Proposition 18. A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Proof: We give a proof of this result using the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 3 in Section 5.2). A more number-theoretic proof is outlined in the exercises, or Proposition 5 in Section 6.1 may be used in place of the Fundamental Theorem. By the Fundamental Theorem, the finite subgroup can be written as the direct product of cyclic groups

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

where $n_k \mid n_{k-1} \mid \cdots \mid n_2 \mid n_1$. In general, if G is a cyclic group and $d \mid |G|$ then G contains precisely d elements of order dividing d. Since n_k divides the order of each of the cyclic groups in the direct product, it follows that each direct factor contains n_k elements of order dividing n_k. If k were greater than 1, there would therefore be a total of more than n_k such elements. But then there would be more than n_k roots of the polynomial $x^{n_k} - 1$ in the field F, contradicting Proposition 17. Hence $k = 1$ and the group is cyclic.

Corollary 19. Let p be a prime. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes mod p is cyclic.

Proof: This is the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$.

Corollary 20. Let $n \geq 2$ be an integer with factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ in $\mathbb{Z}$, where $p_1, \ldots, p_r$ are distinct primes. We have the following isomorphisms of (multiplicative) groups:

(1) $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$

(2) $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$, for all $\alpha \geq 2$

(3) $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$, for all odd primes p.

Remark: These isomorphisms describe the group-theoretic structure of the automorphism group of the cyclic group, Z_n, of order n since $\mathrm{Aut}(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ (cf. Proposition 16 in Section 4.4). In particular, for p a prime the automorphism group of the cyclic group of order p is cyclic of order $p-1$.

Proof: This is mainly a matter of collecting previous results. The isomorphism in (1) follows from the Chinese Remainder Theorem (see Corollary 18, Section 7.6). The isomorphism in (2) follows directly from Exercises 22 and 23 of Section 2.3.

For p an odd prime, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is an abelian group of order $p^{\alpha-1}(p-1)$. By Exercise 21 of Section 2.3 the Sylow p-subgroup of this group is cyclic. The map

$$\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \qquad \text{defined by} \qquad a + (p^\alpha) \mapsto a + (p)$$

is a ring homomorphism (reduction mod p) which gives a surjective group homomorphism from $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ onto $(\mathbb{Z}/p\mathbb{Z})^\times$. The latter group is cyclic of order $p-1$

(Corollary 19). The kernel of this map is of order $p^{\alpha-1}$, hence for all primes $q \neq p$, the Sylow q-subgroup of $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$ maps isomorphically into the cyclic group $(\mathbb{Z}/p\mathbb{Z})^{\times}$. All Sylow subgroups of $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$ are therefore cyclic, so (3) holds, completing the proof.

EXERCISES

1. Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Describe the nilradical of $F[x]/(f(x))$ in terms of the factorization of $f(x)$ (cf. Exercise 29, Section 7.3).
2. For each of the fields constructed in Exercise 6 of Section 4 exhibit a generator for the (cyclic) multiplicative group of nonzero elements.
3. Let p be an odd prime in $\mathbb{Z}$ and let n be a positive integer. Prove that $x^n - p$ is irreducible over $\mathbb{Z}[i]$. [Use Proposition 18 in Chapter 8 and Eisenstein's Criterion.]
4. Prove that $x^3 + 12x^2 + 18x + 6$ is irreducible over $\mathbb{Z}[i]$. [Use Proposition 8.18 and Eisenstein's Criterion.]
5. Let φ denote Euler's φ-function. Prove the identity $\sum_{d|n} \varphi(d) = n$, where the sum is extended over all the divisors d of n. [First observe that the identity is valid when $n = p^m$ is the power of a prime p since the sum telescopes. Write $n = p^m n'$ where p does not divide n'. Prove that $\sum_{d|n} \varphi(d) = \sum_{d''|p^m} \varphi(d'') \sum_{d'|n'} \varphi(d')$ by multiplying out the right hand side and using the multiplicativity $\varphi(ab) = \varphi(a)\varphi(b)$ when a and b are relatively prime. Use induction to complete the proof. This problem may be done alternatively by letting Z be the cyclic group of order n and showing that since Z contains a unique subgroup of order d for each d dividing n, the number of elements of Z of order d is $\varphi(d)$. Then $|Z|$ is the sum of $\varphi(d)$ as d runs over all divisors of n.]
6. Let G be a finite subgroup of order n of the multiplicative group $F^{\times}$ of nonzero elements of the field F. Let φ denote Euler's φ-function and let $\psi(d)$ denote the number of elements of G of order d. Prove that $\psi(d) = \varphi(d)$ for every divisor d of n. In particular conclude that $\psi(n) \geq 1$, so that G is a cyclic group. [Observe that for any integer $N \geq 1$ the polynomial $x^N - 1$ has at most N roots in F. Conclude that for any integer N we have $\sum_{d|N} \psi(d) \leq N$. Since $\sum_{d|N} \varphi(d) = N$ by the previous exercise, show by induction that $\psi(d) \leq \varphi(d)$ for every divisor d of n. Since $\sum_{d|n} \psi(d) = n = \sum_{d|n} \varphi(d)$ show that this implies $\psi(d) = \varphi(d)$ for every divisor d of n.]
7. Prove that the additive and multiplicative groups of a field are never isomorphic. [Consider three cases: when $|F|$ is finite, when $-1 \neq 1$ in F, and when $-1 = 1$ in F.]

9.6 POLYNOMIALS IN SEVERAL VARIABLES OVER A FIELD AND GRÖBNER BASES

In this section we consider polynomials in many variables, present some basic computational tools, and indicate some applications. The results of this section are not required in Chapters 10 through 14. Additional applications will be given in Chapter 15.

We proved in Section 2 that a polynomial ring $F[x]$ in a variable x over a field F is a Euclidean Domain, and Corollary 8 showed that the polynomial ring $F[x_1, \ldots, x_n]$ is a U.F.D. However it follows from Corollary 8 in Section 8.2 that the latter ring is not a P.I.D. unless $n = 1$. Our first result below shows that ideals in such polynomial rings, although not necessarily principal, are always finitely generated. General rings with this property are given a special name:

Definition. A commutative ring R with 1 is called *Noetherian* if every ideal of R is finitely generated.

Noetherian rings will be studied in greater detail in Chapters 15 and 16. In this section we develop some of the basic theory and resulting algorithms for working with (finitely generated) ideals in $F[x_1, \ldots, x_n]$.

As we saw in Section 1, a polynomial ring in n variables can be considered as a polynomial ring in one variable with coefficients in a polynomial ring in $n-1$ variables. By following this inductive approach—as we did in Theorem 7 and Corollary 8—we can deduce that $F[x_1, x_2, \ldots, x_n]$ is Noetherian from the following more general result.

Theorem 21. *(Hilbert's Basis Theorem)* If R is a Noetherian ring then so is the polynomial ring $R[x]$.

Proof: Let I be an ideal in $R[x]$ and let L be the set of all leading coefficients of the elements in I. We first show that L is an ideal of R, as follows. Since I contains the zero polynomial, $0 \in L$. Let $f = ax^d + \cdots$ and $g = bx^e + \cdots$ be polynomials in I of degrees d, e and leading coefficients $a, b \in R$. Then for any $r \in R$ either $ra - b$ is zero or it is the leading coefficient of the polynomial $rx^e f - x^d g$. Since the latter polynomial is in I we have $ra - b \in L$, which shows L is an ideal of R. Since R is assumed Noetherian, the ideal L in R is finitely generated, say by $a_1, a_2, \ldots, a_n \in R$. For each $i = 1, \ldots, n$ let f_i be an element of I whose leading coefficient is a_i. Let e_i denote the degree of f_i, and let N be the maximum of $e_1, e_2, \ldots, e_n$.

For each $d \in \{0, 1, \ldots, N-1\}$, let L_d be the set of all leading coefficients of polynomials in I of degree d together with 0. A similar argument as that for L shows each L_d is also an ideal of R, again finitely generated since R is Noetherian. For each nonzero ideal L_d let $b_{d,1}, b_{d,2}, \ldots, b_{d,n_d} \in R$ be a set of generators for L_d, and let $f_{d,i}$ be a polynomial in I of degree d with leading coefficient $b_{d,i}$.

We show that the polynomials $f_1, \ldots, f_n$ together with all the polynomials $f_{d,i}$ for all the nonzero ideals L_d are a set of generators for I, i.e., that

$$I = (\{f_1, \ldots, f_n\} \cup \{f_{d,i} \mid 0 \le d < N,\ 1 \le i \le n_d\}).$$

By construction, the ideal I' on the right above is contained in I since all the generators were chosen in I. If $I' \neq I$, there exists a nonzero polynomial $f \in I$ of minimum degree with $f \notin I'$. Let $d = \deg f$ and let a be the leading coefficient of f.

Suppose first that $d \ge N$. Since $a \in L$ we may write a as an R-linear combination of the generators of L: $a = r_1 a_1 + \cdots + r_n a_n$. Then $g = r_1 x^{d-e_1} f_1 + \cdots + r_n x^{d-e_n} f_n$ is an element of I' with the same degree d and the same leading coefficient a as f. Then $f - g \in I$ is a polynomial in I of smaller degree than f. By the minimality of f, we must have $f - g = 0$, so $f = g \in I'$, a contradiction.

Suppose next that $d < N$. In this case $a \in L_d$ for some $d < N$, and so we may write $a = r_1 b_{d,1} + \cdots + r_{n_d} b_{n_d}$ for some $r_i \in R$. Then $g = r_1 f_{d,1} + \cdots + r_{n_d} f_{n_d}$ is a polynomial in I' with the same degree d and the same leading coefficient a as f, and we have a contradiction as before.

It follows that $I = I'$ is finitely generated, and since I was arbitrary, this completes the proof that $R[x]$ is Noetherian.