $\mathbb{Q}$ over $\mathbb{R}$? Not.
- (viii) the vector space $\mathbb{Q}$ over $\mathbb{C}$? Not.

(b) Which of the above vector spaces have dimension 2? Write down a basis in each such case?
- (i) $[\mathbb{C} : \mathbb{R}] = 2$ meaning the dimension of the vector space $\mathbb{C}$ over $\mathbb{R}$ is 2. A valid basis is $B = \{1, i\}$ since any v in the vector space can be written $v = a_1 + a_1 i$, for $a_1, a_2 \in \mathbb{R}$.
- (ii) $[\mathbb{C} : \mathbb{Q}] = 2$. A valid basis is $B = \{1, i\}$ since any v in the vector space can be written $v = a_1 + a_1 i$, for $a_1, a_2 \in \mathbb{Q}$.

Exercise 1.1.2. How many subfields of $\mathbb{Q}$ are there? Justify your answer.
There is only 1 subfield of $\mathbb{Q}$, $\mathbb{Q}$ itself.

Proof. Let $S \subseteq \mathbb{Q}$ be arbitrary. Well since $\mathbb{Q} \subseteq \mathbb{C}$, then $S \subseteq \mathbb{C}$, but as Proposition 1.1.1 in the book states, $\mathbb{Q}$ is a subset of any subset of $\mathbb{C}$, so $\mathbb{Q} \subseteq S \subseteq \mathbb{Q}$ so $S = \mathbb{Q}$. □

Exercise 1.1.3.

(a) Is $\{(1 + i\sqrt{2}), (\sqrt{2} + 2i)\}$ a linearly independent subset of the vector space $\mathbb{C}$ over $\mathbb{R}$?
No. $(\sqrt{2}+2i) - \sqrt{2}(1+i\sqrt{2}) = 0$ which is not the trivial solution to where the linear combination of the vectors is 0, hence linearly dependent.
(b) Is $\{(1 + i\sqrt{2}), (\sqrt{2} + i)\}$ a linearly independent subset of $\mathbb{C}$ over $\mathbb{Q}$?
Yes, as $\sqrt{2} \notin \mathbb{Q}$ so the above argument does not apply for any constant.

Exercise 1.1.4.

(a) Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices with entries from $\mathbb{R}$. What are the natural vector space addition and scalar multiplication which make $M_2(\mathbb{R})$ a vector space over $\mathbb{R}$.
We can define matrix addition and scalar multiplication element-wise to make this set a vector space.
(b) Find a basis for $M_2(\mathbb{R})$
We can define our basis
$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$
(c) Let $M_2(\mathbb{C})$ be the set of all 2×2 matrices with entries from $\mathbb{C}$. Show that it is a vector space over $\mathbb{R}$ and find a basis for it. Is it also a vector space over $\mathbb{C}$?
We can see that $M_2(\mathbb{C})$ is a vector space over $\mathbb{R}$ since we defined the relevant operations of vector addition and scalar multiplication are defined element-wise and we know each of the vector space axioms hold for each individual element of the matrix between real and complex numbers. This results in the entire matrix obeying the vector space axioms and so the matrix is still a vector space over $\mathbb{R}$. Such a basis for $M_2(\mathbb{C})$ over $\mathbb{R}$ would be
$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & i \end{pmatrix} \right\}.$$
$M_2(\mathbb{C})$ over $\mathbb{C}$ would also be a vector space though its basis would have fewer elements (4 elements).

Exercise 1.1.5. Let $\mathbb{F} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

(a) Prove that $\mathbb{F}$ is a vector space over $\mathbb{Q}$ and write down a basis for it.
To show that $\mathbb{F}$ is a vector space over $\mathbb{Q}$ then we first show that $(\mathbb{F}, +)$ is an abelian group. Showing it is an abelian group follows directly from the properties of $\mathbb{Q}$ as a field. The rest of the vector space axioms like the associativity and distributive

properties as well as existence of multiplicative identity of the field applied to the vector space $\mathbb{F}$ also follow directly from $\mathbb{Q}$ being a field. So then all the vector space axioms can be satisfied and $\mathbb{F}$ is a vector space.

(b) *Prove that $\mathbb{F}$ is a field.
To show this we can first show that $(\mathbb{F}, +, \cdot)$ is a valid ring and then that $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group. We have already shown that $(\mathbb{F}, +)$ is an abelian group so to show that $(\mathbb{F}, +, \cdot)$ is a ring, we show closure and associativity of the multiplication operation as well as left and right distribution of the multiplication operation over the addition of two ring elements. Let $a = a_1 + a_2\sqrt{2}, b = b_1 + b_2\sqrt{2}, c = c_1 + c_2\sqrt{2} \in \mathbb{F}$.

$$ab = (a_1b_1 + 2a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbb{F} \qquad \text{Closure}$$

For associativity:

$$(ab)c = a_1b_1c_1 + 2a_1b_2c_2 + 2a_2b_1c_2 + 2a_2b_2c_1 + (a_2b_1c_1 + a_1b_2c_1 + a_1b_1c_2 + 2a_2b_2c_2)\sqrt{2}$$
$$c(ab) = a_1b_1c_1 + 2a_1b_2c_2 + 2a_2b_1c_2 + 2a_2b_2c_1 + (a_2b_1c_1 + a_1b_2c_1 + a_1b_1c_2 + 2a_2b_2c_2)\sqrt{2}$$
$$(ab)c = c(ab)$$

For the distributive property, keeping in mind that multiplication here is commutative which we will show shortly.

$$a(b + c) = a_1b_1 + 2a_2b_2 + a_1c_1 + 2a_2c_2 + (a_1b_2 + a_2b_1 + a_1c_2 + a_2c_1)\sqrt{2} = ab + ac$$
$$ab + ac = ba + ca = (b + c)a.$$

So then we only need to show that $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian multiplicative group. Everything for $(\mathbb{F} \setminus \{0\}, \cdot)$ is already proven or immediate except for the existence of an inverse for each element in the set. We can find this inverse element by letting $a = a_1 + a_2\sqrt{2}$ rationalizing $1/a$. Given $a \neq 0$, we then have

$$a^{-1} = \frac{a_1}{a_1^2 - 2a_2^2} - \frac{a_2}{a_1^2 - 2a_2^2}\sqrt{2}.$$

So then $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group and thus $\mathbb{F}$ is a field.

(c) Find the value of $[F : Q]$.
$[F : Q] = 2$ which can be seen by the basis set $B = \{1, \sqrt{2}\}$. No rational times 1 can give any multiple of $\sqrt{2}$.

Exercise 1.1.6. A ring R is said to be an *integral domain* if its multiplication is commutative, if there is an element 1 such that $1x = x1 = x$ for all $x \in R$, and if there are no zero-divisors.

(a) Is $\mathbb{Z}_4$ an integral domain?
No as $2 \in \mathbb{Z}_4$ and $2 \times 2 = 0 \in Z_4$, but $2 \neq 0$, so $\mathbb{Z}_4$ has zero-divisors.

(b) * For what $n \in \mathbb{N}$ is $\mathbb{Z}_n$ an integral domain?
Only for prime n is $\mathbb{Z}_n$ an integral domain. Since all $\mathbb{Z}_n$ have the multiplicative identity and commutative multiplication, then we only need to see which $\mathbb{Z}_n$ have zero divisors or not.

Proof. First we show, if n is composite then it is not an integral domain. This can be seen as n is composite so $n = ab$ with $1 < a, b < n$, and so $a, b \in \mathbb{Z}_n$. But then $a \cdot b \equiv ab = n \equiv 0$ in $\mathbb{Z}_n$ meaning $\mathbb{Z}_n$ has a zero divisor for composite n.

Now we show if n is prime that $\mathbb{Z}_n$ does not have a zero divisor. As n is prime then there are no natural numbers $1 < a, b < n$ such that $ab = n$. This does not immediately imply that $\mathbb{Z}_n$ has no zero divisors however as due to modular multiplication we have not ruled out that there could be an a, b such that $ab = kn$, for $k \in \mathbb{N}$ and so $a \cdot b \equiv ab = kn \equiv 0$ in $\mathbb{Z}_n$. This however is not possible. Assume for contradiction that $ab = kn$ with $a, b, k, n \in \mathbb{N}$ and $1 < a, b < n$. Then $k|ab$ and so $k|a$ or $k|b$. Without loss of generality, assume $k|a$. Then let $ck = a$ for some $c \in \mathbb{N}$. This implies $cb = n$, but this contradicts n being prime, so $ab \neq kn$, for some $k \in \mathbb{N}$. One could also argue using prime factorization and the Fundamental Theorem of Arithmetic. The result is the same, if n is prime then it has no zero divisors. □

Exercise 1.1.7. Let $\mathbb{E}$ be a subfield of a finite field $\mathbb{F}$ such that $[\mathbb{F} : \mathbb{E}] = n$, for some $n \in \mathbb{N}$. If $\mathbb{E}$ has m elements, for some $m \in \mathbb{N}$, how many elements does $\mathbb{F}$ have?
There are m^n vectors in the set $\mathbb{F}$. This can be seen by looking at the span of the vector space. Since $[\mathbb{F}, \mathbb{E}] = n$ then there are n basis vectors $\{b_1, b_2, ..., b_n\}$, together linearly independent such that each vector $v \in \mathbb{F}$, can be represented as a unique linear combination of these basis vectors. Such a generic linear combination using scalars $\lambda_1, \lambda_2, ..., \lambda_n$ from $\mathbb{E}$, looks like:

$$v = \lambda_1 b_1 + \lambda_2 b_2 + ... + \lambda_n b_n.$$

Since there are n places to choose the value for λ_i and m possible independent choices for each λ_i, then naturally there are m^n choices considering all λ_i together, and as each linear combination is a one-one correspondence to the vectors then there are m^n vectors in the space and so $\mathbb{F}$ has m^n elements.

Exercise 1.1.8.

(a) If $A, B,$ and C are finite fields with A a subfield of B and B a subfield of C, prove that $[C : A] = [C : B] \cdot [B : A]$. [Hint: Use the result of exercise 7.]

Proof. As seen in exercise 7, we established the formula that in situations of where Y is a subfield of X, then

$$|X| = |Y|^{[X:Y]}$$

which can be rearranged into

$$[X : Y] = \log_{|Y|}(|X|)$$

. Applying this here and using the change of base identity and reciprocal log identity gives us:

$$[C : A] = \log_{|A|}(|C|) = \log_{|B|}(|C|)\frac{1}{\log_{|B|}(|A|)} = \log_{|B|}(|C|)\log_{|A|}(|B|) = [C : B][B : A]$$

□

(b) If furthermore $[C : A]$ is a prime number, deduce that $B = C$ or $B = A$.
Based on the formula proved above $[C : A] = n$ being prime means that $[C : B]$ is either 1 or n and $[B : A]$ is the other (either n or 1 respectively). We proceed by cases for clarity.

Case 1: $[C : B] = 1$ and $[B : A] = n$. Here, then $\log_{|B|}(|C|) = 1$ and so $|B| = |C|$, but since $B \subseteq C$, then $B = C$.

Case 2: $[C : B] = n$ and $[B : A] = 1$. Here, then $\log_{|A|}(|B|) = 1$ and so $|A| = |B|$ but since $A \subseteq B$, then $A = B$.

Section 1.2 Polynomials.

Exercise 1.2.1. Give an example of an element of the polynomial ring $\mathbb{R}[X]$ which is not a member of $\mathbb{Q}[X]$.
Let us define $f(X) = \sqrt{2}$. This is a polynomial of degree 0. We have $f(X) \in \mathbb{R}[X]$ but $f(X) \notin \mathbb{Q}[X]$.

Exercise 1.2.2. In each of the following cases give a pair of nonzero polynomials $f(X), g(X) \in \mathbb{Q}[X]$ which satisfies the condition:

(i) $\deg(f(X) + g(X)) < \deg f(X) + \deg g(X)$
Let $f(X) = 1 + X$ and $g(X) = 1 - X$. Then the LHS is 0 and the RHS is 2.

(ii) $\deg(f(X) + g(X)) = \deg f(X) + \deg g(X)$
Let $f(X) = 1$ and let $g(X) = X^n$ for $n \geq 1$ ($n = 0$ would also be valid if the polynomial form's definition was a_0X^0 for the constant term in the polynomial, but the textbook did not define it like that). The LHS is n and the RHS is also n.

(iii) $\deg(f(X) + g(X))$ is undefined
Let $f(X) = -1$ and $g(X) = 1$. Then the sum of the two forms is the zero polynomial with undefined degree.

Exercise 1.2.3.

(a) Let $\mathbb{F}$ be a field. Verify that if $f(X)$ and $g(X)$ are nonzero polynomials in $\mathbb{F}[X]$ then $f(X)g(X) \neq 0$ and

$$\deg f(X)g(X) = \deg f(X) + \deg g(X)$$

Let $\deg f(X) = n$ and $\deg g(X) = m$. Then we can define $f(X) = a_nX^n + f_l(X)$ where $f_l(X)$ represents the lower order terms so $0 \leq \deg f_l(X) \leq n - 1$ or $f_l(X)$ is the zero polynomial. Similarly we can define $g(X) = b_n + g_l(X)$ where $g_l(X)$ represents lower order terms in the same manner. Now we calculate

$$\begin{aligned}
\deg f(X)g(X) &= \deg (a_nX^n + f_l(X))(b_nX^m + g_l(X)) \\
&= \deg (a_nb_nX^nX^m + a_nX^ng_l(X) + b_nX^mf_l(X) + f_l(X)g_l(X)) \\
&= n + m \\
&= \deg f(X) + \deg g(X).
\end{aligned}$$

Step 2 to step 3 can be explained by the fact that $g_l(X)$ has a max degree of $m-1$ and similarly $f_l(X)$ has a max degree of $n-1$ so the highest order term will only be $a_n b_n X^n X^m$ which has degree $n+m$. We can only conclude this because $a_n b_n \neq 0$ as a field has no zero divisors and $a_n, b_n \in \mathbb{F}$.

(b) Deduce that the ring $\mathbb{F}[X]$ is an integral domain. (See Exercises 1.1 #6 for the definition of integral domain.)
It is easily shown that $\mathbb{F}[X]$ has commutative multiplication and a multiplicative identity so we only check that $\mathbb{F}[X]$ has no zero divisors. Let $f(X), g(X) \in \mathbb{F}[X]\setminus\{0\}$ be arbitrary. Let's say deg $f(X) = n$ and deg $g(X) = m$, then from part (a) we have $f(X)g(X) = n+m$, which is defined. The zero polynomial has undefined degree, so $f(X)g(X)$ cannot be the zero polynomial, and so $\mathbb{F}[X]$ has no zero divisors.

(c) Is $\mathbb{Z}_6[X]$ an integral domain (Justify your answer).
No it is not an integral domain. Multiplication is commutative and there does exist a multiplicative identity but there is a zero divisor. Let $f(X) = 2$ and let $g(X) = 3$ then $f(X)g(X) = 0$.

Exercise 1.2.4. Let $f(X)$ denote the polynomial form over the ring $\mathbb{Z}_6$ given by $f(X) = X^3$. Find a polynomial form $g(X)$, with $f(X) \neq g(X)$, such that $f(X)$ and $g(X)$ determine the same polynomial function.
Let $g(X) = X$. Then, considering the arithmetic mod 6, we have

$$\begin{aligned} g(0) &= 0 & f(0) &\equiv 0^3 = 0 \equiv 0 \\ g(1) &= 1 & f(1) &\equiv 1^3 = 1 \equiv 1 \\ g(2) &= 2 & f(2) &\equiv 2^3 = 8 \equiv 2 \\ g(3) &= 3 & f(3) &\equiv 3^3 = 27 \equiv 3 \\ g(4) &= 4 & f(4) &\equiv 4^3 = 64 \equiv 4 \\ g(5) &= 5 & f(5) &\equiv 5^3 = 125 \equiv 5 \end{aligned}$$

Exercise 1.2.5.* Let R be any finite ring. Prove that there exist unequal polynomial forms $f(X)$ and $g(X)$ over R such that $f(X)$ and $g(X)$ determine the same polynomial function.
Let's say R has n elements in it. Since R is finite with n elements then there are only n^n unique functions, f following $f : R \to R$. But there are (countably) infinite polynomial forms over R (as the degree can become arbitrarily high) and each determines a polynomial function. So by the pigeonhole principle there must be exist some determined polynomial function, coming from at least two (in fact infinite) distinct polynomial forms.

Exercise 1.2.6. Let $\mathbb{F}$ be any subfield of the complex number field $\mathbb{F}$ and $f(X)$ and $g(X)$ be polynomial forms over the field $\mathbb{F}$. If the polynomial functions f and g are equal (that is, $f(x) = g(x)$, for all $x \in \mathbb{F}$), prove that the polynomial forms are equal (that is, $f(X) = g(X)$). [Hint. You may assume the well-known result that for any polynomial

function h of degree n, there are at most n complex numbers x such that $h(x) = 0$.] Let $f(X), g(X) \in \mathbb{F}[X]$ such that $f(x) = g(x)$ for all $x \in \mathbb{F}$. These have the form

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$$
$$g(X) = b_m X^m + b_{m-1} X^{m-1} + ... + b_1 X + b_0$$

for $n, m \in \mathbb{N}$ which determine

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + ... + b_1 x + b_0.$$

Note that a_{n+k} and b_{m+k} for $k \geq 1$ exist but are all 0. As seen earlier $\mathbb{Q} \subseteq \mathbb{F}$ so $f(x) = g(x)$ for all $x \in \mathbb{Q}$. But $\mathbb{Q}$ is dense in $\mathbb{R}$, so for any real number r we can create a sequence of rationals, (q_n) such that $\lim(q_n) = r$ and taking into account that polynomials are continuous everywhere then $f(q_n) = g(q_n)$ implies $\lim(f(q_n)) = \lim(g(q_n))$ which implies $g(r) = f(r)$. So we have that if $f(x) = g(x)$ for all $x \in \mathbb{F}$ then $f(x) = g(x)$ for all $x \in \mathbb{R}$. Now we show all coefficients a_i, b_i are equal. First, note $f(0) = g(0)$, so directly $a_0 = b_0$ as all other terms vanish. Now in the general ith case, take the ith derivative of both sides of $f(x) = g(x)$ (as polynomials are infinitely differentiable) and examine with input 0. Observe this looks like:

$$\begin{aligned} & f(x) = g(x) \\ \implies & f^{(i)}(0) = g^{(i)}(0) \\ \implies & (i!)a_i = (i!)b_i \\ \implies & a_i = b_i. \end{aligned}$$

So then we have each coefficient $a_i = b_i$ for all $i \geq 0$. As polynomial forms are defined by their coefficients so since these are equal then $g(X) = f(X)$.

Section 1.3 The Division Algorithm.

Exercise 1.3.1. Find the quotient and remainder when X^3+2X+1 is divided by $2X+1$ in $\mathbb{Q}[X]$.

$$\begin{array}{r}
\frac{1}{2}X^2-\frac{1}{4}X+\frac{9}{8} \\
2X+1\overline{)X^3+2X+1} \\
-(X^3+\frac{1}{2}X^2) \\
\hline
-\frac{1}{2}X^2+2X+1 \\
-(-\frac{1}{2}X^2-\frac{1}{4}X) \\
\hline
\frac{9}{4}X+1 \\
-(\frac{9}{4}X+\frac{9}{8}) \\
\hline
-\frac{1}{8}.
\end{array}$$

Based on our calculation above, we have that the quotient is $q(x)=\frac{X^2}{2}-\frac{X}{4}+\frac{9}{8}$, with remainder $r(x)=-\frac{1}{8}$, so that

$$X^3+2X+1=(2X+1)q(X)+r(X).$$

Exercise 1.3.2.

(a) Repeat Exercise 1 above with $\mathbb{Z}_7[X]$ replacing $\mathbb{Q}[X]$.
Note that 2^{-1} in this field is 4 as $2\cdot 4\equiv 8\equiv 1$.

$$\begin{array}{r}
4X^2-1X+5 \\
2X+1\overline{)X^3+2X+1} \\
-(X^3+4X^2) \\
\hline
-2X^2+2X+1 \\
-(-2X^2-1X) \\
\hline
3X+1 \\
-(3X+5) \\
\hline
-4.
\end{array}$$

Based on our calculation above, we have that the quotient is $q(x)=4X^2-1X+5$, with remainder $r(x)=-4$, so that

$$X^3+2X+1=(2X+1)q(X)+r(X).$$

(b) Write your answer to (a) without using any "-" signs.
That would become $q(X)=4X^2+6X+5$ and $r(X)=3$.

Exercise 1.3.3. Use the division algorithm to find the quotient and remainder when $X^3 + iX^2 + 3X + i$ is divided by $X^2 - i$ in $\mathbb{C}[X]$.

$$\begin{array}{rl} & X \quad + \quad i \\ X^2 - i) & \overline{X^3 \quad + \quad iX^2 \quad + \quad 3X \quad + \quad i} \\ & -(X^3 \qquad\qquad - iX) \\ & \overline{\qquad\qquad iX^2 + (3+i)X + i} \\ & \qquad -(iX^2 \qquad\qquad + 1) \\ & \qquad\qquad \overline{(3+i)X + (-1+i).} \end{array}$$

Based on our calculation above, we have that the quotient is $q(x) = X+i$, with remainder $r(x) = (3+i)X + (-1+i)$, so that

$$X^3 + iX^2 + 3X + i = (X^2 - i)q(X) + r(X).$$

Exercise 1.3.4. Use the division algorithm to find the quotient and remainder when $X^2 + \sqrt{2}X - 3$ is divided by $X - \sqrt{3}$ in $\mathbb{R}[X]$.

$$\begin{array}{rl} & X + (\sqrt{2} + \sqrt{3}) \\ X - \sqrt{3} & \overline{)X^2 + \sqrt{2}X - 3} \\ & -(X^2 - \sqrt{3}X) \\ & \overline{\qquad (\sqrt{2} + \sqrt{3})X - 3} \\ & \qquad -((\sqrt{2} + \sqrt{3})X - (\sqrt{2} + \sqrt{3})\sqrt{3}) \\ & \qquad \overline{\qquad\qquad\qquad\qquad \sqrt{6}} \end{array}$$

Based on our calculation above, we have that the quotient is $q(x) = X + (\sqrt{2} + \sqrt{3})$, with remainder $r(x) = \sqrt{6}$, so that

$$X^2 + \sqrt{2}X - 3 = (X - \sqrt{3})q(X) + r(X).$$

Exercise 1.3.5.* Write out the proof of Theorem 1.3.2 in detail. [Hint. Your proof may use mathematical induction.]

First we note that if $\deg g(X) > \deg f(X)$, we can choose $q(X) = 0$ and $r(X) = f(X)$, and the theorem holds, so we focus on the case where $\deg g(X) \leq \deg f(X)$. First we give and prove a small lemma.

Lemma. For a given $f(X), g(X) \in \mathbb{F}[X]$ with $g(X) \neq 0$ and $\deg g(X) \leq \deg f(X)$ then we can write $f(X)$ as

$$f(X) = g(X)q(X) + r(X),$$

where $q(X), r(X) \in \mathbb{F}[X]$ and $r(X) = 0$ or $\deg r(X) < \deg f(X)$ and $q(X)$ is a monic polynomial.

Proof of lemma. Let us define $f(X) = a_nX^n + ... + a_1X + a_0$ with $\deg f(X) = n$ and similarly define $g(X) = b_mX^m + ... + b_1X + b_0$, with $\deg g(X) = m$. Then we can choose $q(X)$ and $r(X)$ follows to be:

$$q(X) = \frac{a_n}{b_m}X^{n-m}$$
$$r(X) = f(X) - g(X)q(X).$$

We now show that this choice of $q(X)$ consequently has $r(X)$ satisfying the property that $\deg r(X) < \deg f(X)$.

$$r(X) = f(X) - g(X)q(X)$$
$$r(X) = (a_nX^n + ... + a_1X + a_0) - \frac{a_n}{b_m}X^{n-m}(b_mX^m + ... + b_1X + b_0)$$
$$r(X) = (a_nX^n + \ldots + a_1X + a_0) - \left(a_nX^n + \ldots + \frac{a_nb_1}{b_m}X^{n-m+1} + \frac{a_nb_0}{b_m}X^{n-m}\right)$$
$$r(X) = (a_{n-1}X^{n-1} + ... + a_1X + a_0) - \left(\frac{a_nb_{m-1}}{b_m}X^{n-1} + ... + \frac{a_nb_1}{b_m}X^{n-m+1} + \frac{a_nb_0}{b_m}X^{n-m}\right)$$

As we can see, the highest power on X in $r(X)$ is $n-1$, so even before considering terms cancelling out (which could lead to the case where $r(X) = 0$, $\deg r(X) < n = \deg f(X)$. Also $r(X), q(X) \in \mathbb{F}[X]$ due to the closure of the coefficients under the addition, subtraction, multiplication, and division operations guaranteed by the field properties. □

Now we are ready for the main proof of this exercise.

Proof. Let $\deg f(X) = n$ and $\deg g(X) = m$. Using the lemma just shown and proved, we can rewrite the given $f(X)$ and using $g(X)$ into

$$f(X) = g(X)q_1(X) + r_1(X),$$

where $q_1(X)$ is a monic polynomial and $r_1(X) = 0$ or $\deg r_1(X) < n$. Then we apply the same lemma again to $r_1(X)$ and $g(X)$ to produce

$$r_1(X) = g(X)q_2(X) + r_2(X).$$

with $\deg r_2(X) < \deg r_1(X) < n$. We inductively repeat this process until either $r_i(X) = 0$ or $\deg r_i(X) < m$ where i is the number of times we repeat this process. We know that eventually $r_i(X) = 0$ or $\deg r_i(X) < m$ since the inequality is strict and the $\deg r_i(X)$ is an integer with $\deg r_i(X) < \deg r_{i-1}(X) < ... < \deg r_1(X) < n$ so the degree of each successive remainder must be at least one lower than then previous. The minimum value for m is 1, so the degree of the remainder could always fall to 0 if needed and satisfy the

condition. That means through this process we have

$$\begin{aligned} f(X) &= g(X)q_1(X) + r_1(X) \\ r_1(X) &= g(X)q_2(X) + r_2(X) \\ &\vdots \\ r_{i-1}(X) &= g(X)q_i(X) + r_i(X) \end{aligned}$$

with $r_i(X) = 0$ or $\deg r_i(X) < \deg g(X)$. This allows us to write

$$\begin{aligned} f(X) &= g(X)q_1(X) + g(X)q_2(X) + ... + g(X)q_i(X) + r_i(X) \\ f(X) &= g(X)(q_1(X) + q_2(X) + ... + q_i(X)) + r_i(X) \\ f(X) &= g(X)q(X) + r_i(X) \end{aligned}$$

where we define $q(X) = q_1(X) + q_2(X) + ... + q_i(X)$. Now note that this is exactly what we were trying to prove since $r_i(X) = 0$ or $\deg r_i(X) < \deg g(X)$. □

Exercise 1.3.6.* Find an example which shows that Theorem 1.3.2 would be false if we assumed that $\mathbb{F}$ was only a ring rather than a field.
Let the ring be the integers, $\mathbb{Z}$ with the standard operations. So $f(X), g(X), q(x), r(X) \in \mathbb{Z}[X]$. Now let f be the polynomial $f(X) = 1$ and let $g(X) = 2$. Then based on the division theorem we have

$$1 = 2q(X) + r(X).$$

But the function $r(X)$ has to satisfy either $r(X) = 0$ or $\deg r(X) < \deg g(X)$, but $\deg g(X) = 0$, so $r(X)$ must be $r(X) = 0$. Then we have

$$1 = 2q(X),$$

in which it is obvious $q(X)$ must be $q(X) = \frac{1}{2}$, but $q(X) = \frac{1}{2} \notin \mathbb{Z}[X]$. So there do not always exist $q(X), r(X)$ which satisfies Theorem 1.3.2 if the field is allowed to be a ring.

Exercise 1.3.7.* In Theorem 1.3.2 if $\mathbb{F}$, $f(X)$ and $g(X)$ are given, show that $q(X)$ and $r(X)$ are uniquely determined.

Proof. Let

$$f(X) = g(X)q(X) + r(X).$$

where $q(X)$ and $r(X)$ are guaranteed to exist by Theorem 1.3.2. Suppose for the sake of contradiction that there exists another distinct remainder polynomial we call $r'(X)$ such that the theorem is still satisfied. Let us define $r'(X)$ in terms of $r(X)$ with a difference function such that

$$r'(X) = r(X) + d(X),$$

with $d(X) \neq 0$. Note that since $\deg r(X) < \deg g(X)$ then $\deg d(X) < \deg g(X)$ must be true so that $\deg r'(X) < \deg g(X)$. Note that we can modify our original equation to

use $r'(X)$ and maintain the equality by "adding 0" to get

$$f(X) = g(X)q(X) + r(X) + \left(d(X) - \frac{g(X)d(X)}{g(X)}\right)$$
$$f(X) = \left(g(X)q(X) - \frac{g(X)d(X)}{g(X)}\right) + (r(X) + d(X))$$
$$f(X) = g(X)\left(q(X) - \frac{d(X)}{g(X)}\right) + r'(X).$$

But note that since $\deg d(X) < \deg g(X)$, $\frac{d(X)}{g(X)}$ will have terms with negative exponents which are not allowed in $\mathbb{F}[X]$. So with a $r'(X) \neq r(X)$ we have found that $(q(X) - d(X)/g(X)) \notin \mathbb{F}[X]$ which contradicts our assumption that there is another remainder polynomial that satisfies the Theorem. So we conclude that $r(X)$ is uniquely determined. Using this we quickly show that $q(X)$ is uniquely determined. Let $q'(X)$ be another quotient polynomial satisfying the theorem not necessarily distinct from $q(X)$. Then we have

$$\begin{aligned} f(X) &= g(X)q(X) + r(X) \\ f(X) &= g(X)q'(X) + r(X) \\ \implies g(X)q(X) + r(X) &= g(X)q'(X) + r(X) \\ g(X)q(X) &= g(X)q'(X) \\ q(X) &= q'(X). \end{aligned}$$

So $q'(X) = q(X)$ and $q(X)$ is also uniquely determined. Then we have found both $q(X), r(X)$ to be uniquely determined by the theorem. □

Section 1.4 The Rational Roots Test.

Exercise 1.4.1. Let $p(X)$ be the element of $\mathbb{Q}[X]$ given by

$$p(X) = 2X^3 + 3X^2 + 2X + 3.$$

(a) Use the Rational Roots Test to find all possible rational zeros of p(X).
Based on the Rational Root Test, if $\beta = \frac{r}{s}$ is a rational root of $p(X)$ written in lowest terms then r is a factor of 3 and s is a factor of 2. So the possible values for r are $r = 1, -1, 3, -3$ and the possible values for s are $s = 1, -1, 2, -2$. Then the possible values for $\frac{r}{s}$ are $\frac{r}{s} = \pm 1, \pm\frac{1}{2}, \pm 3, \pm\frac{3}{2}$.
(b) Is -1 a zero of $p(X)$?
We plug in to check. $p(-1) = 2$ so -1 is not a zero.
(c) Is $-\frac{3}{2}$ a zero of $p(X)$?
We plug in to check. $p(-\frac{3}{2}) = 0$ so $-\frac{3}{2}$ is a zero of $p(X)$.

Exercise 1.4.2. Use the Rational Roots Test to prove that $\sqrt{5}$ is irrational.

Proof. Lets define $p(X) = X^2 - 5$. It is clear that $\sqrt{5}$ is a zero of $p(X)$. Also $p(X) \in \mathbb{Z}[X]$ so we can use the rational root test and if there are no rational roots then $\sqrt{5}$ is not a rational number. Rational root test tells us that the possible rational roots are $\pm 1, \pm 5$. However, none of these are actual zeros of $p(X)$, so $p(X)$ has no rational roots. Then $\sqrt{5}$ being a root means it is not rational. □

Exercise 1.4.3. Find a polynomial in $\mathbb{Q}[X]$ which has $\sqrt{2} + \sqrt{3}$ as a zero. Hence show that $\sqrt{2} + \sqrt{3}$ is irrational. [Hint. To obtain the polynomial, first let $\alpha = \sqrt{2} + \sqrt{3}$ and then square both sides.]
Observe the calculation to find our polynomial in $\mathbb{Q}[X]$.

$$\begin{aligned} \alpha &= \sqrt{2} + \sqrt{3} \\ \alpha^2 &= 2 + 2\sqrt{6} + 3 \\ (\alpha^2 - 5) &= 2\sqrt{6} \\ (\alpha^2 - 5)^2 &= 4 * 6 \\ \alpha^4 - 10\alpha^2 + 25 &= 24 \\ \alpha^4 - 10\alpha^2 + 1 &= 0. \end{aligned}$$

So then we have directly that for $p(X) = X^4 - 10X^2 + 1$, $p(\alpha) = 0$. Since $p(X) \in \mathbb{Z}[X]$, we can use the rational root test and see that the possible rational roots are ± 1. But $p(1) \neq 0$ and $p(-1) \neq 0$, so $p(X)$ has no rational roots and therefore $\alpha = \sqrt{2} + \sqrt{3}$ is irrational.

Exercise 1.4.4.

(a) Use the Rational Roots Test to prove that for each $m \in \mathbb{N}$, $\sqrt{m}$ is rational if and only if m is a perfect square.

Proof. We start by proving the forward implication. Assume that $\sqrt{m}$ is rational. Then $\sqrt{m}$ is a zero found by the rational root test on the polynomial

$$p(X) = X^2 - m.$$

The Rational Root Test applied to $p(X)$ tells us a rational solutions must be a factor of m. So $\sqrt{m}$, given to be a rational zero, is a factor of m and therefore an integer. This makes m equal to the square of integer, which is the definition of a perfect square.

The reverse implication is very direct. If m is a perfect square then it can be written $m = a^2$, for $a \in \mathbb{Z}$, so $\sqrt{m} = a$, implying $\sqrt{m} \in \mathbb{Z}$ and further $\sqrt{m} \in \mathbb{Q}$.

Thus both directions have been shown. □

(b) Let m and n be any positive integers. Prove that $\sqrt[n]{m}$ is a rational number if and only if it is an integer.

Proof. We start by proving the forward implication. Assume that $\sqrt[n]{m}$ is a rational number. Now we prove it must be an integer. Observe that $\sqrt[n]{m}$ is zero of the

polynomial $p(X) = X^n - m$ which has $p(X) \in \mathbb{Z}[X]$ so we can use the Rational Root Test. This test tells us any rational root must be a factor of m. But factors of m are all integers themselves so $\sqrt[n]{m}$ is an integer.

The reverse direction is immediate. Assume $\sqrt[n]{m}$ is an integer. Since all integers are also rational numbers then $\sqrt[n]{m}$ is a rational number.

Thus both directions have been shown. □

Exercise 1.4.5. If n is any positive integer, prove that $\sqrt{n} + \sqrt{n+1}$ and $\sqrt{n} - \sqrt{n+1}$ are irrational.

We will see both expressions are covered by the same polynomial. Let $\alpha = \sqrt{n} \pm \sqrt{n+1}$ and then we can construct the polynomial such that α is a zero of the the function. Observe

$$\begin{aligned}
\alpha &= \sqrt{n} \pm \sqrt{n+1} \\
\alpha^2 &= n \pm 2\sqrt{n(n+1)} + n + 1 \\
\alpha^2 - (2n+1) &= \pm 2\sqrt{n(n+1)} \\
(\alpha^2 - (2n+1))^2 &= 4n(n+1) \\
\alpha^4 - 2(2n+1)\alpha^2 + (2n+1)^2 &= 4n(n+1) \\
\alpha^4 - 2(2n+1)\alpha^2 + (2n+1)^2 - 4n(n+1) &= 0 \\
\alpha^4 - 2(2n+1)\alpha^2 + (4n^2 + 4n + 1) - (4n^2 + 4n) &= 0 \\
\alpha^4 - 2(2n+1)\alpha^2 + 1 &= 0,
\end{aligned}$$

so that we can choose $p(X) = X^4 - 2(2n+1)X^2 + 1$ and $p(\alpha) = 0$. Note that $p(X) \in \mathbb{Z}[X]$ so we can apply the rational root test which tells us all possible rational zeroes are ± 1. Plugging in, we get $p(-1) = p(1) = 3 - 4n$ which is clearly never zero for any positive integer n. So there are no rational zeroes to this polynomial and $\sqrt{n} + \sqrt{n+1}$ as well as $\sqrt{n} - \sqrt{n+1}$ is an irrational number for all positive integers n.

Exercise 1.4.6. Prove that $\sqrt{n+1} + \sqrt{n-1}$ is irrational, for every positive integer n.

Let $\alpha = \sqrt{n+1} - \sqrt{n-1}$ and then we can construct the polynomial such that α is a

zero of the the function. Observe

$$\begin{aligned}
\alpha &= \sqrt{n+1} - \sqrt{n-1} \\
\alpha^2 &= n+1-2\sqrt{(n+1)(n-1)} + n - 1 \\
\alpha^2 - (2n) &= -2\sqrt{(n+1)(n-1)} \\
(\alpha^2 - (2n))^2 &= 4(n+1)(n-1) \\
\alpha^4 - 2(2n)\alpha^2 + (2n)^2 &= 4(n+1)(n-1) \\
\alpha^4 - 4n\alpha^2 + (2n)^2 - 4(n+1)(n-1) &= 0 \\
\alpha^4 - 4n\alpha^2 + (4n^2) - (4n^2 - 4) &= 0 \\
\alpha^4 - 4n\alpha^2 + 4 &= 0,
\end{aligned}$$

so that we can choose $p(X) = X^4 - 4nX^2 + 4$ and $p(\alpha) = 0$. Note that $p(X) \in \mathbb{Z}[X]$ so we can apply the rational root test which tells us all possible rational zeroes are either ± 1 or ± 2. Plugging in we see

$$\begin{aligned}
p(-1) = p(1) &= 5 - 4n \\
p(-2) = p(2) &= 18 - 16n
\end{aligned}$$

with neither $5-4n$ or $18-16n$ ever being 0 for any positive n. So $p(X)$ has no rational zeroes and $\sqrt{n+1} - \sqrt{n-1}$ is irrational for all positive integer n.

Exercise 1.4.7.

(a)* Prove that $\sqrt{3} + \sqrt{5} + \sqrt{7}$ is irrational.

Observe the following derivation of the polynomial in for which the above is 0.

$$\begin{aligned}
x - \sqrt{3} &= \sqrt{5} + \sqrt{7} \\
\left(x - \sqrt{3}\right)^2 &= \left(\sqrt{5} + \sqrt{7}\right) \\
\left(x^2 - 2x\sqrt{3} + 3\right) &= 12 + 2\sqrt{35} \\
x^2 - 9 &= 2\left(\sqrt{35} + x\sqrt{3}\right) \\
x^4 - 18x^2 + 81 &= 4\left(35 + 3x^2 + 2x\sqrt{105}\right) \\
x^4 - 18x^2 + 81 &= 140 + 12x^2 + 8x\sqrt{105} \\
x^4 - 30x^2 - 59 &= 8x\sqrt{105} \\
\left(x^4 - 30x^2 - 59\right)^2 &= \left(8x\sqrt{105}\right)^2 \\
x^8 + 2\left(-30\right)x^6 + 2\left(-59\right)x^4 + 900x^4 + 2\left(-30\right)\left(-59\right)x^2 + \left(-59\right)^2 &= 64x^2\left(105\right) \\
x^8 + 2\left(-30\right)x^6 + 2\left(-59\right)x^4 + 900x^4 + 2\left(-30\right)\left(-59\right)x^2 - 64\left(105\right)x^2 + \left(-59\right)^2 &= 0.
\end{aligned}$$

So we can choose our polynomial to be

$$p(X) = x^8 + ... + (-59)^2,$$

where the middle terms can be seen above such that $p(X) \in \mathbb{Z}[x]$ and $p(\sqrt{3}+\sqrt{5}+\sqrt{7}) = 0$. Since $p(X) \in \mathbb{Z}[X]$ and 59 is a prime number then the rational root test can tell us that all possible rational roots are $\pm 1, \pm 59, \pm 59^2$. Note

$$\begin{aligned} p(-1) = p(1) &= 1024 \\ p(-59) = p(59) &> 10^{24} \\ p(-59^2) = p(59^2) &> 10^{48} \end{aligned}$$

so there are no rational roots of this polynomial and thus $\sqrt{3}+\sqrt{5}+\sqrt{7}$ is irrational.

(b)* Prove that $\sqrt{2}+\sqrt{3}+\sqrt{5}$ is irrational.

Observe the following derivation of the polynomial in for which the above is 0.

$$\begin{aligned} x &= \sqrt{2}+\sqrt{3}+\sqrt{5} \\ x-\sqrt{2} &= \sqrt{3}+\sqrt{5} \\ \left(x-\sqrt{2}\right)^2 &= \left(\sqrt{3}+\sqrt{5}\right)^2 \\ x^2-2x\sqrt{2}+2 &= 8+2\sqrt{15} \\ x^2-6 &= 2\left(\sqrt{15}+x\sqrt{2}\right) \\ \left(x^2-6\right)^2 &= \left(2\left(\sqrt{15}+x\sqrt{2}\right)\right)^2 \\ x^4-12x^2+36 &= 4\left(15+2x\sqrt{30}+2x^2\right) \\ x^4-12x^2+36 &= 60+8x\sqrt{30}+8x^2 \\ x^4-20x^2-24 &= 8x\sqrt{30} \\ \left(x^4-20x^2-24\right)^2 &= \left(8x\sqrt{30}\right)^2 \\ x^8+2\left(-20\right)x^6+2\left(-24\right)x^4+20^2x^4+2\left(-20\right)\left(-24\right)x^2+\left(-24\right)^2 &= 64\left(30\right)x^2 \\ x^8+2\left(-20\right)x^6+2\left(-24\right)x^4+20^2x^4+2\left(-20\right)\left(-24\right)x^2-64\left(30\right)x^2+\left(-24\right)^2 &= 0 \end{aligned}$$

So we can choose our polynomial to be

$$p(X) = x^8 + ... + (-24)^2,$$

where the middle terms can be seen above such that $p(X) \in \mathbb{Z}[x]$ and $p(\sqrt{2}+\sqrt{3}+\sqrt{5}) = 0$. Since $p(X) \in \mathbb{Z}[X]$ and $24^2 = 576$ has factors

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 32, 36, 48, 64, 72, 96, 144, 192, 288, \text{ and } 576,$$

then the rational root test can tell us that all possible rational roots are

$$\pm(1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 32, 36, 48, 64, 72, 96, 144, 192, 288, 576).$$

After using computer software to plug in these values, we see that none of them are a zero of our polynomial $p(X)$ and so there are no rational roots of this polynomial and thus $\sqrt{2}+\sqrt{3}+\sqrt{5}$ is irrational.

Exercise 1.4.8. Find a polynomial in $\mathbb{Q}[X]$ with α as a zero, where $\alpha = \sqrt[3]{4} - \sqrt[3]{2}$ and then deduce that $\alpha \notin \mathbb{Q}$ by applying the Rational Roots Test.
Observe the following derivation of the polynomial in for which the above is 0.

$$\begin{aligned}
x &= \sqrt[3]{4} - \sqrt[3]{2} \\
x &= 4^{\frac{1}{3}} - 2^{\frac{1}{3}} \\
x^3 &= \left(4^{\frac{1}{3}} - 2^{\frac{1}{3}}\right)^3 \\
x^3 &= 4 - 2 - 3\left(4^{\frac{2}{3}}\right)\left(2^{\frac{1}{3}}\right) + 3\left(4^{\frac{1}{3}}\right)\left(2^{\frac{2}{3}}\right) \\
x^3 &= 2 - 3\left(2^{\frac{4}{3}}\right)\left(2^{\frac{1}{3}}\right) + 3\left(2^{\frac{2}{3}}\right)\left(2^{\frac{2}{3}}\right) \\
x^3 &= 2 - 3\left(2^{\frac{5}{3}}\right) + 3\left(2^{\frac{4}{3}}\right) \\
x^3 - 2 &= -3\left(2^{\frac{5}{3}} - 2^{\frac{4}{3}}\right) \\
x^3 - 2 &= -3 \cdot 2^{\frac{3}{3}}\left(2^{\frac{2}{3}} - 2^{\frac{1}{3}}\right) \\
x^3 - 2 &= -3 \cdot 2^{\frac{3}{3}}\left(4^{\frac{1}{3}} - 2^{\frac{1}{3}}\right) \\
x^3 - 2 &= -3\,(2x) \\
x^3 + 6x - 2 &= 0
\end{aligned}$$

So we can choose our polynomial to be

$$p(X) = X^3 + 6X - 2,$$

and $p(\sqrt[3]{4} - \sqrt[3]{2}) = 0$. As $p(X) \in \mathbb{Z}[X]$ the rational root test tells us that any rational roots of $p(X)$ are a factor of -2 so possible roots are ± 1 and ± 2. Plugging these into $p(X)$, we see that none of them are a zero of the polynomial and so the polynomial has no rational roots and hence $\sqrt[3]{4} - \sqrt[3]{2}$ is irrational.

Exercise 1.4.9.

(1) Use the Fundamental Theorem of Arithmetic to prove that if r and s are natural numbers such that a prime p is a factor of the product rs, then p must be a factor of r or of s (or of both).

Proof. The fundamental theorem of arithmetic tells us that r and s each have a unique prime factorization (unless they are equal) so

$$\begin{aligned}
r &= p_1^{a_1} p_2^{a_2} ... p_n^{a_n} \\
s &= q_1^{b_1} q_2^{b_2} ... q_m^{b_m},
\end{aligned}$$

where q_i, p_i are prime and a_i, b_i are positive integers. Then we have our product is $rs = p_1^{a_1} p_2^{a_2} ... p_n^{a_n} q_1^{b_1} q_2^{b_2} ... q_m^{b_m}$. So if p is a factor of rs then it may come from the r prime factors or the s prime factors or both which is what we wanted. □

(2) Let r, s and b be positive integers such that r and s have no common factors except 1 and -1. Use the Fundamental Theorem of Arithmetic to show that if r is a factor of bs, then r must be a factor of b.

Proof. The fundamental theorem of arithmetic tells us that r, s, and b each have a unique prime factorization so

$$\begin{aligned} r &= p_{1_r}^{a_{1_r}} p_{2_r}^{a_{2_r}} ... p_{k_r}^{a_{k_r}} \\ s &= p_{1_s}^{a_{1_s}} p_{2_s}^{a_{2_s}} ... p_{k_s}^{a_{k_s}} \\ b &= p_{1_b}^{a_{1_b}} p_{2_b}^{a_{2_b}} ... p_{k_b}^{a_{k_b}}, \end{aligned}$$

where $p_{i_r}, p_{i_s}, p_{i_b}$ are prime and $a_{i_r}, a_{i_s}, a_{i_b}$ are positive integers. Given that r and s have no common factors then we know $p_{i_r} \neq p_{r_s}$ for all $1 \leq i_r \leq k_r$ and all $1 \leq i_s \leq k_s$. Then

$$bs = p_{1_b}^{a_{1_b}} p_{2_b}^{a_{2_b}} ... p_{k_b}^{a_{k_b}} p_{1_s}^{a_{1_s}} p_{2_s}^{a_{2_s}} ... p_{k_s}^{a_{k_s}}$$

and since r has no common factors with s then the factors of r in bs must come from b, so r must be a factor of b. □

(3) Let r, s, b, and m be positive integers such that r and s have no common factors except 1 and -1. Show that if r is a factor of bs^m, then r must be a factor of b. The fundamental theorem of arithmetic tells us that r, s, and b each have a unique prime factorization so

$$\begin{aligned} r &= p_{1_r}^{a_{1_r}} p_{2_r}^{a_{2_r}} ... p_{k_r}^{a_{k_r}} \\ s &= p_{1_s}^{a_{1_s}} p_{2_s}^{a_{2_s}} ... p_{k_s}^{a_{k_s}} \\ b &= p_{1_b}^{a_{1_b}} p_{2_b}^{a_{2_b}} ... p_{k_b}^{a_{k_b}}, \end{aligned}$$

where $p_{i_r}, p_{i_s}, p_{i_b}$ are prime and $a_{i_r}, a_{i_s}, a_{i_b}$ are positive integers. Given that r and s have no common factors then we know $p_{i_r} \neq p_{r_s}$ for all $1 \leq i_r \leq k_r$ and all $1 \leq i_s \leq k_s$. Then

$$\begin{aligned} bs^m &= p_{1_b}^{a_{1_b}} p_{2_b}^{a_{2_b}} ... p_{k_b}^{a_{k_b}} \left(p_{1_s}^{a_{1_s}} p_{2_s}^{a_{2_s}} ... p_{k_s}^{a_{k_s}} \right)^m \\ bs^m &= p_{1_b}^{a_{1_b}} p_{2_b}^{a_{2_b}} ... p_{k_b}^{a_{k_b}} p_{1_s}^{a_{1_s} m} p_{2_s}^{a_{2_s} m} ... p_{k_s}^{a_{k_s} m}. \end{aligned}$$

As only the exponents of the primes changed by raising s to the power of m, r still has no common factors with s^m, and so the conclusion is the same as the previous item above. Since r has common factors with s^m then the factors of r in bs^m must come from b, so r must be a factor of b.

Exercise 1.4.10. Use the Rational Roots Test to prove that the number $\sin\frac{\pi}{9}$ (that is, $\sin 20°$) is irrational. [Hint. First. use the formulae

$$\begin{aligned}\cos^2(\theta)+\sin^2(\theta)&=1,\\ \sin(\theta+\phi)&=\sin(\theta)\cos(\phi)+\cos(\theta)\sin(\phi),\\ \cos(\theta+\phi)&=\cos(\theta)\cos(\phi)-\sin(\theta)\sin(\phi)\end{aligned}$$

to write $\sin(3\theta)$ in terms of $\sin(\theta)$ (without any cos terms). Next, put $\theta=\frac{\pi}{9}$, $x=\sin(\theta)$, and use $\sin(\frac{\pi}{3})=\frac{\sqrt{3}}{2}$.]

$$\begin{aligned}\sin(3\theta)&=\sin(\theta+2\theta)\\ &=\sin(\theta)\cos(2\theta)+\cos(\theta)\sin(2\theta)\\ &=\sin(\theta)\left(\cos^2(\theta)-\sin^2(\theta)\right)+\cos(\theta)\left(2\sin(\theta)\cos(\theta)\right)\\ &=\sin(\theta)\left(1-2\sin^2(\theta)\right)+2\sin(\theta)\left(1-\sin^2(\theta)\right)\\ &=\sin(\theta)-2\left(\sin(\theta)\right)^3+2\sin(\theta)-2\left(\sin(\theta)\right)^3\\ &=3\sin(\theta)-4\left(\sin(\theta)\right)^3,\end{aligned}$$

Now if we let $\theta=\frac{\pi}{9}$ and $x=\sin(\theta)$ then we have

$$\begin{aligned}sin(3\theta)&=3sin(\theta)-4(\sin(\theta))^3\\ \frac{\sqrt{3}}{2}&=3x-4x^3\\ \left(\frac{\sqrt{3}}{2}\right)^2&=\left(3x-4x^3\right)^2\\ \frac{3}{4}&=9x^2-2\left(12x^4\right)+16x^6\\ 3&=36x^2-96x^4+64x^6\\ 0&=-3+36x^2-96x^4+64x^6\end{aligned}$$

so then $p(X)=64X^6-96X^{-4}+36X^2-3$ such that $p\left(\sin(\frac{\pi}{9})\right)=0$. Since $p(X)\in\mathbb{Z}[X]$ we can use the rational root test which tells us for a rational solution $\alpha=\frac{r}{s}$, r is a factor of -3 and s is a factor of 64. Note that the factors of 64 are $1,2,4,8,16,32,64$ so α could be $\alpha=\pm(1,\frac{1}{2},\frac{1}{4},\frac{1}{8},\frac{1}{16},\frac{1}{32},\frac{1}{64},3,\frac{3}{2},\frac{3}{4},\frac{3}{8},\frac{3}{16},\frac{3}{32},\frac{3}{64})$. After checking each of these possible rational solutions, we see that none of them are zeroes of the polynomial, $p(X)$ and so $p(X)$ has no rational solutions. Then we can conclude that $\sin(\frac{\pi}{9})$ is irrational.