Section IV.23. Factorizations of Polynomials over a Field

Note. Our experience with classical algebra tells us that finding the zeros of a polynomial is equivalent to factoring the polynomial. We find that the same holds in $F[x]$ when F is a field (as we see in the "Factor Theorem"). In this section, we consider factoring polynomials and conditions under which a polynomial cannot be factored (when it is "irreducible"; you see this in Calculus 2 [MATH 1920] when considering partial fraction decompositions , as in my online notes on Section 8.4 Integration of Rational Functions by Partial Fractions).

Theorem 23.1. Division Algorithm for $F[x]$.
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2x^2 + b_1x + b_0$ be in $F[x]$, with a_n and b_m both nonzero and $m > 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$.

Note. We illustrate the Division Algorithm for $F[x]$ on the next page.

Exercise 23.4. For $f(x) = x^4 + 5x^3 + 8x^2$ and $g(x) = 5x^2 + 10x + 2$ in $\mathbb{Z}_{11}[x]$, find $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$.

Solution. We can perform simple long division (but in $\mathbb{Z}_{11}$):

$$\begin{array}{r|rrrrrrrr}
 & & & & & 9x^2 & + & 5x & + & 10 \\
\hline
5x^2 + 10x + 2 & x^4 & + & 5x^3 & + & 8x^2 & & & & \\
 & x^4 & + & 2x^3 & + & 7x^2 & & & & \\
\hline
 & & & 3x^3 & + & x^2 & & & & \\
 & & & 3x^3 & + & 6x^2 & + & 10x & & \\
\hline
 & & & & & 6x^2 & + & x & & \\
 & & & & & 6x^2 & + & x & + & 9 \\
\hline
 & & & & & & & & & 2
\end{array}$$

So $q(x) = 9x^2 + 5x + 10$ and $r(x) = 2$.

Corollary 23.3. Factor Theorem.

An element $a \in F$ (for a field F) is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.

Exercise 23.10. The polynomial $x^3 + 2x^2 + 2x + 1$ can be factored into linear factors in $\mathbb{Z}_7[x]$. Find the factorization.

Solution. This is equivalent to finding the zeros of the polynomial by Corollary 23.3. So we check each element of $\mathbb{Z}_7$ as follows:

x	$x^3 + 2x^2 + 2x + 1$
0	1
1	$1 + 2 + 2 + 1 = 6$
2	$8 + 8 + 4 + 1 \equiv 0$
3	$27 + 18 + 6 + 1 = 62 \equiv 6$
$4 \equiv -3$	$-27 + 18 - 6 + 1 = -14 \equiv 0$
$5 \equiv -2$	$-8 + 8 - 4 + 1 = -3 \equiv 4$
$6 \equiv -1$	$-1 + 2 - 2 + 1 = 0$

(Notice the use of "negatives.") So the zeros are 2, 4, and 6 and so in $\mathbb{Z}_7$, $x^3 + 2x^2 + 2x + 1 = (x - 2)(x - 4)(x - 6) = (x + 5)(x + 3)(x + 1)$.

Corollary 23.5. A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.

Corollary 23.6. If G is a finite subgroup of the multiplicative group $\langle F^*, \cdot\rangle$ of a field F, then G is cyclic. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Definition 23.7. A nonconstant polynomial $f(x) \in F[x]$ (F a field) is *irreducible over* F or is an *irreducible polynomial in* $F[x]$ if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree than the degree of $f(x)$. If $f(x) \in F[x]$ is a nonconstant polynomial that is not irreducible over F, then $f(x)$ is *reducible over* F.

Example 23.8. Since $x^2 - 2$ has no zeros in $\mathbb{Q}[x]$, then $x^2 - 2$ is irreducible over $\mathbb{Q}$. However, $x^2 - 2$ is reducible over $\mathbb{R}$ since $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ in $\mathbb{R}[x]$.

Example. Since $x^2 + 1$ has no zeros in $\mathbb{R}[x]$, then $x^2 + 1$ is irreducible over $\mathbb{R}$. However, $x^2 + 1$ is reducible over $\mathbb{C}$ since $x^2 + 1 = (x - i)(x + i)$ in $\mathbb{C}[x]$.

Theorem 23.10. Let $f(x) \in F[x]$, and let $f(x)$ be of degree 2 or 3. Then $f(x)$ is reducible over F if and only if it has a zero in F.

Note. A polynomial $f(x)$ may be reducible and still not have a zero. For example, $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$ in $\mathbb{R}[x]$, but $x^4 + 2x^2 + 1$ has no zero in $\mathbb{R}$.

Theorem 23.11. If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if and only if it has such a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$. (The text omits the proof of this.)

Corollary 23.12. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ is in $\mathbb{Z}[x]$ with $a_0 \neq 0$ and if $f(x)$ has a zero in $\mathbb{Q}$, then it has a zero m in $\mathbb{Z}$, and m must divide a_0.

Exercise 23.16. Demonstrate that $x^3 + 3x^2 - 8$ is irreducible over $\mathbb{Q}$.

Solution. By Corollary 23.12, if $f(x) = x^3 + 3x^2 - 8$ has a zero in $\mathbb{Q}$, then it has a zero $m \in \mathbb{Z}$ which divides -8. So we test the divisors of -8 to see if they are zeros of $f(x)$:

x	$f(x)$
-8	-328
-4	-24
-2	-4
-1	-6
1	-4
2	12
4	104
8	696

Since there is no zero in $\mathbb{Z}$, there is no zero in $\mathbb{Q}$. So by the Factor Theorem there is no linear factor and by Theorem 23.10 we have that $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 23.15. Eisenstein Criterion.

Let $p \in \mathbb{Z}$ be a prime. Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$, and $a_n \not\equiv 0 \pmod{p}$, but $a_i \equiv 0 \pmod{p}$ for all $i < n$, with $a_0 \not\equiv 0 \pmod{p^2}$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Exercise 23.19. Is $8x^3 + 6x^2 - 9x + 24$ reducible over $\mathbb{Q}$?

Solution. With $p = 3$, we have $a_0 \equiv a_1 \equiv a_2 \equiv 0 \pmod{p}$ since $24 \equiv -9 \equiv 6 \equiv 0 \pmod{3}$, $a_n = a_3 \not\equiv 0 \pmod{3}$ since $a_3 = 8 \equiv 2 \pmod{3}$, and $a_0 \not\equiv 0 \pmod{p^2}$ since $a_0 = 24 \equiv 6 \pmod{9}$. So, by the Eisenstein Criterion, $8x^3 + 6x^2 - 9x + 24$ is irreducible over $\mathbb{Q}$.

Corollary 23.17. The polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$$

is irreducible over $\mathbb{Q}$ for any prime p.

Definition. The polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$$

for prime p is the *pth cyclotomic polynomial.*

Note. The zeros of Φ_p are the pth roots of unity in $\mathbb{C}$, excluding 1.

Theorem 23.18. Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x)s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.

Note. The proof of Theorem 23.18 is given in Section 27 as the proof of Theorem 27.27. The strength of Theorem 23.18 is given in Theorem 23.20 which gives a uniqueness result for the factorization of polynomials.

Corollary 23.19. If $p(x)$ is irreducible in $F[x]$ and $p(x)$ divides the product $r_1(x)r_2(x)\cdots r_n(x)$ for $r_i(x) \in F[x]$, then $p(x)$ divides $r_i(x)$ for at least one i.

Note. The proof of Corollary 23.19 follows from Theorem 23.18 by Mathematical Induction.

Theorem 23.20. If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit (that is, nonzero constant) factors in F.

Example. In Exercise 23.10 we saw that in $\mathbb{Z}_7$,

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

Since $2^3 \equiv 1 \pmod{7}$, we also have

$$x^3 + 2x^2 + 2x + 1 = (2x+3)(2x+6)(2x+2).$$

Revised: 7/15/2023