1 Polynomials over Finite Fields

In all that follows $\mathbb{F}$ will denote a finite field with $q$ elements. The model for such a field is $\mathbb{Z}/p\mathbb{Z}$, where $p$ is a prime number. This field has $p$ elements. In general the number of elements in a finite field is a power of a prime, $q = p^f$. Of course, $p$ is the characteristic of $\mathbb{F}$.

Let $A = \mathbb{F}[T]$, the polynomial ring over $\mathbb{F}$. $A$ has many properties in common with the ring of integers $\mathbb{Z}$. Both are principal ideal domains, both have a finite unit group, and both have the property that every residue class ring modulo a non-zero ideal has finitely many elements. We will verify all this shortly. The result is that many of the number theoretic questions we ask about $\mathbb{Z}$ have their analogues for $A$. We will explore these in some detail.

Every element in $A$ has the form $f(T) = \alpha_0 T^n + \alpha_1 T^{n-1} + \cdots + \alpha_n$. If $\alpha_0 \neq 0$ we say that $f$ has degree $n$, notationally $\deg(f) = n$. In this case we set $\text{sgn}(f) = \alpha_0$ and call this element of $\mathbb{F}^*$ the sign of $f$. Note the following very important properties of these functions. If $f$ and $g$ are non-zero polynomials we have

$$\deg(fg) = \deg(f) + \deg(g) \quad \text{and} \quad \text{sgn}(fg) = \text{sgn}(f)\text{sgn}(g).$$

$$\deg(f + g) \leq \max(\deg(f), \deg(g)).$$

In the second line, equality holds if $\deg(f) \neq \deg(g)$.

If $\text{sgn}(f) = 1$ we say that $f$ is a monic polynomial. Monic polynomials play the role of positive integers. It is sometimes useful to define the sign of the zero polynomial to be 0 and its degree to be $-\infty$. The above properties of degree then remain true without restriction.
Proposition 1.1. Let \( f, g \in A \) with \( g \neq 0 \). Then there exist elements \( q, r \in A \) such that \( f = qg + r \) and \( r \) is either 0 or \( \deg(r) < \deg(g) \). Moreover, \( q \) and \( r \) are uniquely determined by these conditions.

Proof. Let \( n = \deg(f) \), \( m = \deg(g) \), \( \alpha = \text{sgn}(f) \), \( \beta = \text{sgn}(g) \). We give the proof by induction on \( n = \deg(f) \). If \( n < m \), set \( q = 0 \) and \( r = f \). If \( n \geq m \), we note that \( f_1 = f - \alpha \beta^{-1} T^{n-m} g \) has smaller degree than \( f \). By induction, there exist \( q_1, r_1 \in A \) such that \( f_1 = q_1 g + r_1 \) with \( r_1 \) being either 0 or with degree less than \( \deg(g) \). In this case, set \( q = \alpha \beta^{-1} T^{n-m} + q_1 \) and \( r = r_1 \) and we are done.

If \( f = qg + r = q'g + r' \), then \( g \) divides \( r - r' \) and by degree considerations we see \( r = r' \). In this case, \( qg = q'g \) so \( q = q' \) and the uniqueness is established.

This proposition shows that \( A \) is a Euclidean domain and thus a principal ideal domain and a unique factorization domain. It also allows a quick proof of the finiteness of the residue class rings.

Proposition 1.2. Suppose \( g \in A \) and \( g \neq 0 \). Then \( A/gA \) is a finite ring with \( q^{\deg(g)} \) elements.

Proof. Let \( m = \deg(g) \). By Proposition 1.1 one easily verifies that \( \{ r \in A \mid \deg(r) < m \} \) is a complete set of representatives for \( A/gA \). Such elements look like

\[ r = \alpha_0 T^{m-1} + \alpha_1 T^{m-2} + \cdots + \alpha_{m-1} \quad \text{with} \quad \alpha_i \in F. \]

Since the \( \alpha_i \) vary independently through \( F \) there are \( q^m \) such polynomials and the result follows.

Definition. Let \( g \in A \). If \( g \neq 0 \), set \( |g| = q^{\deg(g)} \). If \( g = 0 \), set \( |g| = 0 \).

\(|g|\) is a measure of the size of \( g \). Note that if \( n \) is an ordinary integer, then its usual absolute value, \(|n|\), is the number of elements in \( \mathbb{Z}/n\mathbb{Z} \). Similarly, \(|g|\) is the number of elements in \( A/gA \). It is immediate that \(|fg| = |f| \cdot |g|\) and \(|f + g| \leq \max(|f|, |g|)\) with equality holding if \(|f| \neq |g|\).

It is a simple matter to determine the group of units in \( A, A^* \). If \( g \) is a unit, then there is an \( f \) such that \( fg = 1 \). Thus, 0 = \( \deg(1) = \deg(f) + \deg(g) \) and so \( \deg(f) = \deg(g) = 0 \). The only units are the non-zero constants and each such constant is a unit.

Proposition 1.3. The group of units in \( A \) is \( \mathbb{F}^* \). In particular, it is a finite cyclic group with \( q - 1 \) elements.

Proof. The only thing left to prove is the cyclicity of \( \mathbb{F}^* \). This follows from the very general fact that a finite subgroup of the multiplicative group of a field is cyclic.

In what follows we will see that the number \( q - 1 \) often occurs where the number 2 occurs in ordinary number theory. This stems from the fact that the order of \( \mathbb{Z}^* \) is 2.
Proposition 1.1. Let \( f, g \in A \) with \( g \neq 0 \). Then there exist elements \( q, r \in A \) such that \( f = qg + r \) and \( r \) is either 0 or \( \deg(r) < \deg(g) \). Moreover, \( q \) and \( r \) are uniquely determined by these conditions.

**Proof.** Let \( n = \deg(f) \), \( m = \deg(g) \), \( \alpha = \text{sgn}(f) \), \( \beta = \text{sgn}(g) \). We give the proof by induction on \( n = \deg(f) \). If \( n < m \), set \( q = 0 \) and \( r = f \). If \( n \geq m \), we note that \( f_1 = f - \alpha \beta^{-1}T^{n-m}g \) has smaller degree than \( f \). By induction, there exist \( q_1, r_1 \in A \) such that \( f_1 = q_1g + r_1 \) with \( r_1 \) being either 0 or with degree less than \( \deg(g) \). In this case, \( q = \alpha \beta^{-1}T^{n-m} + q_1 \) and \( r = r_1 \) and we are done.

If \( f = qg + r = q'g + r' \), then \( g \) divides \( r - r' \) and by degree considerations we see \( r = r' \). In this case, \( qg = q'g \) so \( q = q' \) and the uniqueness is established.

This proposition shows that \( A \) is a Euclidean domain and thus a principal ideal domain and a unique factorization domain. It also allows a quick proof of the finiteness of the residue class rings.

**Proposition 1.2.** Suppose \( g \in A \) and \( g \neq 0 \). Then \( A/gA \) is a finite ring with \( q^{\deg(g)} \) elements.

**Proof.** Let \( m = \deg(g) \). By Proposition 1.1 one easily verifies that \( \{ r \in A \mid \deg(r) < m \} \) is a complete set of representatives for \( A/gA \). Such elements look like

\[
r = \alpha_0 T^{m-1} + \alpha_1 T^{m-2} + \cdots + \alpha_{m-1} \quad \text{with} \quad \alpha_i \in \mathbb{F}.
\]

Since the \( \alpha_i \) vary independently through \( \mathbb{F} \) there are \( q^m \) such polynomials and the result follows.

**Definition.** Let \( g \in A \). If \( g \neq 0 \), set \( |g| = q^{\deg(g)} \). If \( g = 0 \), set \( |g| = 0 \).

\(|g|\) is a measure of the size of \( g \). Note that if \( n \) is an ordinary integer, then its usual absolute value, \(|n|\), is the number of elements in \( \mathbb{Z}/n\mathbb{Z} \). Similarly, \(|g|\) is the number of elements in \( A/gA \). It is immediate that \(|fg| = |f||g|\) and \( |f + g| \leq \max(|f|, |g|) \) with equality holding if \( |f| \neq |g| \).

It is a simple matter to determine the group of units in \( A, A^* \). If \( g \) is a unit, then there is an \( f \) such that \( fg = 1 \). Thus, \( 0 = \deg(1) = \deg(f) + \deg(g) \) and so \( \deg(f) = \deg(g) = 0 \). The only units are the non-zero constants and each such constant is a unit.

**Proposition 1.3.** The group of units in \( A \) is \( \mathbb{F}^* \). In particular, it is a finite cyclic group with \( q - 1 \) elements.

**Proof.** The only thing left to prove is the cyclicity of \( \mathbb{F}^* \). This follows from the very general fact that a finite subgroup of the multiplicative group of a field is cyclic.

In what follows we will see that the number \( q - 1 \) often occurs where the number 2 occurs in ordinary number theory. This stems from the fact that the order of \( \mathbb{Z}^* \) is 2.

By definition, a non-constant polynomial \( f \in A \) is irreducible if it cannot be written as a product of two polynomials, each of positive degree. Since every ideal in \( A \) is principal, we see that a polynomial is irreducible if and only if it is prime (for the definitions of divisibility, prime, irreducible, etc., see Ireland and Rosen [1]). These words will be used interchangeably. Every non-zero polynomial can be written uniquely as a non-zero constant times a monic polynomial. Thus, every ideal in \( A \) has a unique monic generator. This should be compared with the statement that every non-zero ideal in \( \mathbb{Z} \) has a unique positive generator. Finally, the unique factorization property in \( A \) can be sharpened to the following statement. Every \( f \in A, f \neq 0 \), can be written uniquely in the form

\[
f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_i^{e_i},
\]

where \( \alpha \in \mathbb{F}^* \), each \( P_i \) is a monic irreducible, \( P_i \neq P_j \) for \( i \neq j \), and each \( e_i \) is a non-negative integer.

The letter \( P \) will often be used for a monic irreducible polynomial in \( A \). We use \( p \) instead of \( p \) since the latter letter is reserved for the characteristic of \( F \). This is a bit awkward, but it is compensated for by being less likely to lead to confusion.

The next order of business will be to investigate the structure of the rings \( A/fA \) and the unit groups \( (A/fA)^* \). A valuable tool is the Chinese Remainder Theorem.

**Proposition 1.4.** Let \( m_1, m_2, \ldots, m_k \) be elements of \( A \) which are pairwise relatively prime. Let \( m = m_1 m_2 \cdots m_k \) and \( \phi_i \) be the natural homomorphism from \( A/mA \) to \( A/m_iA \). Then, the map \( \phi : A/mA \to A/m_1A \oplus A/m_2A \oplus \cdots \oplus A/m_kA \) given by

\[
\phi(a) = (\phi_1(a), \phi_2(a), \ldots, \phi_k(a))
\]

is a ring isomorphism.

**Proof.** This is a standard result which holds in any principal ideal domain (properly formulated it holds in much greater generality).

**Corollary.** The same map \( \phi \) restricted to the units of \( A, A^* \), gives rise to a group isomorphism

\[
(A/mA)^* \approx (A/m_1A)^* \times (A/m_2A)^* \times \cdots \times (A/m_kA)^*.
\]

**Proof.** This is a standard exercise. See Ireland and Rosen [1], Proposition 3.4.1.

Now, let \( f \in A \) be non-zero and not a unit and suppose that \( f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_i^{e_i} \) is its prime decomposition. From the above considerations we have

\[
(A/fA)^* \approx (A/P_1^{e_1} A)^* \times (A/P_2^{e_2} A)^* \times \cdots \times (A/P_i^{e_i} A)^*.
\]
This isomorphism reduces our task to that of determining the structure of the groups $(A/P^eA)^*$ where $P$ is an irreducible polynomial and $e$ is a positive integer. When $e = 1$ the situation is very similar to that in $Z$.

**Proposition 1.5.** Let $P \in A$ be an irreducible polynomial. Then, $(A/PA)^*$ is a cyclic group with $|P| - 1$ elements.

**Proof.** Since $A$ is a principal ideal domain, $PA$ is a maximal ideal and so $A/PA$ is a field. A finite subgroup of the multiplicative group of a field is cyclic. Thus $(A/PA)^*$ is cyclic. That the order of this group is $|P| - 1$ is immediate.

We now consider the situation when $e > 1$. Here we encounter something which is quite different in $A$ from the situation in $Z$. If $p$ is an odd prime number in $Z$ then it is a standard result that $(Z/p^eZ)^*$ is cyclic for all positive integers $e$. If $p = 2$ and $e \geq 3$ then $(Z/2^eZ)^*$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{e-2}$. The situation is very different in $A$.

**Proposition 1.6.** Let $P \in A$ be an irreducible polynomial and $e$ a positive integer. The order of $(A/P^eA)^*$ is $|P|^{e-1}(|P| - 1)$. Let $(A/P^eA)^{(1)}$ be the kernel of the natural map from $(A/P^eA)^*$ to $(A/PA)^*$. It is a $p$-group of order $|P|^{e-1}$. As $e$ tends to infinity, the minimal number of generators of $(A/P^eA)^{(1)}$ tends to infinity.

**Proof.** The ring $A/P^eA$ has only one maximal ideal $PA/P^eA$ which has $|P|^{e-1}$ elements. Thus, $(A/P^eA)^* = A/P^eA - PA/P^eA$ has $|P|^{e-1}(|P| - 1)$ number of elements. Since $(A/P^eA)^* \to (A/PA)^*$ is onto, and the latter group has $|P| - 1$ elements the assertion about the size of $(A/P^eA)^{(1)}$ follows. It remains to prove the assertion about the minimal number of generators. It is instructive to first consider the case $e = 2$. Every element in $(A/P^2A)^{(1)}$ can be represented by a polynomial of the form $a = 1 + bP$. Since we are working in characteristic $p$ we have $a^p = 1 + b^pP^p \equiv 1 \pmod{P^2}$. So, we have a group of order $|P|$ with exponent $p$. If $q = p^f$ it follows that $(A/P^2A)^{(1)}$ is a direct sum of $f \deg(P)$ number of copies of $Z/pZ$. This is a cyclic group only under the very restrictive conditions that $q = p$ and $\deg(P) = 1$.

To deal with the general case, suppose that $s$ is the smallest integer such that $p^s \geq e$. Since $(1 + bP)^{p^s} = 1 + (bP)^{p^s} \equiv 1 \pmod{P^s}$ we have that raising to the $p^s$-power annihilates $G = (A/P^eA)^{(1)}$. Let $d$ be the minimal number of generators of this group. It follows that there is an onto map from $(Z/p^sZ)^d$ onto $G$. Thus, $p^{ds} \geq p^d \deg(P)(e - 1)$ and so

$$d \geq \frac{f \deg(P)(e - 1)}{s}.$$

Since $s$ is the smallest integer bigger than or equal to $\log_{p^f}(e)$ it is clear that $d \to \infty$ as $e \to \infty$. 
1. Polynomials over Finite Fields

It is possible to do a much closer analysis of the structure of these groups, but it is not necessary to do so now. The fact that these groups get very complicated does cause problems in the more advanced parts of the theory.

We have developed more than enough material to enable us to give interesting analogues of the Euler $\phi$-function and the little theorems of Euler and Fermat.

To begin with, let $f \in A$ be a non-zero polynomial. Define $\Phi(f)$ to be the number of elements in the group $(A/fA)^*$. We can give another characterization of this number which makes the relation to the Euler $\phi$-function even more evident. We have seen that $\{r \in A | \deg(r) < \deg(f)\}$ is a set of representatives for $A/fA$. Such an $r$ represents a unit in $A/fA$ if and only if it is relatively prime to $f$. Thus $\Phi(f)$ is the number of non-zero polynomials of degree less than $\deg(f)$ and relatively prime to $f$.

**Proposition 1.7.**

$$\Phi(f) = |f| \prod_{P|f} (1 - \frac{1}{|P|}).$$

**Proof.** Let $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ be the prime decomposition of $f$. By the corollary to Propositions 1.4 and by Proposition 1.6, we see that

$$\Phi(f) = \prod_{i=1}^{t} \Phi(P_i^{e_i}) = \prod_{i=1}^{t} (|P_i|^{e_i} - |P_i|^{e_i-1}),$$

from which the result follows immediately.

The similarity of the formula in this proposition to the classical formula for $\phi(n)$ is striking.

**Proposition 1.8.** If $f \in A$, $f \neq 0$, and $a \in A$ is relatively prime to $f$, i.e., $(a, f) = 1$, then

$$a^{\Phi(f)} \equiv 1 \pmod{f}.$$

**Proof.** The group $(A/fA)^*$ has $\Phi(f)$ elements. The coset of a modulo $f$, $\bar{a}$, lies in this group. Thus, $\bar{a}^{\Phi(f)} = 1$ and this is equivalent to the congruence in the proposition.

**Corollary.** Let $P \in A$ be irreducible and $a \in A$ be a polynomial not divisible by $P$. Then,

$$a^{|P|-1} \equiv 1 \pmod{P}.$$

**Proof.** Since $P$ is irreducible, it is relatively prime to $a$ if and only if it does not divide $a$. The corollary follows from the proposition and the fact that for an irreducible $P$, $\Phi(P) = |P| - 1$ (Proposition 1.5).

It is clear that Proposition 1.8 and its corollary are direct analogues of Euler’s little theorem and Fermat’s little theorem. They play the same very important role in this context as they do in elementary number theory. By
way of illustration we proceed to the analogue of Wilson's theorem. Recall that this states that \((p - 1)! \equiv -1 \pmod{p}\) where \(p\) is a prime number.

**Proposition 1.9.** Let \(P \in A\) be irreducible of degree \(d\). Suppose \(X\) is an indeterminate. Then,

\[
X^{\left|P\right| - 1} - 1 \equiv \prod_{0 \leq \deg(f) < d} (X - f) \pmod{P}.
\]

**Proof.** Recall that \(\{f \in A \mid \deg(f) < d\}\) is a set of representatives for the cosets of \(A/PA\). If we throw out \(f = 0\) we get a set of representatives for \((A/PA)^*\). We find

\[
X^{\left|P\right| - 1} - 1 = \prod_{0 \leq \deg(f) < d} (X - f),
\]

where the bars denote cosets modulo \(P\). This follows from the corollary to Proposition 1.8 since both sides of the equation are monic polynomials in \(X\) with the same set of roots in the field \(A/PA\). Since there are \(|P| - 1\) roots and the difference of the two sides has degree less than \(|P| - 1\), the difference of the two sides must be 0. The congruence in the Proposition is equivalent to this assertion.

**Corollary 1.** Let \(d\) divide \(|P| - 1\). The congruence \(X^d \equiv 1 \pmod{P}\) has exactly \(d\) solutions. Equivalently, the equation \(X^d = 1\) has exactly \(d\) solutions in \((A/PA)^*\).

**Proof.** We prove the second assertion. Since \(d \mid |P| - 1\) it follows that \(X^d - 1\) divides \(X^{|P| - 1} - 1\). By the proposition, the latter polynomial splits as a product of distinct linear factors. Thus so does the former polynomial. This establishes the result.

**Corollary 2.** With the same notation,

\[
\prod_{0 \leq \deg(f) < \deg P} f \equiv -1 \pmod{P}.
\]

**Proof.** Just set \(X = 0\) in the proposition. If the characteristic of \(F\) is odd \(|P| - 1\) is even and the result follows. If the characteristic is 2 then the result also follows since in characteristic 2 we have \(-1 = 1\).

The above corollary is the polynomial version of Wilson's theorem. It's interesting to note that the left-hand side of the congruence only depends on the degree of \(P\) and not on \(P\) itself.

As a final topic in this chapter we give some of the theory of \(d\)-th power residues. This will be of importance in Chapter 3 when we discuss quadratic reciprocity and more general reciprocity laws for \(A\).
If $f \in A$ is of positive degree and $a \in A$ is relatively prime to $f$, we say that $a$ is a $d$-th power residue modulo $f$ if the equation $x^d \equiv a \pmod{f}$ is solvable in $A$. Equivalently, $\bar{a}$ is a $d$-th power in $(A/fA)\ast$.

Suppose $f = \alpha P_1^{\epsilon_1} P_2^{\epsilon_2} \ldots P_t^{\epsilon_t}$ is the prime decomposition of $f$. Then it is easy to check that $\alpha$ is a $d$-th power residue modulo $f$ if and only if $\alpha$ is a $d$-th power residue modulo $P_i^{\epsilon_i}$ for all $i$ between 1 and $t$. This reduces the problem to the case where the modulus is a prime power.

**Proposition 1.10.** Let $P$ be irreducible and $a \in A$ not divisible by $P$. Assume $d$ divides $|P|-1$. The congruence $x^d \equiv a \pmod{P^e}$ is solvable if and only if

$$\frac{|P|-1}{d} \equiv 1 \pmod{P}.$$ 

There are $\frac{\Phi(P^e)}{d}$ $d$-th power residues modulo $P^e$.

**Proof.** Assume to begin with that $e = 1$.

If $b^d \equiv a \pmod{P}$, then $b^{(P^e-1)} \equiv b^{P^e-1} \equiv 1 \pmod{P^e}$ by the corollary to Proposition 1.8. This shows the condition is necessary. To show it is sufficient recall that by Corollary 1 to Proposition 1.9 all the $d$-th roots of unity are in the field $A/P^e$. Consider the homomorphism from $(A/P^e)\ast$ to itself given by raising to the $d$-th power. It’s kernel has order $d$ and its image is the $d$-th powers. Thus, there are precisely $\frac{|P|-1}{d}$ $d$-th power residues in $(A/P^e)\ast$. We have seen that they all satisfy $x^{|P|-1} - 1 = 0$. Thus, they are precisely the roots of this equation. This proves all assertions in the case $e = 1$.

To deal with the remaining cases, we employ a little group theory. The natural map (i.e., reduction modulo $P^e$) is a homomorphism from $(A/P^eA)\ast$ onto $(A/P^eA)\ast$ and the kernel is a $p$-group as follows from Proposition 1.6. Since the order of $(A/P^eA)\ast$ is $|P|-1$ which is prime to $p$ it follows that $(A/P^eA)\ast$ is the direct product of a $p$-group and a copy of $(A/P^eA)\ast$. Since $(d,p) = 1$, raising to the $d$-th power in an abelian $p$-group is an automorphism. Thus, $a \in A$ is a $d$-th power modulo $P^e$ if and only if $a$ is a $d$-th power modulo $P$. The latter has been shown to hold if and only if $a^{(P^e-1)/P} \equiv 1 \pmod{P^e}$. Now consider the homomorphism from $(A/P^eA)\ast$ to itself given by raising to the $d$-th power. It easily follows from what has been said that the kernel has $d$ elements and the image is the subgroup of $d$-th powers. It follows that the latter group has order $\frac{\Phi(P^e)}{d}$.

**Exercises**

1. If $m \in A = F[T]$, and $\deg(m) > 0$, show that $q - 1 \mid \Phi(m)$.

2. If $q = p$ is a prime number and $P \in A$ is an irreducible, show $(F[T]/P^2A)\ast$ is cyclic if and only if $\deg P = 1$. 

The above corollary is the polynomial version of Wilson’s theorem. It’s interesting to note that the left-hand side of the congruence only depends on the degree of $P$ and not on $P$ itself.

As a final topic in this chapter we give some of the theory of $d$-th power residues. This will be of importance in Chapter 3 when we discuss quadratic reciprocity and more general reciprocity laws for $A$. 

of illustration we proceed to the analogue of Wilson’s theorem. Recall that this states that $(p - 1)! \equiv -1 \pmod{p}$ where $p$ is a prime number.
3. Suppose \( m \in A \) is monic and that \( m = m_1m_2 \) is a factorization into two monics which are relatively prime and of positive degree. Show \((A/mA)^*\) is not cyclic except possibly in the case \( q = 2 \) and \( m_1 \) and \( m_2 \) have relatively prime degrees.

4. Assume \( q \neq 2 \). Determine all \( m \) for which \((A/mA)^*\) is cyclic (see the proof of Proposition 1.6).

5. Suppose \( d \mid q - 1 \). Show \( x^d \equiv -1 \mod F \) is solvable if and only if \((-1)^{\frac{q-1}{d}} \deg P = \pm 1\).

6. Show \( \prod_{\alpha \in F^*} \alpha = -1 \).

7. Let \( P \in A \) be a monic irreducible. Show

\[
\prod_{\deg f < d} f \equiv \pm 1 \pmod{P},
\]

where \( d = \deg P \). Determine the sign on the right-hand side of this congruence.

8. For an integer \( m \geq 1 \) define \([m] = T^m - T\). Show that \([m] \) is the product of all monic irreducible polynomials \( P(T) \) such that \( \deg P(T) \) divides \( m \).

9. Working in the polynomial ring \( \mathbb{F}[u_0, u_1, \ldots, u_n] \), define \( D(u_0, u_1, \ldots, u_n) = \det [u_i^j] \), where \( i, j = 0, 1, \ldots, n \). This is called the Moore determinant. Show

\[
D(u_0, u_1, \ldots, u_n) = \prod_{i=0}^{n} \prod_{c_{-1} \in \mathbb{F}} \prod_{c_0 \in \mathbb{F}} (u_i + c_{i-1}u_{i-1} + \cdots + c_0u_0).
\]

Hint: Show each factor on the right divides the determinant and then count degrees.

10. Define \( F_j = \prod_{i=0}^{j-1}(T^{q^i} - T^{q^j}) = \prod_{i=0}^{j-1}(j - i)^{q^j} \). Show that

\[
D(1, T, T^2, \ldots, T^n) = \prod_{j=0}^{n} F_j.
\]

Hint: Use the fact that \( D(1, T, T^2, \ldots, T^n) \) can be viewed as a Vandermonde determinant.

11. Show that \( F_j \) is the product of all monic polynomials in \( A \) of degree \( j \).

12. Define \( L_j = \prod_{i=1}^{j}(T^{q^i} - T) = \prod_{i=1}^{j} |i| \). Use Exercise 8 to prove that \( L_j \) is the least common multiple of all monics of degree \( j \).
3. Suppose \( m \in A \) is monic and that \( m = m_1 m_2 \) is a factorization into two monics which are relatively prime and of positive degree. Show \((A/mA)^*\) is not cyclic except possibly in the case \( q = 2 \) and \( m_1 \) and \( m_2 \) have relatively prime degrees.

4. Assume \( q \neq 2 \). Determine all \( m \) for which \((A/mA)^*\) is cyclic (see the proof of Proposition 1.6).

5. Suppose \( d \mid q - 1 \). Show \( x^d \equiv -1 \pmod{P} \) is solvable if and only if \((-1)^{\frac{q - 1}{d}} \deg P = 1\).

6. Show \( \prod_{\alpha \in F} \alpha = -1 \).

7. Let \( P \in A \) be a monic irreducible. Show

\[
\prod_{\deg f < d \atop f \text{ monic}} f \equiv \pm 1 \pmod{P},
\]

where \( d = \deg P \). Determine the sign on the right-hand side of this congruence.

8. For an integer \( m \geq 1 \) define \([m] = T^m - T\). Show that \([m]\) is the product of all monic irreducible polynomials \( P(T) \) such that \( \deg P(T) \) divides \( m \).

9. Working in the polynomial ring \( F[u_0, u_1, \ldots, u_n] \), define \( D(u_0, u_1, \ldots, u_n) = \det |u_i^r| \), where \( i, j = 0, 1, \ldots, n \). This is called the Moore determinant. Show

\[
D(u_0, u_1, \ldots, u_n) = \prod_{i=0}^{n} \prod_{c_{i-1} \in F} \cdots \prod_{c_0 \in F} (u_i + c_{i-1} u_{i-1} + \cdots + c_0 u_0).
\]

Hint: Show each factor on the right divides the determinant and then count degrees.

10. Define \( F_j = \prod_{i=0}^{j-1} (T^{q^i} - T^{q^i}) = \prod_{i=0}^{j-1} |j - i|^{q^i} \). Show that

\[
D(1, T, T^2, \ldots, T^n) = \prod_{j=0}^{n} F_j.
\]

Hint: Use the fact that \( D(1, T, T^2, \ldots, T^n) \) can be viewed as a Vandermonde determinant.

11. Show that \( F_j \) is the product of all monic polynomials in \( A \) of degree \( j \).

12. Define \( L_j = \prod_{i=1}^{j} (T^{q^i} - T) = \prod_{i=1}^{j} [i] \). Use Exercise 8 to prove that \( L_j \) is the least common multiple of all monics of degree \( j \).

13. Show

\[
\prod_{\deg f < d} (u + f) = \frac{D(1, T, T^2, \ldots, T^{d-1}, u)}{D(1, T, T^2, \ldots, T^{d-1})}.
\]

14. Deduce from Exercise 13 that

\[
\prod_{\deg f < d} (u + f) = \sum_{j=0}^{d} (-1)^{d-j} \frac{F_d}{F_j L_j^{q^i}} u^{q^j}.
\]

15. Show that the product of all the non-zero polynomials of degree less than \( d \) is equal to \((-1)^d F_d / L_d \).

16. Prove that

\[
u \prod_{\deg f < d} \left( 1 - \frac{u}{f} \right) = \sum_{j=0}^{d} (-1)^j \frac{L_d}{F_j L_j^{q^i}} u^{q^j}.
\]

In the product the term corresponding to \( f = 0 \) is omitted.