4 The complex numbers

We will always be working within the set of complex numbers, **C**, i.e., the set {a + bi | a and b are real numbers} where $i = \sqrt{-1}$. Although they are in many ways similar, there is a profound difference between the the complex numbers and either the real numbers, the rational numbers, or the integers, which we will now explain.

In **Z**, there is a solution to 2X = 4, (since $\frac{4}{2} \in \mathbf{Z}$), but there is no solution to 3X = 4, (since $\frac{4}{3} \notin \mathbf{Z}$). In **Q**, there is a solution to 3X = 4, but there is no solution to $X^2 = 2$ (since $\sqrt{2} \notin \mathbf{Q}$). In **R**, there is a solution to $X^2 = 2$, but there is no solution to $X^2 = -2$ (since $\sqrt{-2} \notin \mathbf{R}$). In **C**, there is a solution to each of 2X = 4, 3X = 4, $X^2 = 2$, and $X^2 = -2$. In fact, the profound property of **C** is that in **C**, there is a solution to any polynomial equation f(X) = 0, with f(X) a nonconstant polynomial.

(4.1) The Fundamental Theorem of Algebra. Let $a_0, a_1, \ldots, a_n$ be complex numbers, with $n \geq 1$. Then there are complex numbers $b_1, b_2, \ldots, b_n$, such that
$a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = (X - b_1)(X - b_2) \ldots (X - b_n)$. In particular, the numbers $b_1, b_2, \ldots, b_n$ are all the solutions to the equation $a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = 0$.
(Thus, $b_1, b_2, \ldots, b_n$ are the roots of this polynomial.)

The proof of this fact is too involved to deal with here. The first rigorous proof was given by Gauss.

5 Number Fields

Definition: By a number field, or for short, a field, we will mean a subset of the complex numbers which is closed under addition, subtraction, multiplication, and division by nonzero elements, and which contains at least one nonzero number. That is, if F is a (number) field, then $F \subseteq \mathbf{C}$, and if $a,b \in F$, then $a + b$, $a - b$, ab, and a/b (if $b \neq 0$) are all in F, and $\exists\ c \in F$ with $c \neq 0$. ($\exists$ is shorthand for the phrase "there exists. $\forall$ is shorthand for "for all".)

(5.1) Exercises: a) Show that **Q**, **R**, and **C** are fields.

b) Show that $\{a + b\sqrt{2}) \mid a,b \in \mathbf{Q}\}$ is a field.

c) Show that if F is a (number) field, then $\mathbf{Q} \subseteq F$.

d) Show that if F and K are fields, then $F \cap K$ is also a field, but $F \cup K$ may not be a field.

Remark: The term "field" has a more general meaning then the special case we are studying; fields which are contained in the complex numbers (i.e., number fields). Galois Theory works for all fields, not just our number fields, but most of the main ideas of Galois Theory can be adequately illustrated in our special case.

(5.2) Exercise: If you are familiar with the integers modulo n, $\mathbf{Z}_n$, show that $\mathbf{Z}_n$ is always closed under addition, subtraction, and multiplicaion, but is only closed under division by nonzero elements when n is prime. (For n prime, $\mathbf{Z}_n$ is a field in the more general meaning mentioned above, but is not a number field, and so we will not be considering it here.)

6 Adjoining Elements

Suppose that F is a field, and that $\alpha \in \mathbf{C}$. Suppose we wish to find a field K which contains all of the elements of F as well as α. Suppose that a, b, c, and d are in F. Since K is to be closed under addition, subtraction, and multiplication, we see that K must contain such things as $\alpha + a$, $b\alpha$, $c\alpha^2 + a\alpha$, and $a\alpha^3 - b\alpha^2 + c\alpha + d$. In fact, in general, K must contain all polynomials $f(\alpha)$ where the coefficients of f come from F.

Definition: $F[\alpha] = \{f(\alpha) \mid f(X) \in F[X]\}$. (Here, F[X] is the set of all polynomials in the indeterminate having coefficients from F. For example, if a,b,c, and d are in F, then $X + a$, bX, $cX^2 + aX$, and $aX^3 - bX^2 + cX + d$ are all in F[X].)

(6.1) Exercise: Show that $F[\alpha]$ is closed under addition, subtraction, and multiplication, and that $F \subseteq F[\alpha]$, and

$\alpha \in F[\alpha]$.

(6.2) Exercise: Show that $Q[\sqrt{2}]$ is a field. (Hint: Relate this problem to Exercise (5.1)(b).)

Definition: $F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \mid f(X), g(X) \in F[X]$, and $g(\alpha) \neq 0\}$.

(6.3) Exercises: a) Show that $F(\alpha)$ is a field, with $F \subseteq F(\alpha)$ and $\alpha \in F(\alpha)$.

b) Show that $F(\alpha)$ equals the intersection of all those fields which contain α and all the elements of F.

c) Suppose that α and β are both complex numbers. Let $K = F(\alpha)$, and $L = F(\beta)$. Show that $K(\beta) = L(\alpha)$. In view of this fact, instead of writing either $K(\beta)$ or $L(\alpha)$, we write $F(\alpha, \beta)$. (This problem can be done in a brute force way, but try to use part (b) to find a clever way.)

d) Suppose that $a,b \in F$, with $b \neq 0$. Show that $F(\alpha) = F(a + b\alpha)$.

In general, given a field F and and element $\alpha \in \mathbf{C}$, $F[\alpha]$ may or may not be a field. For example, exercise (6.2) says that $\mathbf{Q}[\sqrt{2}]$ is a field. On the other hand, it can be shown that

$\frac{1}{\pi} \notin \mathbf{Q}[\pi]$, so that $\mathbf{Q}[\pi]$ is not closed under division by nonzero elements, and so is not a field. In this work, we will be interested in cases where $F[\alpha]$ is a field. The next two sections develop the ideas we need in order to understand when that occurs.

(6.4) Exercise: Show that $F[\alpha]$ is a field if and only if $F[\alpha] = F(\alpha)$.

7. Polynomials

Let F be a field. In this section, we will study the set of polynomials F[X]. For example, if F = $\mathbf{Q}$, then $f(X) = \frac{1}{2}X^2 - 3X + \frac{1}{3}$ and $g(X) = \frac{3}{4}X^3 - \frac{1}{2}X^2 + 6X - \frac{3}{2}$ are in $\mathbf{Q}$[X]. We know from high school how to add, subtract, and multiply two such polynomials in $\mathbf{Q}$[X], and we will simply say that for any field F, two polynomials in F[X] are added, subtracted, or multiplied according to the same rules used in the special case that F is $\mathbf{Q}$.

Now let us consider division. Given two polynomials in $\mathbf{Q}$[X], say f(X) and g(X) as above, we know how do do the long division $f(x)\,\overline{|\,g(x)}$. Thus

$$\begin{array}{r|rrrr}
 & \frac{3}{2}X & + 8 & & \\ \cline{2-5}
\frac{1}{2}X^2 - 3X + \frac{1}{3} & \frac{3}{4}X^3 & - \frac{1}{2}X^2 & + 6X & - \frac{3}{2} \\
 & \frac{3}{4}X^3 & - \frac{9}{2}X^2 & + \frac{1}{2}X & \\ \cline{2-5}
 & & 4X^2 & + \frac{11}{2}X & - \frac{3}{2} \\
 & & 4X^2 & - 24X & + \frac{8}{3} \\ \cline{3-5}
 & & & \frac{59}{2}X & - \frac{25}{6}
\end{array}$$

This calculation shows that

$$\frac{3}{4}X^3 - \frac{1}{2}X^2 + 6X - \frac{3}{2} = (\frac{3}{2}X + 8)(\frac{1}{2}X^2 - 3X + \frac{1}{3}) + (\frac{59}{2}X - \frac{25}{6}).$$

That is, $g(X) = (\frac{3}{2}X + 8)f(X) + (\frac{59}{2}X - \frac{25}{6})$,

or $g(X) = q(X)f(X) + r(X)$ with $q(X) = \frac{3}{2}X + 8$, and

$r(X) = \frac{59}{2}X - \frac{25}{6}$.

Notice that the process of long division guarantees that either $r(X) = 0$, or the degree of $r(X)$ will be less than the degree of $f(X)$. Of course there is nothing special about **Q** in the above, for in fact we could do long divison of polynomials over any field F. Therefore, we see the truth of the next theorem.

(7.1) Theorem: (The division algorithm for polynomials over a field.) Let F be a field, and let $f(X)$ and $g(X)$ be in $F[X]$, with $f(X) \neq 0$. Then there are $q(X)$ and $r(X)$ in $F[X]$, with $g(X) = q(X)f(X) + r(X)$, and with either $r(X) = 0$ or $\deg r(X) < \deg f(X)$.

(7.2) Exercise: If $g(X) \in F[X]$, and if $a \in F$ with $g(a) = 0$, show that $g(X) = (X - a)q(X)$ for some $q(X) \in F[X]$.

Remarks: 1) We note that if we are not in a field, the division algorithm may not hold. For instance, suppose we are working in $\mathbf{Z}[X]$, i.e., the set of polynomials with integral coefficients. We see that we cannot do the division $2X + 1 \,|\overline{\,3X^2 + 4X + 6}$, since $3/2 \notin \mathbf{Z}$.

2) Even in $\mathbf{Z}[X]$, we can do long division of polynomials if the divisor $h(X)$ is monic, that is if the leading coefficient of $h(X)$ is 1. For instance, we can do the division
$X^2 + 2X + 1 \,|\overline{\,5X^3 - 7X + 3}$.

3) Of course we can do long divison in $\mathbf{Z}$. Thus if we divide -27 by 5, we get -6 and a remainder of 3. That is, $-27 = (-6)(5) + 3$. In general, if a and b are integers with $b \neq 0$, then we can write $a = qb + r$, with $q,r \in \mathbf{Z}$ and with $0 \leq r < |b|$. This fact is called the division algorithm for integers.

4) It is common to either say that the zero polynomial has no degree, or to say it has degree minus infinity. (If we said the degree of the zero polynomial was 0, then the useful formula $\deg(f(X)g(X)) = \deg f(X) + \deg g(X)$ would fail when $f(X) = 0$ and $\deg g(X) \neq 0$. We do not want this formula to fail, and so we do not say that the degree of the zero polynomial is zero.) If the degree of the zero polynomial is defined to be minus infinity, then the conclusion of the division algorithm can be simplified by deleting the phrase "either $r(X) = 0$ or".

Definition: Let F be a field, and let $f(X) \in F[X]$, with $\deg f(X) > 0$. We call $f(X)$ irreducible (in $F[X]$) if it is impossible to write $f(X) = g(X)k(X)$ with $g(X), k(X) \in F[X]$ and with $g(X)$ and $k(X)$ both nonconstant.

In $\mathbf{Q}[X]$, since $X^2 - 1 = (X + 1)(X - 1)$, we see that $X^2 - 1$ is not irreducible. (We say it is reducible, or factorable.) On the other hand, $X^2 + 1$ is irreducible. Note that we could write $X^2 + 1 = (2)(\frac{1}{2}X^2 + \frac{1}{2})$. However, 2 is a constant polynomial, and so we ignore this factorization, and ones like it. Also note that $X^2 + 1$ is irreducible in $\mathbf{Q}[X]$, but is not irreducible in $\mathbf{C}[X]$, since in $\mathbf{C}[X]$ we may write $X^2 + 1 = (X + i)(X - i)$. Finally note that we have only defined irreducibility for polynomials of degree greater than zero. Therefore, we do not say that a constant polynomial, such as $f(X) = 3$, is irreducible.

Let us briefly discuss unique factorization. You know that any integer can be factored into prime integers in a unique way. For instance $12 = (2)(2)(3)$, and there is no other way of factoring 12 into primes. Of course, we could write $12 = (2)(3)(2)$, but that is just changing the order of the factors, which we agree to not count as a different way. We could also write $12 = (-2)(2)(-3)$, but again this change is so trivial we agree to not count it as different. (Yes, -2 is considered a prime.) We call $(2)(2)(3)$ the unique prime (or irreducible) factorization of 12.

We now consider factoring polynomials in F[X], with F a field. For example, let F = **Q**. In **Q**[X], we see that $X^4 + 3X^3 + 2X^2 - 3X - 3 = (X - 1)(X + 1)(X^2 + 3X + 3)$, and that each of these factors is irreducible. It is a true fact that there is no other way of factoring $X^4 + 3X^3 + 2X^2 - 3X - 3$ into irreducible polynomials in **Q**[X]. Of course, we again agree to not count trivial changes, such as changing the order of the factors, as different. We also agree not to count a change like $X^4 + 3X^3 + 2X^2 - 3X - 3 = (2X - 2)(\frac{1}{2}X + \frac{1}{2})(X^2 + 3X + 3)$ as diferent, since all we did was multiply the factor X - 1 by 2, and at the same time divide the factor X + 1 by 2. With this understanding of what we mean by the word unique, we state (without proof) a theorem.

(7.3) Theorem: If F is a field, then any polynomial in F[X] can be factored into irreducible polynomials in a unique way.

Definition: Let F be a field, and let f(X) and g(X) be two nonzero polynomials in F[X]. We say that $h(X) \in F[X]$ is a greatest common divisor of f(X) and g(X) if h(X) divides both f(X) and g(X), and if no polynomial with degree larger than the degree of h(X) divides both f(X) and g(X).

Consider two polynomials in $\mathbf{Q}[X]$, such as $f(X) = X^4 + 3X^3 + 2X^2 - 3X - 3$, and $g(X) = X^5 - X^3 - X^2 + 1$. Since the irreducible factorizations of $f(X)$ and $g(X)$ are $f(X) = X^4 + 3X^3 + 2X^2 - 3X - 3 = (X - 1)(X + 1)(X^2 + 3X + 3)$, and $g(X) = X^5 - X^3 - X^2 + 1 = (X - 1)^2(X + 1)(X^2 + X + 1)$, we see that $(X - 1)(X + 1)$ is a greatest common divisor of $f(X)$ and $g(X)$. Of course since $f(X) = (\frac{1}{7})(X - 1)(7X + 7)(X^2 + 3X + 3)$ and

$g(X) = (\frac{1}{7})(X - 1)^2(7X + 7)(X^2 + X + 1)$, we see that

$(X - 1)(7X + 7)$ is also a greatest common divisor of $f(X)$ and $g(X)$. Obviously, $(X - 1)(7X + 7)$ is just $7(X - 1)(X + 1)$. It is a true fact that any greatest common divisor of $f(X)$ and $g(X)$ will look like $c(X - 1)(X + 1)$ for some nonzero constant c. (Notice why we defined "a greatest common divisor" instead of "the greatest common divisor".)

(7.4) Theorem: Let F be a field, and let $f(X)$ and $g(X)$ be two nonzero polynomials in $F[X]$. Then $f(X)$ and $g(X)$ have a greatest common divisor. Also, if $h(X)$ is a greatest common divisor of $f(X)$ and $g(X)$, then the set of all greatest common divisors of $f(X)$ and $g(X)$ is $\{ch(X) \mid c \text{ is a nonzero constant in } F\}$.

Remark: Theorems (7.3) and (7.4) might look rather obvious to you. However, there are interesting mathematical structures in which both of these theorems fail. Although we choose not to give the proofs of Theorems (7.3) and (7.4), both of them do require nontrivial proofs.

We come to an important result.

(7.5) Theorem: Let $f(X)$ and $g(X)$ be two nonzero polynomials in $F[X]$. Suppose that $h(X) \in F[X]$ is a greatest common divisor of $f(X)$ and $g(X)$. Then there are polynomials $u(X)$ and $v(X)$ in $F[X]$, such that $u(X)f(X) + v(X)g(X) = h(X)$.

Before giving the proof of Theorem (7.5), we will give a concrete example of how the argument goes. For this, let $f(X) = X^3 + X^2 - 4X - 4$, and $g(X) = X^4 - 2X^2 + 1$. By doing some long division, we find that

(eq. 1) $X^4 - 2X^2 + 1 = (X - 1)(X^3 + X^2 - 4X - 4) + (3X^2 - 3)$.

That is,

(eq. 1′) $g(X) = q_1(X)f(X) + r_1(X)$,

with $q_1(X) = X - 1$, and $r_1(X) = 3X^2 - 3$.

We now divide $f(X)$ by $r_1(X)$, and find that

(eq. 2) $X^3 + X^2 - 4X - 4 = (\frac{1}{3}X + \frac{1}{3})(3X^2 - 3) + (-3X - 3)$.

That is,

(eq 2′) $f(X) = q_2(X)r_1(X) + r_2(X)$,

with $q_2(X) = \frac{1}{3}X + \frac{1}{3}$ and $r_2(X) = -3X - 3$.

We now repeat the process, dividing $3X^2 - 3$ by $-3X - 3$, getting

(eq. 3) $3X^2 - 3 = (-X + 1)(-3X - 3) + 0$.

That is,

(eq. 3′) $r_1(X) = q_3(X)r_2(X) + r_3(X)$,

with $q_3(X) = -X + 1$ and $r_3(X) = 0$.

Had $r_3(X)$ not been zero, we would have done another step, writing $r_2(X) = q_4(X)r_3(X) + r_4(X)$, and so on. However, since $r_3(X)$ is 0, we stop, and organize the above information.

First, we note that $r_2(X) = -3X - 3$ is a greatest common divisor of $f(X)$ and $g(X)$. To see this directly, just note that the irreducible factorizations of $f(X)$ and $g(X)$ are $f(X) = (X + 1)(X + 2)(X - 2)$ and $g(X) = (X + 1)^2(X - 1)^2$. Thus $h(X) = X + 1$ is a greatest common divisor of $f(X)$ and $g(X)$, and of course so is $r_2(X) = -3(X + 1)$. Therefore, the above process has found a greatest common divisor of $f(X)$ and $g(X)$. (In the proof that follows, we shall show that this always works.)

Now we rewrite the above equations. From (eq. 2′), we get

(eq. 4) $r_2(X) = f(X) - q_2(X)r_1(X)$.

From (eq. 1′) we get

(eq. 5) $r_1(X) = g(X) - q_1(X)f(X)$.

Substituting (eq. 5) into (eq. 4) gives us

(eq. 6) $r_2(X) = (1 + q_2(X)q_1(X))f(X) + (-q_2(X))g(X)$, which becomes

(eq. 7) $X + 1 = -\frac{1}{3}r_2(x) = -\frac{1}{3}(1 + q_2(X)q_1(X))f(X) + (-\frac{1}{3})(-q_2(X))g(X)$.

Let $u(X) = -\frac{1}{3}(1 + q_2(X)q_1(X)$ and $v(X) = -\frac{1}{3}(-q_2(X))$.

Then $X + 1 = u(X)f(X) + v(X)g(X)$. Substituting the above values for $q_1(X)$ and $q_2(X)$ into $u(X)$ and $v(X)$, we see that $(-\frac{1}{9}X^2 - \frac{2}{9})f(X) + (\frac{1}{9}X + \frac{1}{9})g(X) = X + 1$, which you can verify by direct calculation. This illustrates the truth of Theorem (7.5).

The process we gave in the preceding example is called the Euler algorithm. The proof of Theorem (7.5) (which follows) is simply a theoretical presentation of that process, in which we incorporate the use of induction (since in general, we do not know how many steps the process might take).

(7.6) Exercise: Let $f(X) = X^3 - 7X + 7$ and $g(X) = X^4 - 2X^3 - 7X^2 + 8X + 12$. Use the Euler algorithm to find a greatest common divisor $h(X)$ of $f(X)$ and $g(X)$, and an expression $h(X) = u(X)f(X) + v(X)g(X)$.

(7.7) Exercise: Using that we can do long division in $\mathbf{Z}$, use the Euler algorithm to find the greatest common divisor d of 612 and 1785, and write $d = u(612) + v(1785)$ for some u and v in $\mathbf{Z}$.

Proof of Theorem (7.5): We may suppose that $\deg g(X) \geq \deg f(X)$. Since $h(X)$ divides $f(X)$, $\deg f(X) \geq \deg h(X)$. We will induct on $\deg f(X) - \deg h(X)$. To start the induction, suppose that $\deg f(X) - \deg h(X) = 0$. Since $h(X)$ divides $f(X)$, we can write $f(X) = h(X)p(X)$ for some $p(X) \in F(X)$. (Note that $p(X) \neq 0$, since $f(X) \neq 0$.) Thus $\deg f(X) = \deg h(X) + \deg p(X)$. However, we are supposing that $\deg f(X) = \deg h(X)$, and so we see that $\deg p(X) = 0$. Therefore, $p(X)$ is a constant. Write $p(X) = c \in F$. We have $f(X) = ch(X)$, and so $(\frac{1}{c})f(X) + (0)g(X) = h(X)$. Therefore, the result is true with $u(X) = \frac{1}{c}$ and $v(X) = 0$.

Now suppose the result holds whenever

$\deg f(X) - \deg h(X)$ is less than some $n > 0$. We will inductively show that it is true when $\deg f(X) - \deg h(X) = n$. By the division algorithm, we know $g(X) = q(X)f(X) + r(X)$, with $q(X)$ and $r(X)$ in $F[X]$, and with either $\deg r(X) < \deg f(X)$, or with $r(X) = 0$.. We will here treat the case that $r(X) \neq 0$, and leave the case $r(X) = 0$ to an exercise. We claim that $h(X)$ is a greatest common divisor of $f(X)$ and $r(X)$. Since $h(X)$ divides both $f(X)$ and $g(X)$, it clearly divides $g(X) - q(X)f(X) = r(X)$, and so $h(X)$ divides both $r(X)$ and $f(X)$. We must now show that no polynomial of higher degree can divide both $f(X)$ and $r(X)$. Suppose that $k(X)$ divides both $f(X)$ and $r(X)$. (We want to show that $\deg k(X) \leq \deg h(X)$.) Now $k(X)$ also divides $q(X)f(X) + r(X) = g(X)$, and so $k(X)$ divides both $f(X)$ and $g(X)$. Since $h(X)$ is a greatest common divisor of $f(X)$ and $g(X)$, by definition, we have $\deg k(X) \leq \deg h(X)$. Thus, $h(X)$ is a greatest common divisor of $f(X)$ and $r(X)$, as claimed. Since $\deg r(X) < \deg f(X)$, we have $\deg r(X) - \deg h(X) <$ $\deg f(X) - \deg h(X) = n$. By induction, the result holds for the two polynomials $f(X)$ and $r(X)$, and their greatest common divisor $h(X)$. Therefore, there are polynomials $u'(X)$ and $v'(X)$ in $F[X]$, with $u'(X)f(X) + v'(X)r(X) = h(X)$. From earlier, we have $r(X) = g(X) - q(X)f(X)$, which upon substitution gives $(u'(X) - q(X))f(X) + v'(X)g(X) = h(X)$. This shows that the result holds for $u(X) = u'(X) - q(X)$ and $v(X) = v'(X)$. By induction, we are done.

(7.8) Exercise: Complete the proof of Theorem (7.5) by treating the case that $r(X) = 0$. (Hint: If $r(X) = 0$, then $f(X)$ divides both $f(X)$ and $g(X)$, and so deg $f(X) \leq$ deg $h(X)$.)

(7.9) Corollary: Let $f(X)$ and $g(X)$ he nonzero polynomials in $F[X]$, and suppose that $f(X)$ is irreducible in $F[X]$, and is not a factor of $g(X)$. Then there are polynomials $u(X), v(X) \in F[X]$ such that $u(X)f(X) + v(X)g(X) = 1$.

Proof: By Theorem (7.5), we must only show that 1 is a greatest common divisor of $f(X)$ and $g(X)$. Clearly 1 divides both $f(X)$ and $g(X)$, and so we must show no polynomial with higher degree can divide both $f(X)$ and $g(X)$. Thus suppose that $k(X)$ divides both $f(X)$ and $g(X)$. We want to show that deg $k(X) \leq$ deg $1 = 0$. Thus, we want to show that $k(X)$ is really just a constant. Suppose, to the contrary, that $k(X)$ is not a constant. (We will derive a contradiction.) Since $k(X)$ divides $f(X)$, we can write $f(X) = p(X)k(X)$. (Since $f(X) \neq 0$, we have $p(X) \neq 0$.) Since $f(X)$ is ireducible, $p(X)$ and $k(X)$ cannot both be nonconstants. Since $k(X)$ is nonconstant, we must have that $p(X)$ is a constant. Write $p(X) = c \in F$. Thus $f(X) = ck(X)$, so that $k(X) = \frac{1}{c}f(X)$. Now since $k(X)$ divides $g(X)$, write $g(X) = k(X)q(X) = \frac{1}{c}f(X)q(X)$. This contradicts that $f(X)$ is not a factor of $g(X)$, and completes the proof.

We need the following result. We will state it, and then develop a small bit of machinery needed to prove it. (The machinery should look familiar to anyone who knows calculus.)

(7.10) Theorem: Let $f(X) \in F[X]$ be irreducible and have degree n. Then $f(X)$ has n distinct roots in $\mathbf{C}$.

Definition: If $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in F[X]$, then define $f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1$.

(7.11) Exercise:** Show that the standard rules of differentiation work, i.e., $(f + g)' = f' + g'$, $(cf)' = cf'$ (for $c \in F$), and $(fg)' = f'g + fg'$. (Hint: the first two are easy. Use them to reduce the third to just showing $(X^nX^m)' = (X^n)'X^m + X^n(X^m)'$.)

Proof of Theorem (7.10): It follows from the Fundamental Theorem of Algebra, (4.1), that $f(X)$ factors completely in $\mathbf{C}[X]$, so that we may write $f(X) = (X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n)$ with the α_i in $\mathbf{C}$. (Here, we have made the harmless assumption that $f(X)$ is monic.) We must show that no two of the α_i are equal. Suppose to the contrary that two of them were equal (so that $n \geq 2$). By renumbering, we may assume that $\alpha_1 = \alpha_2$. Thus $f(X) = (X - \alpha_1)^2g(X)$, where $g(X) = (X - \alpha_3) \ldots (X - \alpha_n)$. By the preceding exercise, we see that

$f'(X) = 2(X - \alpha_1)g(X) + (X - \alpha_1)^2 g'(X)$. This shows that α_1 is a root of $f'(X)$. However, since $f(X) \in F[X]$, the definition of $f'(X)$ shows that $f'(X) \in F[X]$. Now $f(X)$ is irreducible in $F[X]$, and clearly $f(X)$ is not a factor of $f'(X)$, since $\deg f(X) > \deg f'(X)$. Corollary (7.9) says that we may write $u(X)f(X) + v(X)f'(X) = 1$ for some $u(X)$, $v(X)$ in $F[X]$. However, α_1 is a root of both $f(X)$ and $f'(X)$, and so $1 = u(\alpha_1)f(\alpha_1) + v(\alpha_1)f'(\alpha_1) = u(\alpha_1)(0) + v(\alpha_1)(0) = 0$. This contradiction completes the proof.

We state the next result without proof. Its proof can be found in most advanced undergraduate, or first year graduate level algebra texts.

(7.12) Lemma: (Gauss' Lemma) If $f(X)$ is a nonconstant polynomial in $\mathbf{Z}[X]$, and if it impossible to factor $f(X)$ as $f(X) = g(X)h(X)$ with $g(X)$ and $h(X)$ nonconstant polynomials in $\mathbf{Z}[X]$, then $f(X)$ is irreducible in $\mathbf{Q}[X]$.

(7.13) Theorem: (Eisenstein's Criterion) Suppose that $f(X) = a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \in \mathbf{Z}[X]$. Suppose that p is a prime integer, and p divides each of $a_{n-1}, a_{n-2}, \dots, a_0$, but p does not divide a_n, and p^2 does not divide a_0. Then $f(X)$ is irreducible in $\mathbf{Q}[X]$.

Proof: By Gauss' Lemma, it is enough to show that we cannot write $f(X) = g(X)h(X)$ with $g(X)$ and $h(X)$ nonconstant polynomials in $\mathbf{Z}[X]$. Suppose to the contrary that there is such a factorization, say $f(X) = (b_m X^m + \ldots + b_0)(c_k X^k + \ldots + c_0)$, with both factors in $\mathbf{Z}[X]$, and with $k,m \geq 1$. Since $a_0 = b_0 c_0$ and p divides a_0 but p^2 does not divide a_0, we see that p must divide exactly one of b_0 or c_0. It does no harm to assume that p divides b_0 but not c_0. Now $a_1 = b_0 c_1 + b_1 c_0$. From this, we see that p divides b_1. Now $a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$. From this, we see that p divides b_2. Iterating, we see that p divides all the b_i. In particular, p divides b_m. Thus p divides $b_m c_k = a_n$. This is a contradiction.

(7.13) Exercises: a) Show that $2X^3 + 9X^2 + 6X + 15$ is irreducible in $\mathbf{Q}[X]$.

b) Show that $X^4 + X^3 + X^2 + X + 1$ is irreducible in $\mathbf{Q}[X]$. (Hint: Do a change of variable, by letting $X = Y + 1$.)

c) Show that $15Y^3 + 6Y^2 + 9Y + 2$ is irreducible in $\mathbf{Q}[Y]$. (Hint: Find a useful change of variable.)

8. Algebraic Elements

Definition: Let F be a field, and let $\alpha \in \mathbf{C}$. Suppose that there is a nonzero $f(X) \in F[X]$, such that $f(\alpha) = 0$. Then we say that α is algebraic over F. Otherwise, we say that α is transcendental over F.

Examples: Consider $\sqrt{2}$. Let $f(X) = X^2 - 2$. Since $f(X) \in \mathbf{Q}[X]$ and $f(\sqrt{2}) = 0$, $\sqrt{2}$ is algebraic over $\mathbf{Q}$. Consider $i = \sqrt{-1}$. Let $g(X) = X^2 + 1$. Since $g(X) \in \mathbf{Q}[X]$ and $g(i) = 0$, i is algebraic over $\mathbf{Q}$. In the middle of the nineteenth century, it was shown that there are numbers which are not algebraic over $\mathbf{Q}$, i.e., are transcendental over $\mathbf{Q}$. For example, it can be shown that e and π are transcendental over $\mathbf{Q}$. Also, it is known that e^{π} is transcendental over $\mathbf{Q}$, but it is not known whether or not π^e is transcendental over $\mathbf{Q}$. Such questions tend to be very challanging, and await fresh new minds to attack them.

If α is algebraic over F, then by definition, there is a nonzero $f(X) \in F[X]$ with $f(\alpha) = 0$. In fact, there will be many such f(X). Of all such f(X), consider one whose degree is as small as possible. Furthermore, if the leading coefficient of that f(X) is c, it does no harm to divide through by c and thus assume that f(X) is monic (i.e., has leading coefficient 1). This f(X) is particularly important, and so we name it.

Definition: Suppose that α is algebraic over F. The minimal polynomial of α over F is the monic polynomial $f(X) \in F[X]$ such that $f(\alpha) = 0$, and such that if $g(X) \in F[X]$ with $g(X) \neq 0$ and with $\deg g(X) < \deg f(X)$, then $g(\alpha) \neq 0$.

For example, $\sqrt{2}$ is a root of $X^3 - 2X$ and of $X^4 - 4X^2 + 4$, as well as many other polynomials. However, $X^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbf{Q}$. (Of course, $\sqrt{2}$ is a root of $3X^2 - 6$, but this polynomial is not monic, and so is not the minimal polynomial of $\sqrt{2}$ over $\mathbf{Q}$.) Similarly, $X^2 + 1$ is the minimal polynomial of i over $\mathbf{Q}$.

(8.1) Exercises: a) Is 2 algebraic over $\mathbf{Q}$? If so, what is its minimal polynomial over $\mathbf{Q}$?

b) Note that $\omega = -\frac{1}{2} + (\frac{\sqrt{3}}{2})i$ is a root of $X^3 - 1$, and so is algebraic over $\mathbf{Q}$. What is the minimal polynomial of ω over $\mathbf{Q}$?

c) Note that $\alpha = \sqrt[3]{2}$ is a root of $X^3 - 2$, and so is algebraic over $\mathbf{Q}$. What is the minimal polynomial of α over $\mathbf{Q}$?

d) With ω and α as in parts (b) and (c), notice that $\alpha\omega$ is a root of $X^3 - 2$. What is the minimal polynomial of $\alpha\omega$ over $\mathbf{Q}$?

In the name "the minimal polynomial of α over F", the use of the word "the" implies that there is only one polynomial f(X) which satisfies the preceding definition. Indeed, this is the case. Proving it is the first of the next series of very important exercises.

(8.2) Exercises: Assume that α is algebraic over F, and let f(X) be the minimal polynomial of α over F.

a) Show that f(X) is unique. That is, suppose that f(X) and h(X) both satisfy the definition of the minimal polynomial of α over F, and show that f(X) = h(X).

b) Show that f(X) is irreducible in F[X]. (Some people call f(X) the minimal irreducible polynomial of α over F, or the irreducible polynomial of α over F.)

c) Let $g(X) \in F[X]$. Show that $g(\alpha) = 0$ if and only if f(X) is a factor of g(X). (Hint: Use the division algorithm.)

d) Suppose that h(X) is a monic irreducible polynomial in F[X], and $h(\alpha) = 0$. Show that h(X) = f(X).

e) Let $g(X) \in F[X]$, and suppose that $g(\alpha) \neq 0$. Show that there is a polynomial $v(X) \in F[X]$ such that $v(\alpha)g(\alpha) = 1$. (Hint: Use Corollary (7.9).)

(8.3) Theorem: Let α be algebraic over the field F. Then $F[\alpha] = F(\alpha)$, so that $F[\alpha]$ is a field.

Proof: From the definitions, we immediately see that $F[\alpha] \subseteq F(\alpha)$. Now choose an arbitrary element $\beta \in F(\alpha)$. We must show that $\beta \in F[\alpha]$. Since $\beta \in F(\alpha)$, we can write $\beta = \frac{f(\alpha)}{g(\alpha)}$, where f(X) and g(X) are in F[X], and $g(\alpha) \neq 0$. Thus $\beta = f(\alpha)(\frac{1}{g(\alpha)})$. Since $f(\alpha) \in F[\alpha]$, and since $F[\alpha]$ is closed under multiplication, it will suffice to show that $\frac{1}{g(\alpha)} \in F[\alpha]$.

However, Exercise (8.2)(e) tells us that there is a polynomial $v(X) \in F[X]$, such that $v(\alpha)g(\alpha) = 1$. Since $v(\alpha) \in F[\alpha]$ and since $\frac{1}{g(\alpha)} = v(\alpha)$, we have $\frac{1}{g(\alpha)} \in F[\alpha]$, as desired. This shows that $F[\alpha] = F(\alpha)$, and we already know that $F(\alpha)$ is a field.

(8.4) Exercises: a) Let $\beta = \sqrt[3]{2}$. Let $g(X) = 3X^2 + 4X + 5 \in \mathbf{Q}[X]$, so that $g(\beta) = 3\beta^2 + 4\beta + 5 \in Q[\beta]$. Since β is algebraic over Q, Theorem (8.3) tells us that $Q[\beta]$ is a field. Thus $\frac{1}{g(\beta)} \in \mathbf{Q}[\beta]$, and so $\frac{1}{g(\beta)} = v(\beta)$ for some polynomial $v(X) \in \mathbf{Q}[X]$. Find such a $v(X)$. (Hint: Use the Euler algorithm, and the fact that $X^3 - 2$ is the minimal polynomial of β over **Q** to find the $v(X)$ mentioned in Exercise (8.2)(e).)

b) Show that if $F[\alpha] = F(\alpha)$, then α is algebraic over F. (Hint: For $\alpha \neq 0$, note that $\frac{1}{\alpha} \in F(\alpha)$.)

c)* If α is algebraic over F, show that $F[\alpha] = F[-\alpha]$.

d)* If α is algebraic over F, show that $F[\alpha^2] \subseteq F[\alpha]$. Show by example that for some α, $F[\alpha^2] = F[\alpha]$, while for other α, $F[\alpha^2] \neq F[\alpha]$.

e)* If α and β are both algebraic over F, show that $F[\alpha][\beta] = F[\beta][\alpha] = \{f(\alpha, \beta) \mid f(X, Y)$ is a polynomial in two indeterminates X and Y, with coefficients from F. (We simply write $F[\alpha, \beta]$ instead of $F[\alpha][\beta]$).

f)* Show that $\mathbf{Q}[\sqrt{2}, \sqrt{2}\, i] = \mathbf{Q}[\sqrt{2}, i]$.

g)* Show that $\mathbf{Q}[\sqrt{2} + \sqrt{3}, \sqrt{3}] = \mathbf{Q}[\sqrt{2}, \sqrt{3}]$.

Definition: If $\alpha_1, \alpha_2, \ldots \alpha_n$ are all algebraic over F, by $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ we will mean $F[\alpha_1][\alpha_2]\cdots[\alpha_n]$

(8.5) Exercises: a) Show that $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ a field, and is the intersection of all fields which contain F and α_i for $1 \leq i \leq n$.
b) Show that $F[\alpha_1, \alpha_2, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) \mid f(X_1, \ldots, X_n)$ is a polynomial in the n indeterminates $X_1, \ldots, X_n$, with coefficients in F.
c) Show that $F[\alpha_1, \alpha_2, \ldots, \alpha_n] = F[\beta_1, \beta_2, \ldots, \beta_n]$, where $\beta_1, \beta_2, \ldots, \beta_n$ is any permutation of $\alpha_1, \alpha_2, \ldots, \alpha_n$.
d) Show that if $\gamma_1, \gamma_2, \ldots, \gamma_n$ are in $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ and if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are in $F[\gamma_1, \gamma_2, \ldots, \gamma_n]$, then $F[\alpha_1, \alpha_2, \ldots, \alpha_n] = F[\gamma_1, \gamma_2, \ldots, \gamma_n]$.

If α is algebraic over F, then Theorem (8.3) shows us that the field $F(\alpha)$ is equal to $F[\alpha]$. Now every element in $F[\alpha]$ has the form $f(\alpha)$ for some polynomial $f(X) \in F[X]$. However, we can say much more, and shall do so after the next set of exercises.

(8.6) Exercises: Assume that α is algebraic over F, and let $f(X)$ be the minimal polynomial of α over F.
a) Show that any element in $F[\alpha]$ can be written as $r(\alpha)$, where $r(X) \in F[X]$ is either the zero polynomial or has degree less than the degree of $f(X)$. (Hint : Use the division algorithm).

b) Suppose that $r(X)$ and $r'(X)$ are two polynomials in $F[X]$. both having degree less than the degree of $f(X)$ (here, allowing either $r(X)$ or $r'(X)$ to be the zero polynomial). Suppose also that $r(\alpha) = r'(\alpha)$. Show that $r(X) = r'(X)$.

(8.7) Theorem: Suppose that α is algebraic over F, and that the minimal polynomial of α over F has degree n. Then every element in $F[\alpha]$ can be expressed in a unique way as $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$ with $a_i \in F$ for $0 \leq i \leq n-1$.

Proof: We refer to the preceding exercises. let $\beta \in F[\alpha]$. By part (a), there is an $r(X) \in F[X]$ with $r(\alpha) = \beta$ and either $r(X) = 0$ or $\deg r(X) < n$. Write $r(X) = a_{n-1}X^{n-1} + \ldots + a_1X + a_0$. (Here, some, or even all of the a_i might be 0.) Thus $\beta = r(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, and so β has the desired form. To show the uniqueness of this representation, suppose that we could also write $\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$. Let $r'(X) = b_{n-1}X^{n-1} + \ldots + b_1X + b_0$. Thus $r'(\alpha) = \beta = r(\alpha)$. By part (b), $r(X) = r'(X)$, and so $a_i = b_i$ for $0 \leq i \leq n-1$.

As examples of the use of the above theorem, we see that $Q[\sqrt[3]{2}] = \{a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2 \mid a,b,c \in Q\}$, while $Q[-\frac{1}{2} + (\frac{\sqrt{3}}{2})i] = \{a + b(-\frac{1}{2} + (\frac{\sqrt{3}}{2})i) \mid a,b \in Q\}$, (using Exercise (8.1)(b)).

(8.8) Exercise: Show that $Q[-\frac{1}{2} + \frac{\sqrt{3}}{2}i] = Q[\sqrt{3}\ i]$.