is the solution $a_0 = a_1 = a_2 = 0$. We now proceed to show this. If a solution exists in rationals, by clearing of denominators we can show that a solution exists where a_0, a_1, a_2 are integers. Thus we may assume that a_0, a_1, a_2 are integers satisfying (1). We now assert that we may assume that a_0, a_1, a_2 have no common divisor other than 1, for if $a_0 = b_0 d$, $a_1 = b_1 d$, and $a_2 = b_2 d$, where d is their greatest common divisor, then substituting in (1) we obtain $d^3(b_0^3 + 2b_1^3 + 4b_2^3) = d^3(6b_0b_1b_2)$, and so $b_0^3 + 2b_1^3 + 4b_2^3 = 6b_0b_1b_2$. The problem has thus been reduced to proving that (1) has no solutions in integers which are relatively prime. But then (1) implies that a_0^3 is even, so that a_0 is even; substituting $a_0 = 2\alpha_0$ in (1) gives us $4\alpha_0^3 + a_1^3 + 2a_2^3 = 6\alpha_0 a_1 a_2$. Thus a_1^3, and so, a_1 is even; $a_1 = 2\alpha_1$. Substituting in (1) we obtain $2\alpha_0^3 + 4\alpha_1^3 + a_2^3 = 6\alpha_0\alpha_1 a_2$. Thus a_2^3, and so a_2, is even! But then a_0, a_1, a_2 have 2 as a common factor! This contradicts that they are relatively prime, and we have proved that the equation $a_0^3 + 2a_1^3 + 4a_2^3 = 6a_0a_1a_2$ has no rational solution other than $a_0 = a_1 = a_2 = 0$. Therefore we can solve for α, β, γ and $F[x]/(x^3 - 2)$ is seen, directly, to be a field.

Problems

1. Find the greatest common divisor of the following polynomials over F, the field of rational numbers:
   (a) $x^3 - 6x^2 + x + 4$ and $x^5 - 6x + 1$.
   (b) $x^2 + 1$ and $x^6 + x^3 + x + 1$.
2. Prove that
   (a) $x^2 + x + 1$ is irreducible over F, the field of integers mod 2.
   (b) $x^2 + 1$ is irreducible over the integers mod 7.
   (c) $x^3 - 9$ is irreducible over the integers mod 31.
   (d) $x^3 - 9$ is reducible over the integers mod 11.
3. Let F, K be two fields $F \subset K$ and suppose $f(x), g(x) \in F[x]$ are relatively prime in $F[x]$. Prove that they are relatively prime in $K[x]$.
4. (a) Prove that $x^2 + 1$ is irreducible over the field F of integers mod 11 and prove directly that $F[x]/(x^2 + 1)$ is a field having 121 elements.
   (b) Prove that $x^2 + x + 4$ is irreducible over F, the field of integers mod 11 and prove directly that $F[x]/(x^2 + x + 4)$ is a field having 121 elements.
   *(c) Prove that the fields of part (a) and part (b) are isomorphic.
5. Let F be the field of real numbers. Prove that $F[x]/(x^2 + 1)$ is a field isomorphic to the field of complex numbers.

*6. Define the *derivative* $f'(x)$ of the polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

as

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}.$$

Prove that if $f(x) \in F[x]$, where F is the field of rational numbers, then $f(x)$ is divisible by the square of a polynomial if and only if $f(x)$ and $f'(x)$ have a greatest common divisor $d(x)$ of positive degree.

7. If $f(x)$ is in $F[x]$, where F is the field of integers mod p, p a prime, and $f(x)$ is irreducible over F of degree n prove that $F[x]/(f(x))$ is a field with p^n elements.

3.10 Polynomials over the Rational Field

We specialize the general discussion to that of polynomials whose coefficients are rational numbers. Most of the time the coefficients will actually be integers. For such polynomials we shall be concerned with their irreducibility.

DEFINITION The polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$, where the $a_0, a_1, a_2, \ldots, a_n$ are integers is said to be *primitive* if the greatest common divisor of $a_0, a_1, \ldots, a_n$ is 1.

LEMMA 3.10.1 *If $f(x)$ and $g(x)$ are primitive polynomials, then $f(x)g(x)$ is a primitive polynomial.*

Proof. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$. Suppose that the lemma was false; then all the coefficients of $f(x)g(x)$ would be divisible by some integer larger than 1, hence by some prime number p. Since $f(x)$ is primitive, p does not divide some coefficient a_i. Let a_j be the first coefficient of $f(x)$ which p does not divide. Similarly let b_k be the first coefficient of $g(x)$ which p does not divide. In $f(x)g(x)$ the coefficient of x^{j+k}, c_{j+k}, is

$$c_{j+k} = a_jb_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0) + (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0b_{j+k}). \quad (1)$$

Now by our choice of b_k, $p \mid b_{k-1}, b_{k-2}, \ldots$ so that $p \mid (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0)$. Similarly, by our choice of a_j, $p \mid a_{j-1}, a_{j-2}, \ldots$ so that $p \mid (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0b_{k+j})$. By assumption, $p \mid c_{j+k}$. Thus by (1), $p \mid a_jb_k$, which is nonsense since $p \nmid a_j$ and $p \nmid b_k$. This proves the lemma.

DEFINITION The *content* of the polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$, where the a's are integers, is the greatest common divisor of the integers $a_0, a_1, \ldots, a_n$.

Clearly, given any polynomial $p(x)$ with integer coefficients it can be written as $p(x) = dq(x)$ where d is the content of $p(x)$ and where $q(x)$ is a primitive polynomial.