UNIT GROUPS OF COMMUTATIVE UNITAL RINGS

CHRISTOPHER R. MCMURDIE AND ADVISOR: DR. NICK ROGERS

Abstract. In this paper we classify elements in $U(R[x])$, and then take a cursory
look at how the unit functor interacts with quotients, at least in the special cases
where we can get explicit results. First, we recall some results for $\mathbb{Z}/n\mathbb{Z}$.

1. Units of $\mathbb{Z}/n\mathbb{Z}$

Here, we recall the results about $U(\mathbb{Z}/n\mathbb{Z})$. For a complete treatment, see chapter
4 of [IR90]

Proposition 1.1. Suppose $A, B$ are unital rings. Then $U(A \oplus B) = U(A) \times U(B)$.

Proof. Recall that $U(A \oplus B) = \{(a, b) | a \in A, b \in B \text{ and there exists } (u, v) \in A \oplus B \text{ such that } (a, b) \cdot (u, v) = (au, bv) = (1, 1)\}$. This is the same set as

$\{(a, b) | a \in U(A) \text{ and } b \in U(B)\}$

which is just $U(A) \times U(B)$.

The strategy is then to express $\mathbb{Z}/n\mathbb{Z}$ in terms of its elementary divisor decom-
position. It is essential only to know how to calculate the unit group of $\mathbb{Z}/p^k\mathbb{Z}$ for
$p$ prime and $k \geq 1$.

Theorem 1.2. Suppose $p \in \mathbb{Z}$ is prime. Then

$U(\mathbb{Z}/p^k\mathbb{Z}) = \begin{cases} \mathbb{Z}/p^{k-1}\mathbb{Z} \oplus \mathbb{Z}/(p - 1)\mathbb{Z} & p > 2, k \geq 2 \\ \mathbb{Z}/p^{k-2}\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} & p = 2, k \geq 2 \\ \mathbb{Z}/(p - 1)\mathbb{Z} & k = 1 \end{cases}$

Theorem 1.3. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$. Then $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{e_k}\mathbb{Z}$.

Proof. This is a special case of Proposition 3.1.

Corollary 1.4. Suppose $n = 2^{e_0} p_1^{e_1} \cdots p_k^{e_k}$, $p_i$ odd and distinct. Then

$U(\mathbb{Z}/n\mathbb{Z}) = \begin{cases} \bigoplus_{i=1}^{k} (\mathbb{Z}/p_i^{e_i-1}\mathbb{Z} \oplus \mathbb{Z}/(p_i - 1)\mathbb{Z}) & e_0 < 2 \\ \mathbb{Z}/2\mathbb{Z} \bigoplus_{i=1}^{k} (\mathbb{Z}/p_i^{e_i-1}\mathbb{Z} \oplus \mathbb{Z}/(p_i - 1)\mathbb{Z}) & e_0 = 2 \\ \mathbb{Z}/2^{e_0-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \bigoplus_{i=1}^{k} (\mathbb{Z}/p_i^{e_i-1}\mathbb{Z} \oplus \mathbb{Z}/(p_i - 1)\mathbb{Z}) & e_0 > 2 \end{cases}$

Date: May 2007.
Proof. This is an immediate consequence of Theorem’s 1.3, 1.2 and Proposition 1.1. □

**Corollary 1.5.** Suppose \( n = 2^{e_0}p_1^{e_1} \cdots p_k^{e_k} \) for odd distinct \( p_i \) prime. Then \( U(\mathbb{Z}/n\mathbb{Z}) \) is cyclic if, and only if, \( n = 2, 4, p^e, 2p^e \).

**Proof.** In any case, \( e_0 \) must be either 0, 1 or 2: for \( e_0 \geq 3 \), we have that \( U(\mathbb{Z}/2^{e_0}\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{e_0-2}\mathbb{Z} \), and these direct summands are not relatively prime. If \( k = 1 \), then for odd \( p \), \( U(\mathbb{Z}/p^e\mathbb{Z}) = \mathbb{Z}/p^{e-1}\mathbb{Z} \oplus \mathbb{Z}/(p - 1)\mathbb{Z} \), which is cyclic since \( p - 1 \) and \( p^{e-1} \) are relatively prime. But \( p - 1 \) is a positive even number, so \( e_0 \neq 2 \) in this case. This establishes the cases 2, 4, \( p^k, 2p^k \).

If \( k \geq 2 \), then \( \mathbb{Z}/(p_i - 1)\mathbb{Z} \) and \( \mathbb{Z}/(p_j - 1)\mathbb{Z} \) are both direct summands by the above corollary. However, \( p_i - 1 \) and \( p_j - 1 \) are both even, and hence not relatively prime. Thus, \( k \leq 1 \). □
2. Unit Groups of Polynomial Rings

Given a ring $R$ with 1, we can define a polynomial ring $R[x]$ with one indeterminate in the following obvious way. $R[x] = \{ \sum_{i=0}^{n} r_i x^i : n \in \mathbb{Z}^+, r_i \in R \}$, where $x^0 \equiv 1_R$. Addition is inherited from $R$ by forcing $rx^i + sx^j = (r+s)x^i$, and extending by linearity. Multiplication is also inherited from $R$, by forcing distributivity and requiring that $rx^i \cdot sx^j = rsx^{i+j}$. We can iterate this process of adjoining an indeterminate, and consider $R[x_1, \cdots, x_n]$, supposing that indeterminates commute with each other.

For the purposes of this section, a polynomial ring $P$ will mean a commutative unital ring $R$, adjoined with a finite number of indeterminates. The degree of $p \in P$ is intuitively the largest number of indeterminates appearing in any term. For example, the degree of $3x^2y + y^3x^4 + 17x - y \in \mathbb{Z}[x,y]$ is 7, since the middle term is the product of 7 (not necessarily distinct) indeterminates.

**Proposition 2.1.** Suppose $p, q \in P$, and the base ring $R$ of $P$ has no zero-divisors. Then $\deg(pq) = \deg(p) + \deg(q)$.

**Theorem 2.2.** If $P$ is a polynomial ring with base ring $R$, which has no zero-divisors, then $U(P) = U(R)$.

**Proof.** The degree of $1_P = 1_R x^0$ is zero. Since the degree only increases under multiplication, no element $p \in P$ of degree greater than zero is invertible. The only remaining candidates are the constants, and this subring is isomorphic to $R$. □

**Corollary 2.3.** If $R$ is a field, then $U(P) = R^*$.

We have shown that the only interesting unit groups of polynomial rings occur when the base ring $R$ has zero-divisors. We will show this can be improved, so that the only interesting cases occur when $R$ has non-zero nilpotent elements. We will say that $n \in R$ is nilpotent of degree $e$ if $n^e = 0$, and $n^k \neq 0$ for $k < e$.

**Example 2.4.** Suppose $R = \mathbb{Z}/4\mathbb{Z}$, and $P = R[x]$. Then $1 + 2x$ is a unit, and in fact self-inverse.

It turns out that it is fairly easy to classify all of the elements in $U(R[x])$ for $R$ a unital ring, at least supposing that we know a little about $R$. In the following proof, we make great use of the fact that the coefficient of $x^k$ of the product $f(x)g(x)$ is given by $\sum_{i=0}^{k} f_{k-i}g_i$.

**Proposition 2.5.** If $f(x) = f_0 + f_1 x + \cdots + f_n x^n \in U(R[x])$, then $f_n$ is nilpotent.

**Proof.** Let $g(x)f(x) = 1$, and let $d = \deg(g(x))$. Define $m_i = \min(i, n)$. Without loss of generality, we can assume that $d \geq n$ by interchanging $f$ and $g$, if necessary.
Since $nd > n$, we have that

$$0 = gd_n = -f_0^{-1} \sum_{l=1}^{md+n} gd_{n-l}f_l = gd_f_n.$$ 

Inductively, we have that

$$0 \cdot f_{ni} = gd_{n-i} \cdot f_{ni} = -f_0^{-1} \sum_{l=1}^{md+n-i} gd_{n-i-l}f_{ni}f_l = gd_{n-i}f_{n+i+1}.$$ 

However, $g_0$ is a unit, and not a zero-divisor. It follows that $f_{n+1}^0 = 0$, and $f_n$ is nilpotent.

**Lemma 2.6.** Suppose $g(x) \in R[x], n \in R$ is nilpotent. Then $g(x) \in U(R[x])$ if, and only if, $g(x) + nx^n \in U(R[x])$.

**Proof.** $\Rightarrow$: Consider that $(g(x) + nx^n) (g^{-1}(x) \sum_{i=0}^{n-1} (-1)^i (nx^k g^{-1}(x))^i) = 1$.

$\Leftarrow$: Suppose $(g(x) + nx^n)q(x) = 1 = q(x)g(x) + nx^nq(x)$. Then set $f(x) = q(x) \sum_{i=0}^{n-1} (nx^k q(x))^i$. Then $g(x)f(x) = (1 - nx^nq(x)) \sum_{i=0}^{n-1} (nx^k q(x))^i = 1$.

**Theorem 2.7.** An element $f(x) = f_0 + f_1x + \cdots + f_nx^n \in R[x]$ is a unit if, and only if, $f_0 \in U(R)$ and $f_{i>0}$ is nilpotent in $R$.

**Proof.** $\Rightarrow$: Since $f_n$ is nilpotent, we have that $f^{(n-1)}(x) := f(x) - f_nx^n \in U(R[x])$.

Hence, $f_{n-1}$, the leading coefficient of $f^{(n-1)}(x)$ is nilpotent. Continuing in this fashion, we show that all coefficients $f_{i>0}$ are nilpotent, and that $f_0 \in U(R)$.

$\Leftarrow$: Since $f_0 \in U(R) \subseteq U(R[x])$, we know that $f^{(1)}(x) = f_0 + f_1x \in U(R[x])$.

Continuing in this fashion, we have that $f^{(n)}(x) = f_0 + f_1x + \cdots + f_nx^n \in U(R[x])$.

**Corollary 2.8.** If $R$ has no non-zero nilpotent elements, then $U(R[x]) = U(R)$.

We will now show that theorem 2.7 extends to $R$ adjoined with any number of indeterminates. We will use the notation that $X^1_R = R[x_1], X^2_R = R[x_1, x_2]$, and so on. We omit the subscript when the base ring $R$ is clear. First, a lemma.

**Lemma 2.9.** Suppose $f(x) = f_0 + \cdots + f_nx^n \in R[x]$. Then $f(x)$ is nilpotent if, and only if, $f_i$ is nilpotent for $0 \leq i \leq n$.

**Proof.** $\Rightarrow$: Write $0 = f(x)^k = (f^{(n-1)}(x) + f_nx^n)^k = f^{(n-1)}(x)^k + \cdots + f_n^kx^n$.

Since $x^{nk}$ is the highest degree, its only coefficient $f_n^k = 0$; hence, $f_n \in N(R)$.

Since $f_n^k x^k \in N(R[x])$, and nilpotent elements form an ideal, we conclude that $f^{(n-1)}(x) \in N(R[x])$. Continuing in this fashion, we have that $f_i \in N(R)$ for all $i$.

$\Leftarrow$: This follows since $f_i x^i \in N(R[x])$ (it has degree $e_i$) and the nilpotent elements form an ideal.
This result immediately extends to $X_R^n$ by induction, i.e. $f \in X_R^n$ is nilpotent if, and only if, the coefficient of each term is nilpotent in $R$.

**Theorem 2.10.** Let $X_R^n$ be a polynomial ring. Then $U(X_R^n) = \{ f_0 + g(x_1, \ldots, x_n) : g(0, \ldots, 0) = 0, f_0 \in U(R), g_i \text{ nilpotent in } R \text{ for all } i \in \mathbb{N} \}$.

**Proof.** We will use the recursive definition for $X^n$, i.e. $X^n = X^{n-1}[x_n]$. Consider $f(x) \in U(X^n)$. By theorem 2.7, we have that $f_0 \in U(X^{n-1})$; so inductively, $f_0$ can be written in the form described. Consider that $f_i \in N(X^{n-1})$. Then by the remarks above, $f_i$ can also be written in the above form. This proves that every element in $U(X^n)$ can be written in the above form; the converse is proved by lemma 2.6. \qed

It remains to calculate the isomorphism class of $U(R[x])$, say in terms of $U(R)$ and $\sqrt{0} = N(R)$, the nilpotent ideal of $R$. This seems to be a difficult problem, however. For reference, we provide the following characterization of $N(R)$:

**Proposition 2.11.** Let $R$ be a ring. Then $N(R) = \bigcap\{ P \triangleleft R : P \text{ is prime in } R \}$.

**Proof.** Let $P = \bigcap\{ P \triangleleft R : P \text{ is prime in } R \}$, and let $N = N(R)$, the nilpotent ring. If $x \in N \setminus P$, then $x^k = 0 \in P$ for some $k$. Choose $k'$ minimal so that $x^{k'} \in P$. Since $P$ is prime, and $x \notin P$, $x^{k'-1} \in P$. This contradicts minimality, so that $N \subseteq P$.

Now, consider $i \notin N$. Define $\Sigma = \{ I \triangleleft R : i^n \notin I \text{ for } n > 0 \}$, and partially order $\Sigma$ by set inclusion. By Zorn’s Lemma, $\Sigma$ has a maximal element, say $M$. We will show that $M$ is prime.

Suppose $x, y \notin M$, and $xy \in M$. Since $M$ is maximal, $i^m \in M + \langle x \rangle$, and $i^n \in M + \langle y \rangle$. Hence, $i^{m+n} \in (M + \langle x \rangle) \cap (M + \langle y \rangle)$. But this implies that $i^{m+n} \in M + xy = M$, contradicting that $M \in \Sigma$. Thus, $M$ is prime.

Hence, if $i \notin N$, then $i \notin M \triangleright P$, i.e. $P \subseteq N$. \qed

**Example 2.12.** Suppose $R = \mathbb{Z}/4\mathbb{Z}$. Then $U(R[x]) \cong (\mathbb{Z}/2\mathbb{Z})^N \cong \langle \{ a_i \}_{i \in N} : a_i^2 = a_j^{-1}a_i^{-1}a_ja_i = 1, \ i, j \in N \rangle$

**Proof.** The isomorphism is $\phi : 1 + 2x^i \mapsto a_i$. Every unit can be written as $u(x) = 1 + 2x^{e_1} + \cdots + 2x^{e_k}$

for some choice of exponents $(e_1, \ldots, e_k)$. This has the unique representation as $\prod_i (1 + 2x^{e_i})$.

Noticing commutativity, and that $(1 + 2x^k)^2 = 1$, the result follows. \qed
3. Unit Groups of Quotients

If we consider unital rings \( R_1 \) and \( R_2 \) and some ring-homomorphism \( f : R_1 \to R_2 \), then the following diagram commutes:

\[
\begin{array}{ccc}
R_1 & \xrightarrow{f} & R_2 \\
\downarrow & & \downarrow \\
U(R_1) & \xrightarrow{f_*} & U(R_2)
\end{array}
\]

Here, \( f_* \) is simply \( f \) restricted to \( U(R_1) \). It respects the product in \( U(R_1) \) because \( f \) respects the product in \( R_1 \); it remains only to show that homomorphisms map units to units. So consider a unit \( a \in R_1 \), say \( a \cdot b = 1 \). Then \( f(a \cdot b) = f(a) \cdot f(b) = f(1_{R_1}) = 1_{R_2} \), so indeed \( f(a) \) is a unit in \( R_2 \). This establishes that \( U \) is a functor from the category of unital rings to the category of groups. Furthermore, \( f_* \) is injective (resp. surjective) if \( f \) is injective (surjective).

We would like to know how to express \( U(R/I) \) for any ideal \( I \triangleleft R \). Unfortunately, for a general ring \( R \) this problem seems very hard. For one thing, we do not have a canonical way of representing \( I \). If \( R \) is Noetherian then we can represent \( I \) uniquely in a primary decomposition \( I = \bigcap_{i=1}^m I_i \). This is the well known Lasker-Noether theorem, and will be helpful in calculating \( U(R/I) \).

**Proposition 3.1.** Suppose \( R \) is a unital ring and \( \{I_i : 1 \leq i \leq n\} \) are ideals in \( R \). Furthermore, assume that \( I_i + I_j = R \) for any \( i, j \). Then

\[
U(R/\bigcap_{i=1}^m I_i) \cong U(R/I_1) \times \cdots \times U(R/I_n).
\]

**Proof.** The canonical monomorphism from \( R/\bigcap_{i=1}^m I_i \) into \( \bigoplus_{i=1}^m R/I_i \) is given by

\[
f(r + \bigcap_{i=1}^m I_i) = (r + I_1, \ldots, r + I_n).
\]

This is onto by the Chinese Remainder Theorem. Hence, \( R/\bigcap_{i=1}^m I_i \cong R/I_1 \oplus \cdots \oplus R_m \). The result then follows from Proposition 1.1. \( \square \)

Unfortunately, the minimal primary decomposition of some ideal \( I \) will not, in general, satisfy the hypothesis of the Chinese Remainder Theorem, and we cannot hope that the unit group will decompose so nicely.

**Example 3.2.**

\[
U \left( \frac{\mathbb{Z}/2\mathbb{Z}[x,y]}{\langle x^2 \rangle \cap \langle y^2 \rangle} \right) \ncong U \left( \frac{\mathbb{Z}/2\mathbb{Z}[x,y]}{\langle x^2 \rangle} \right) \oplus U \left( \frac{\mathbb{Z}/2\mathbb{Z}[x,y]}{\langle y^2 \rangle} \right).
\]

**Proof.** We see that

\[
U \left( \frac{\mathbb{Z}/2\mathbb{Z}[x,y]}{\langle x^2 \rangle \cap \langle y^2 \rangle} \right) = \{1, 1 + xy\},
\]
while
\[
U \left( \frac{(\mathbb{Z}/2\mathbb{Z})[x,y]}{\langle x^2 \rangle} \right) = \{1, 1 + x, 1 + xy, 1 + x + xy\}
\]
\[
U \left( \frac{(\mathbb{Z}/2\mathbb{Z})[x,y]}{\langle y^2 \rangle} \right) = \{1, 1 + y, 1 + xy, 1 + x + xy\}.
\]
But \(\mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\).

\[\square\]

**Remark.** There is an injection from \(U(R/\bigcap_I I_\alpha)\) into \(\prod_\alpha U(R/I_\alpha)\) for any collection of ideals.

We will use the following characterization of primary ideals in \(F[x]\):

**Proposition 3.3.** Suppose \(I \triangleleft F[x]\) is an ideal. Then \(I\) is primary if, and only if, \(I = \langle f(x)^k \rangle\) for \(f(x)\) (monic) irreducible in \(F[x]\) and \(k \in \mathbb{Z}^+\).

**Proof.** Suppose \(a(x)b(x) \in I\), and \(a(x) \notin I\). Since \(f(x)^k\) divides \(a(x)b(x)\) but does not divide \(a(x)\), we know that \(f(x)\) divides \(b(x)\). It follows that \(b(x)^k \in I\), and thus \(I\) is primary.

Conversely, since \(F[x]\) is a PID, write \(I = \langle g(x) \rangle\) for \(g(x)\) a monic polynomial. Now, \(g(x) = f_1(x)^{e_1} \cdots f_m(x)^{e_m}\), where \(f_i(x)\) is monic irreducible. If \(m > 1\), then consider that \(f_1(x)^{e_1}, f_2(x)^{e_2} \cdots f_m(x)^{e_m} \notin I\) but their product is. This contradicts that \(I\) is primary, and hence \(m = 1\). The result follows.

**Lemma 3.4.** Suppose \(R = F[x]\), for some field \(F\). Then given primary ideals \(I_1, I_2\) such that \(\sqrt{I_1} \neq \sqrt{I_2}\), \(I_1 + I_2 = R\).

**Proof.** We recall that the radical of a primary ideal is prime. Since \(R\) is a PID, \(\sqrt{I_1} = \langle f_1(x) \rangle\), and \(\sqrt{I_2} = \langle f_2(x) \rangle\) for distinct irreducible \(f_i(x)\). Then, for some \(k_1, k_2 \in \mathbb{Z}^+\), \(I_1 + I_2\) is generated by \(\gcd(f_1(x)^{k_1}, f_2(x)^{k_2}) = 1\). Thus, \(I_1 + I_2 = R\).

**Remark.** The requirement that \(F\) be a field is necessary.

Because of the previous lemma, and primary decomposition, we can use the Chinese remainder theorem to establish the following result.

**Theorem 3.5.** Suppose \(R = F[x]\), and if \(I \triangleleft R\) is any ideal, write \(I = \bigcap_{i=1}^n I_i\) a minimal primary decomposition. Then
\[
U(R/I) = U(R/I_1) \times \cdots \times U(R/I_m).
\]

**Proof.** Follows from Proposition 3.1 and Lemma 3.4.

To find the unit group of \(F[x]/I\) for some ideal \(I\), it suffices to calculate the unit group of \(F[x]/I_i\) where \(I_i\) is primary. By proposition 3.3, we have a characterization of all such ideals.
Now, we change pace for a moment to develop an important isomorphism of quotient rings. The following lemma sets the stage.

**Lemma 3.6.** Let $R$ and $S$ be commutative rings with 1, such that $S$ is a unitary $R$–module. Let $I \triangleleft R[x]$, and $s \in S$. Then

$$R[x]/I \xrightarrow{\phi_s} S/\langle \phi(I) \rangle$$

is a homomorphism where $\phi_s(f(x)) = f(s)$.

**Proof.** Since $S$ is a unitary $R$–module, the substitution $R[s]$ is defined; further, $\phi(1_R) = 1_S$ (since $s^0 = 1_S$). Let $i(x) \in I$, $r(x) \in R[x]$: then $\phi_s(r(x) + i(x)) = (r + i)(s) = r(s) + i(s) = r(s)$ since $i(s) \in \langle \phi(I) \rangle$. Thus, $\phi_s$ is well-defined, and clearly a homomorphism since it is evaluation at a point. $\square$

Suppose $R[x]$ and $S$ are PIDs. Then $I = \langle g(x) \rangle$, and $\langle \phi(I) \rangle = \langle g(s) \rangle$. Also, $\text{Ker}(\phi_s) \triangleleft R[x]$ and contains $I$. Suppose $\text{Ker}(\phi_s) = \langle k(x) \rangle$. Then $k(x)$ divides $g(x)$. Hence, when $g(x) = f(x)^k$ where $f(x)$ is irreducible in $R[x]$, then $k(x) = f(x)^j$ for some $0 \leq j \leq k$. Notice that $\phi_s$ is injective if and only if $j = k$.

Since $f(x)^j \in \text{Ker}(\phi_s)$, we see that $f(s)^j \in \langle f(s)^k \rangle$. Clearly, $f(s)^k \in \langle f(s)^j \rangle$; so in fact, $f(s)^j = f(s)^k \cdot u$, where $u \in U(S)$.

Take $R = F$, $S = E[y]$, where $E$, $F$ are fields. Here is the picture:

$$F[x]/\langle f(x)^k \rangle \xrightarrow{\phi_s} E[y]/\langle f(s)^k \rangle$$

Suppose that there exists $s \in E[y]$ such that $f(s) \in y + \langle y^k \rangle$. Then $f(s)^j = f(s)^k \cdot u$ implies that $j = k$. Hence, $\phi_s$ is injective, provided that such an $s$ exists.

**Theorem 3.7.** Let $F$ be a perfect field, and $f(x)$ an irreducible polynomial in $F[x]$. Let $E$ be the extension field $E = F[x]/f(x)$. Then for each $k \in \mathbb{Z}^+$ there exists $s \in E[y]$ such that $f(s) \in y + \langle y^k \rangle$.

**Proof.** First, we note that since $F$ is perfect, there exists a root $r \in E$ of $f(x)$ such that $f'(r) \neq 0$. We proceed inductively. When $k = 1$, we can find $s$ so that $f(s) = 0 \in y + \langle y \rangle$; we may choose $s = r$ as above. When $k = 2$, we have that $f(g_1y + r) = f(r) + f'(r)g_1y$ (mod $y^2$). Hence, we can choose $g_1 = f'(r)^{-1}$.

So suppose that we have $G_{k-1}(y) = r + g_1y + \cdots + g_{k-1}y^{k-1} \in E[y]$ so that $f(G_{k-1}(y)) \equiv y$ (mod $\langle y^k \rangle$) and $f'(r) \neq 0$. We will construct a solution $G_k(y) = g_ky^k + G_{k-1}(y)$ so that $f(G_k(y)) \equiv y$ (mod $\langle y^{k+1} \rangle$). Expanding, we have that

$$f(g_ky^k + G_{k-1}(y)) \equiv f(G_{k-1}(y)) + f'(G_{k-1}(y))g_ky^k \pmod{\langle y^{k+1} \rangle}$$

$$\equiv (y + g_k \cdot h(y)) + f'(r)g_ky^k \pmod{\langle y^{k+1} \rangle}$$

$$\equiv y + (h(0) + f'(r)g_k)y^k \pmod{\langle y^{k+1} \rangle}$$
where \( f(G_{k-1}(y)) = y^k \cdot h(y) \) in \( E[y] \). Hence, we may choose \( g_k = -\frac{h(0)}{f'(r)} \). This completes the induction and proves the result. \( \square \)

**Corollary 3.8.** Let \( F \) be a perfect field, and suppose \( f(x) \) is an irreducible polynomial in \( F[x] \); let \( E \) be the field \( F[x]/\langle f(x) \rangle \). Then

\[
F[x]/\langle f(x)^k \rangle \cong E[y]/\langle y^k \rangle.
\]

**Proof.** The previous theorem shows that there is an \( s \in E[y] \) so that \( \phi_s \) is a monomorphism by the discussion above. Let \( d = \deg f(x) \). To show surjectivity, we consider two cases. First, suppose that \( F \) is a finite field; then the result follows because the two rings both have \( |F|^{dk} \) elements. Now, suppose that \( F \) has characteristic 0. Then \( F[x]/\langle f(x)^k \rangle \) is an \( F \)-vector space of dimension \( dk \). More explicitly, each coset has a representative polynomial of degree less than \( dk \), and hence can be uniquely represented as a \( dk \)-tuple of elements of \( F \). Moreover, \( \phi_s \) is an \( F \)-linear transformation into \( E[y]/\langle y^k \rangle \), and is injective. It remains to see that \( E[y]/\langle y^k \rangle \) has \( F \)-dimension \( dk \). But this is clear, because \( \dim_F(E) = d \). Thus, \( \phi_s \) is surjective. \( \square \)

**Corollary 3.9.** Suppose \( F \) is a finite field, \( f(x), g(x) \) are irreducible, polynomials in \( F[x] \) and \( \deg(f) = \deg(g) \). Then

\[
U(F[x]/\langle f(x)^k \rangle) \cong U(F[x]/\langle g(x)^k \rangle),
\]

for all \( k \in \mathbb{Z}^+ \).

**Proof.** Recall that the extension fields \( F[x]/\langle f(x) \rangle \) and \( F[x]/\langle g(x) \rangle \) are isomorphic since \( F \) is finite; indeed, let \( d = \deg(f) \). Then if \( F = GF(p^n) \), both extension fields are \( GF(p^{nd}) \). Let \( E \) be a finite field \( GF(p^{nd}) \). From the previous proposition,

\[
F[x]/\langle f(x)^k \rangle \cong E[x]/\langle x^k \rangle \cong F[x]/\langle g(x)^k \rangle,
\]

for all \( k \in \mathbb{Z}^+ \). The result follows immediately. \( \square \)

**Remark.** The corollary fails when \( F \) has characteristic 0, for in this case the extension fields need not be isomorphic. For example, \( f(x) = x^2 - 2 \) and \( g(x) = x^2 + 1 \) yield non-isomorphic extension fields of \( \mathbb{Q} \).

**Proposition 3.10.** Suppose \( E \) is a field, and \( k \in \mathbb{Z}^+ \). Then

\[
U(E[x]/\langle x^k \rangle) \cong E^* \times \{ 1 + a_1 x + \cdots + a_{k-1} x^{k-1} : a_i \in E \}.
\]

**Proof.** Let \( u(x), v(x) \) be units in \( R = E[x]/\langle x^k \rangle \). Since \( \langle x \rangle \) are the only nilpotent elements in \( R \), \( u(x) = u_0 + \cdots + u_{k-1} x^{k-1} \) where \( u_0 \in E^* \), and similarly for \( v(x) \). Hence, we can factor \( u(x) = u_0 \cdot (1 + \cdots + u_0^{-1} u_{k-1} x^{k-1}) \) and \( v(x) \). The map \( \phi \) that sends

\[
u(x) \mapsto (u_0, 1 + \cdots + u_0^{-1} u_{k-1} x^{k-1})
\]
is an isomorphism from \( U(R) \) to \( E^* \oplus \{ 1 + a_1 x + \cdots + a_{k-1} x^{k-1} : a_i \in E \} \).

For the remainder of this section we will be concerned with the case when \( E \) is a finite field of order \( p^{nd} \), and \( R = E[x]/(x^k) \). The group of polynomials \( \{ 1 + a_1 x + \cdots + a_{k-1} x^{k-1} \} \) under multiplication will be referred to as \( Q \). Since \( E = GF(p^{nd}) \), \( |Q| = E^{k-1} = p^{nd(k-1)} \); hence, \( Q \) is a finite abelian \( p \)-group. See appendix A for some useful facts about these groups. We will use them with little comment.

**Definition 3.11.** Consider \( f(x) \in R \), and suppose \( f(x) = f_0 + f_1 x^{i_1} + \cdots + f_i x^{i_i} \), where \( m < n \) implies \( i_m < i_n \) and \( f_j \) is non-zero in \( E \) for all \( j \). We call \( i_1 \) the low degree of \( f \), denoted \( \text{Ldeg}(f) \).

**Proposition 3.12.** Consider \( u(x) \in Q \). If \( u(x) \) has low degree \( i \), then \( u(x) \) has order \( p^a \) where

\[
\left\lfloor \frac{k}{p^a} \right\rfloor \leq i < \left\lceil \frac{k}{p^{a-1}} \right\rceil.
\]

**Proof.** Consider \( (1 + u_i x^{i} + \cdots)^{p^a} \). Expanding, we have \( (1 + p^a u_i x^{i} + \cdots) = (1 + u_i^{p^a} x^{ip^a} + \cdots) \), since the \( E \) has characteristic \( p \). Hence, \( u(x) \) is of order at most \( p^a \) whenever \( ip^a \geq k \). Since \( i \) is an integer, we have \( i \geq \left\lceil \frac{k}{p^a} \right\rceil \). If \( i \) is also \( \geq \left\lceil \frac{k}{p^{a-1}} \right\rceil \), then the order is at most \( p^{a-1} \).

Using only the above proposition and the facts about \( p \)-groups, we can easily calculate the isomorphism class of \( U(R) \). We illustrate the algorithm with two simple examples.

**Example 3.13.** Find \( U((\mathbb{Z}/3\mathbb{Z})[x]/((x^3 + 2x + 1)^3)) \).

Let \( E = GF(3^3) \). Then we know that \( (\mathbb{Z}/3\mathbb{Z})[x]/(x^3 + 2x + 1) \cong E[x]/(x^3) \). Furthermore, since \( \frac{k}{p} = \frac{3}{3} = 1 \), we see that every non-identity element in \( Q \) has order 3. Since \( |Q| = |E|^2 = 3^6 \), we have that \( Q \cong (\mathbb{Z}/3\mathbb{Z})^6 \). Finally, \( E^* \cong \mathbb{Z}/26\mathbb{Z} \), so that \( U(R) \cong (\mathbb{Z}/26\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})^6 \).

**Example 3.14.** Find the unit group of \( E[x]/(x^6) \), where \( E = GF(3^3) \).

We consider \( Q \). We have:

\[
\left\lfloor \frac{6}{3^4} \right\rfloor \leq i < 6 \Rightarrow i \in \{ 2, 3, 4, 5 \}
\]

\[
\left\lfloor \frac{6}{3^2} \right\rfloor \leq i < 2 \Rightarrow i = 1.
\]

So there are \( |E^*| \cdot |E|^4 = 3^{12}(3^3 - 1) \) elements of order 9. It follows that \( Q \cong (\mathbb{Z}/9\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z})^9 \) (see Appendix). Thus, the unit group is isomorphic to \( (\mathbb{Z}/80\mathbb{Z}) \oplus (\mathbb{Z}/9\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z})^9 \).
As in the first example, whenever we can conclude that $[k/p] = 1$, we can describe the unit group very simply. We summarize with the following theorem.

**Theorem 3.15.** Suppose $k \leq p$, where $F = GF(p^n)$, and $f(x)$ is irreducible in $F[x]$ of degree $d$. Then

$$U(F[x]/\langle f(x)^k \rangle) \cong U(F[x]/\langle f(x) \rangle) \oplus F[x]/\langle f(x)^{k-1} \rangle,$$

and both are $\mathbb{Z}/(p^{nd} - 1) \mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})^{nd(k-1)}$.

**Remark.** One should notice the similarity with $U(\mathbb{Z}/p^k\mathbb{Z})$ for $p$ an odd prime; indeed, for such $p$ we have

$$U(\mathbb{Z}/p^k\mathbb{Z}) \cong U(\mathbb{Z}/p\mathbb{Z}) \oplus \mathbb{Z}/p^{k-1}\mathbb{Z}.$$

This is a nice analogy that breaks down in many cases, most often for large values of $k$. In a limited sense, the next section addresses this problem.
4. POWER SERIES RINGS

Suppose $k$ is field, and let $k[[x]]$ denote the ring of formal power series. Intuitively, we think of the ring $k[[x]]$ as polynomials of infinite length with normal polynomial addition and multiplication; but precisely, we must regard elements $f \in k[[x]]$ as sequences $f = (k_i)_{i \in \mathbb{Z}^+}$, with component-wise addition and the obvious multiplication. In this section we will study the unit group of $k[[x]]$ when $k = \mathbb{F}_p$, the finite field with $p$ elements.

First, we can easily classify the units in $k[[x]]$: $f$ is a unit if and only if $f_0$ is a unit in $k$, i.e. non-zero. In fact, $\langle x \rangle$ is a maximal ideal (since $k[[x]]/\langle x \rangle \cong k$ is a field); every proper ideal $I \triangleleft k[[x]]$ is contained in $\langle x \rangle$, so that $k[[x]]$ is a local ring.

We see that $U(k[[x]]) = k^* \oplus Q$, where $Q = \{ 1 + xf(x) : f \in k[[x]] \}$. Consider any $0 \neq f \in U(k[[x]])$, so that $\text{Ldeg}(1 + xf) = i > 0$. If $\text{char}(k) = 0$, it follows that $\text{Ldeg}((1 + xf)^n) = i$ for all $n$. If $\text{char}(k) = p$, then $\text{Ldeg}((1 + xf)^n) = i$ when $(p, n) = 1$, and otherwise $\text{Ldeg}(f^n) = ip^a$ for some $a$. Thus every element in $Q$ has infinite order, and clearly $Q$ is not finitely generated. Hence, calculating $U(k[[x]])$ means finding canonical generators and relations for $Q$.

**Example 4.1.** Consider $\mathbb{F}_3[[x]]$. Then we have

$$1 + 2x = (1 + x)^2 (1 + x^2)^2 (1 + x^3)^2 (1 + x^4)^2 (1 + x^6)^2 (1 + x^8)^2 (1 + x^9)^2 \cdots$$

**Remark.** It is true that $1 + 2x$ is a square in $\mathbb{F}_3[[x]]$. In general, $f(x) \in \mathbb{F}_p[[x]]$ can be written as

$$f(x) = cx^n \cdot q(x)$$

where $q(x) \in Q$. If $n$ is even and $c$ is a square in $\mathbb{F}_p$, then $f(x)$ is a square in $\mathbb{F}_p[[x]]$. This is easily proved by inductively solving the system of equations induced by

$$q(x) = g(x)^2.$$ 

Since $q(x)$ always has a square root, the condition is also necessary.

**Lemma 4.2.** Each $q(x) \in Q$ can be uniquely written as

$$q(x) = (1 + x)^{\alpha_1} (1 + x^2)^{\alpha_2} (1 + x^3)^{\alpha_3} \cdots$$

where $\alpha_i \in \mathbb{Z}$ and $0 \leq \alpha_i < p$.

**Proof.** The existence of this factorization is obvious. So suppose that we have different factorizations for $q(x)$, say

$$q(x) = (1 + x)^{\beta_1} (1 + x^2)^{\beta_2} (1 + x^3)^{\beta_3} \cdots = (1 + x)^{\alpha_1} (1 + x^2)^{\alpha_2} (1 + x^3)^{\alpha_3} \cdots .$$

Choose the smallest $i \in \mathbb{N}^+$ such that $\beta_i \neq \alpha_i$. Then

$$1 + x^i = (1 + x^i)^{\beta_i} (1 + x^{i+1})^{\beta_{i+1}} \cdots = (1 + x^i)^{\alpha_i} (1 + x^{i+1})^{\alpha_{i+1}} \cdots$$
since both are equal to
\[
q(x) = \prod_{k=1}^{i-1} (1 + x^k)^{\alpha_k}.
\]
Expanding each side of (1) we have
\[
1 + \beta_i x^i + O(x^{i+1}) = 1 + \alpha_i x^i + O(x^{i+1})
\]
where \(\beta\) is just the image of \(z\) \(\in\mathbb{Z}\) under the quotient map onto \(\mathbb{F}_p\). But this implies that \(\beta_i = \alpha_i\) since \(0 \leq \beta, \alpha < p\); hence, the factorization is unique. \(\square\)

Recall that for any \(n \in \mathbb{N}\), \(\nu_p(n) = a\) where \(p^a\) divides \(n\) but no larger power of \(p\) divides \(n\).

**Definition 4.3.** For \(n \in \mathbb{Z}\), we define
\[
\rho(n) := \frac{n}{p^{\nu_p(n)}}.
\]

**Remark.** We omit \(p\) from the notation, since our \(p\) will be fixed throughout.

**Theorem 4.4.** Consider \(\mathbb{F}_p[[x]]\), and recall that its unit group decomposes as \(\mathbb{F}_p^* \oplus Q\). Then
\[
Q \cong \bigoplus_{\mathbb{N}_0} \mathbb{Z}_p,
\]
where \(\mathbb{Z}_p\) is the \(p\)-adic integers.

**Proof.** Consider a general element \(q(x) \in Q\). Then
\[
q(x) = (1 + x)^{\alpha_1} (1 + x^2)^{\alpha_2} (1 + x^3)^{\alpha_3} \cdots
\]
where \(\alpha_i \in \mathbb{Z}\) and \(0 \leq \alpha_i < p\). For clarity, we will write this in a vector notation:
\[
q(x) = [\alpha_1, \alpha_2, \alpha_3, \ldots].
\]

Consider the following map: \(\phi : Q \to \bigoplus_{(i,p)=1} (\mathbb{Z}_p)_i :\)
\[
[\alpha_1, \alpha_2, \alpha_3, \ldots] \mapsto [\alpha_1 + \alpha_p \cdot p + \alpha_p^2 \cdot p^2 + \cdots, \ldots, \alpha_i + \alpha_{ip^2} \cdot p^2 + \cdots, \ldots].
\]
We will show that \(\phi\) is an isomorphism. First, notice that it is identity preserving, and surjective. It is a homomorphism because
\[
(1 + x^i)^{\alpha_p} = (1 + x^ip)^{\alpha_p} (\in \mathbb{F}_p[[x]]) \iff (pa_i)p^{\nu_p(i)} = \alpha_i p^{\nu_p(i)+1} (\in (\mathbb{Z}_p)_{p^{\nu_p(i)}}).
\]
Finally, \(\phi\) is injective because \(q(x) = [\alpha_1, \alpha_2, \alpha_3, \ldots] \in \text{Ker}(\phi) \iff \alpha_i = 0\) for all \(i \in \mathbb{N}^+\). The result follows immediately, since there are countably many integers relatively prime to \(p\). \(\square\)

We will now clarify what we meant at the end of the last section. Since \(\mathbb{F}_p[[x]]\) is the inverse limit of \(\{\mathbb{F}_p[x]/(x^i)\}_{i \in \mathbb{N}^+}\), and since the unit functor commutes with
inverse limit, every finite group

\[ U(\mathbb{F}_p[x]/\langle x^k \rangle) \]

is realized as a quotient of \( U(\mathbb{F}_p[[x]]) \).
Appendix A. Finite Abelian $p$-groups

Here we prove some results about finite abelian $p$-groups, i.e. an abelian group $A$ of order $p^k$. We eventually will give a complete description of any such group based on the orders of its elements. This is used to recognize the isomorphism class of $Q$ in section 3.

Recall that in $\mathbb{Z}/p^k \mathbb{Z}$, there are $\phi(p^k) = p^k - p^{k-1}$ many elements of order $p^k$, where $\phi$ is the totient function. We would like to extend this idea to groups like $\mathbb{Z}/p^k \mathbb{Z} \oplus \mathbb{Z}/p^k \mathbb{Z}$, and eventually to all finite abelian $p$-groups.

**Proposition A.1.** Let $G = (\mathbb{Z}/p^k \mathbb{Z})^a$. Then there are $p^ka - p^{(k-1)a}$ elements in $G$ of order $p^k$.

**Proof.** We proceed by induction on $a$. If $a = 1$, the result is as above. So consider $(\mathbb{Z}/p^k \mathbb{Z})^a = (\mathbb{Z}/p^k \mathbb{Z}) \oplus (\mathbb{Z}/p^k \mathbb{Z})^{a-1}$.

We know that there are $p^k - p^{k-1}$ elements in the first component of order $p^k$; these can be paired with any of the remaining $p^{k(a-1)}$ elements in the second component. If the first component contains one of the $p^{k-1}$ elements of order less than $p^k$, we can still pair it with an element of order $p^k$ in the second component. By induction, there are $p^{k(a-1)} - p^{(k-1)(a-1)}$ elements of this type. Thus, in total, we have

$$(p^k - p^{k-1})(p^{k(a-1)}) + p^{k-1}(p^{k(a-1)} - p^{(k-1)(a-1)}) = p^{ka} - p^{(k-1)a}.$$  □

**Corollary A.2.** Let $G = (\mathbb{Z}/p^k \mathbb{Z})^a$. Then there are $p^{ja} - p^{(j-1)a}$ elements in $G$ of order $p^j$.

**Proof.** Let $i = k - j$. Then there is an exact sequence

$$0 \longrightarrow (\mathbb{Z}/p^j \mathbb{Z})^a \stackrel{p}{\longrightarrow} (\mathbb{Z}/p^k \mathbb{Z})^a \longrightarrow (\mathbb{Z}/p^j \mathbb{Z})^a \longrightarrow 0$$

where $p(z + \langle p^j \rangle) = z + p^j \cdot (\langle p^j \rangle)$ (applied to the $k^{th}$ component). It follows that every element of order $p^j$ in $(\mathbb{Z}/p^k \mathbb{Z})^a$ is the image of an element of order $p^j$ in $(\mathbb{Z}/p^j \mathbb{Z})^a$, so the previous theorem implies the result.  □

**Theorem A.3.** Let $A$ be a finite abelian $p$-group of order $p^k$. Then there exist numbers $e_i \in \mathbb{N}$, $1 \leq i \leq k$ so that

$$A \cong (\mathbb{Z}/p^k \mathbb{Z})^{e_k} \oplus \cdots \oplus (\mathbb{Z}/p^1 \mathbb{Z})^{e_1}.$$  

Furthermore, if $1 \leq j \leq k$, there are $p^j \sum_{i=j}^{k} e_i + \sum_{i=1}^{j-1} i e_i - p^{(j-1)} \sum_{i=j}^{k} e_i + \sum_{i=1}^{j-1} i e_i$ elements of order $p^j$. 

Proof. The first statement is a corollary of the classification of finite abelian groups. Consider that there are
\[ p^{(j-1) \sum_{i=j}^{k} e_i + \sum_{i=1}^{j-1} ie_i} \]
elements of order less than \( p^j \). Then the difference of this form at \( j+1 \) and \( j \) counts elements of order less than \( p^{j+1} \) and not less than \( p^j \), i.e. elements of order \( p^j \). □

The usefulness of this formula for finding the isomorphism class of a given \( p \)-group is given when we factor the form; in particular, there are
\[ p^{\sum_{i=1}^{k} ie_i - \sum_{i=1}^{j-1} ie_i + (j-1)} \left( p^{\sum_{i=j}^{k} e_i} - 1 \right) \]
elements of order \( p^j \). Thus, particularly if \( p \neq 2 \), then knowing the number of elements of each order allows one to easily read off the exponents \( \{e_i\} \), thus determining the isomorphism class.

References

