1. Valuations

Definition 1.1. A valuation on a field $K$ is a function $|·| : K \to \mathbb{R}$ satisfying

1. $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$

((3') $|x + y| \leq \max(|x|, |y|)$)

If $|·|$ satisfies (3'), then it is called nonarchimedean. Otherwise, it is called archimedean.

Proposition 1.2. Let $|·|$ be a valuation on a field $K$. The followings are equivalent:

1. $|·|$ is nonarchimedean.
2. If $|\alpha| \leq 1$ for some $\alpha \in K$, then $|\alpha + 1| \leq 1$.
3. The set $\{|n| \mid n \in \mathbb{Z}\}$ is bounded.

Proof. Note that $|1||1| = |1|$ gives $|1| = 1$ because $|1| \neq 0$. Similarly, we have $|-1| = 1$.

(1) $\Rightarrow$ (2) If $|·|$ is nonarchimedean and $|\alpha| \leq 1$, then $|\alpha + 1| \leq \max(|\alpha|, |1|) = 1$.

(2) $\Rightarrow$ (3) For $n \geq 0$, we use induction on $n$ to get $|n| = |(n - 1) + 1| \leq 1$. For $n < 0$, we have $|n| = |-n|-1 = |-n| \leq 1$.

(3) $\Rightarrow$ (1) Suppose $|n| \leq N$ for all $n \in \mathbb{Z}$. Then for $x, y \in K$ and $r \in \mathbb{Z}_{\geq 0}$,

$$|x + y|^r = |(x + y)^r| = \left| \sum_{i=0}^{r} \binom{r}{i} x^i y^{r-i} \right|$$

$$\leq \sum_{i=0}^{r} |\binom{r}{i}| |x|^i |y|^{r-i}$$

$$\leq (r + 1)N \max(|x|^r, |y|^r)$$
because \((r_i) \in \mathbb{Z}\) and \(|x|^i|y|^{r_i-i} \leq \max(|x|^r, |y|^r)\) for all \(0 \leq i \leq r\). Thus we have
\[|x + y| \leq (r + 1)^{1/r} N^{1/r} \max(|x|, |y|)\]

Letting \(r \to \infty\) shows that \(|\cdot|\) is nonarchimedean. \(\square\)

**Example 1.3.**
1. There is a trivial valuation on any field \(K\) defined by \(|x| = 1\) for \(x \neq 0\) and \(|0| = 0\).
2. If \(K\) is a finite field of order \(q^e\), then there is only trivial valuation on \(K\). This is because for each \(0 \neq x \in K\) we have \(x^{q^e-1} = 1\) and \(|x|^{q^e-1} = 1\). But \(|x| \in \mathbb{R}_{\geq 0}\), thus \(|x| = 1\).
3. If \(\text{char } K > 0\), then all valuations on \(K\) is nonarchimedean by 1.2(3).
4. We have an archimedean valuation \(|\cdot|_\infty : \mathbb{C} \to \mathbb{R}_{\geq 0}\) with \(|z|_\infty = |z|\) (usual complex absolute value).
5. For a prime number \(p\), we have \(|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}\) defined by \(|a|_p = \frac{1}{p^n}\) for \(a = p^mb^n \in \mathbb{Q}\) where \(b, c, m \in \mathbb{Z}\) and \((p, bc) = 1\). \(|\cdot|_p\) is a well-defined nonarchimedean valuation.
6. If we have an embedding \(\sigma : K \to \mathbb{C}\), then we can define the valuation \(|\cdot|_\sigma : K \to \mathbb{R}_{\geq 0}\) by \(|a|_\sigma = |\sigma(a)|_\infty\).

**Remark 1.4.** Any valuation \(|\cdot|\) gives a metric on \(K\) (thus a metric topology) by \(d_{|\cdot|}(x, y) = |x-y|\).

**Definition 1.5.** Two valuations \(|\cdot|_1, |\cdot|_2 : K \to \mathbb{R}\) are equivalent if \(|\cdot|_1 = |\cdot|_2^s\) for some \(s > 0\). (This means that they define the same topology on \(K\).)

**Lemma 1.6.** Suppose two nontrivial valuations \(|\cdot|_1\) and \(|\cdot|_2\) on \(K\) are not equivalent. Then there is \(x \in K\) such that \(|x|_1 < 1\) and \(|x|_2 \geq 1\).

**Proof.** Suppose that there is no such \(x \in K\) (i.e., \(|x|_1 < 1\) implies \(|x|_2 < 1\)). Choose \(y \in K\) with \(|y|_1 > 1\). (Such \(y\) always exists because \(|\cdot|_1\) is nontrivial thus there is some element \(z \neq 0\) having \(|z|_1 > 1\) or \(|z|_1 < 1\). In the latter case, we can take \(y = \frac{1}{z}\).) For \(x \in K\), choose \(\alpha \in \mathbb{R}\) satisfying \(|x|_1 = |y|^\alpha_1\). We can also take an increasing sequence of rational numbers \(\frac{m_i}{n_i} \in \mathbb{Q}\) converging to \(\alpha\). Now we have
\[|x|_1 = |y|^\alpha_1 > \left|\frac{m_i}{n_i}\right|\]
for all \(i\). \(\frac{m_i}{n_i} \geq 1\) implies \(\frac{m_i}{n_i} \geq 1\) for all \(i\) by assumption. This gives us \(|x|_2 > \left|\frac{m_i}{n_i}\right|\) for all \(i\), thus \(|x|_2 \geq |y|^\alpha_2\). On the other hand, by taking a decreasing sequence of rational numbers converging to \(\alpha\), we can get \(|x|_2 \leq |y|^\alpha_2\). Thus we get \(|x|_2 = |y|^\alpha_2\). This shows that
\[s = \frac{\log |x|_1}{\log |x|_2} = \frac{\log |y|_1}{\log |y|_2} > 0\]
is a constant for all \(x \in K\), thus \(|x|_1 = |x|_2^\alpha\). But this means \(|\cdot|_1\) and \(|\cdot|_2\) are equivalent. \(\square\)

**Theorem 1.7** (Weak Approximation Theorem). Let \(|\cdot|_1, |\cdot|_2, \cdots, |\cdot|_n\) be non-equivalent non-trivial valuations on \(K\), and \(a_1, \cdots, a_n \in K\). For any \(\epsilon > 0\), there is \(x \in K\) such that \(|x-a_i|_i < \epsilon\) for all \(i\).

**Proof.** **Step 1** : For \(0 \neq z \in K\),
\[\lim_{m \to \infty} \frac{z^m}{1 + z^m} = \begin{cases} 1 & \text{if } |z| > 1 \\ 0 & \text{if } |z| < 1 \end{cases}\]
If \(|z| > 1\), then
\[\left|\frac{z^m}{1 + z^m} - 1\right| = \frac{1}{|1 + z^m|} \leq \frac{1}{|z|^m - 1} \to 0\]
If $|z| < 1$, then
\[ \left| \frac{z^m}{1 + z^m} \right| = \frac{1}{1 + \frac{1}{z^m}} \leq \frac{1}{|1/z^m - 1|} \to 0 \]
as $m \to \infty$.

**Step 2**: There is $z \in K$ satisfying $|z| > 1$ and $|z|_j < 1$ for $j = 2, \ldots, n$.

We use induction on $n$. Suppose $n = 2$. There are $\alpha, \beta \in K$ such that $|\alpha|_1 < 1, |\alpha|_2 \geq 1$ and $|\beta|_1 \geq 1, |\beta|_2 < 1$ by the previous lemma. Take $z = \frac{\beta}{\alpha}$.

Suppose we have $z \in K$ satisfying $|z| > 1$ and $|z|_j < 1$ for $j = 2, \ldots, n - 1$. Choose $y \in K$ such that $|y|_1 > 1, |y|_n < 1$. If $|z|_n \leq 1$, then for large $m$, we have
\[ |z^m y|_1 > 1, |z^m y|_j < 1 \text{ for } j = 2, \ldots, n \]

If $|z|_n > 1$, then for large $m$,
\[ \left| \frac{z^m y}{1 + z^m} \right|_1 > 1, \left| \frac{z^m y}{1 + z^m} \right|_j < 1 \text{ for } j = 2, \ldots, n \]

by Step 1.

**Step 3**: proof of theorem

We can choose $y_i \in K$ satisfying $|y_i|_i > 1$ and $|y_i|_j < 1$ for $j \neq i$ by Step 2. Let $M = \max_{i,j} |a_i|_j$ and choose integers $m_i \in \mathbb{Z}$ such that
\[ \left| \frac{y_i^{m_i}}{1 + y_i^{m_i}} - 1 \right|_i < \frac{\epsilon}{nM} \quad \text{and} \quad \left| \frac{y_i^{m_i}}{1 + y_i^{m_i}} \right|_j < \frac{\epsilon}{nM} \text{ for } j \neq i \]

for all $i$ (by Step 1). Let $x = \sum_{i=1}^n \frac{a_i y_i^{m_i}}{1 + y_i^{m_i}}$, then
\[ |x - a_i|_i \leq |a_i|_i \left| \frac{y_i^{m_i}}{1 + y_i^{m_i}} - 1 \right|_i + \sum_{j \neq i} |a_j|_i \left| \frac{y_j^{m_j}}{1 + y_j^{m_j}} \right|_i < \epsilon \]

\[ \square \]

**Theorem 1.8** (Ostrowski). Every nontrivial valuation on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime $p$ or $|\cdot|_{\infty}$.

---

2. Counting irreducible polynomials over finite fields

**Theorem 2.1.** For any prime $p$ and $n \in \mathbb{N}$, there is a unique (up to isomorphism) finite field of order $p^n$, and that is the splitting field of $t^n - x \in \mathbb{F}_p[t]$ over $\mathbb{F}_p$.

**Theorem 2.2.** Let $F$ be a finite field of order $p^n$. Then $F \cong \mathbb{F}_p[t]/(f)$ for some irreducible polynomial $f(t) \in \mathbb{F}_p[t]$ of degree $n$.

**Proof.** Note that $F^\times$ is cyclic. Let $F^\times = \langle \gamma \rangle$ and define the map
\[ \phi : \mathbb{F}_p[t] \to F, \quad g(t) \mapsto g(\gamma) \]

$\phi$ is surjective because $F = \langle \gamma \rangle \cup \{0\}$. Now $F \cong \mathbb{F}_p[t]/\ker \phi$, and $\ker \phi = (f(t))$ for some irreducible polynomial $f$ because $\ker \phi$ is maximal and $\mathbb{F}_p[t]$ is a PID. \[ \square \]
Theorem 2.7. Let $F$ be a field.

For the polynomials of degree 2, only $x^2 + x + 1$ is irreducible, and others are not because $x^2 = x \cdot x, x^2 + 1 = (x + 1)^2$ and $x^2 + x = x(x + 1)$.

Theorem 2.5. In $\mathbb{F}_p[t]$, we have $t^{p^n} - t = \prod_{d|n} \prod_{\substack{\deg f = d \\ f \in \mathbb{F}_p[t]}} f$

Proof. Let $F$ be the splitting field of $t^{p^n} - t \in \mathbb{F}_p[t]$. Note that $\mathbb{F}_p$ is perfect (every irreducible polynomial over $\mathbb{F}_p$ is separable.) Suppose first $g \in \mathbb{F}_p[t]$ is an irreducible factor of $t^{p^n} - t$. Let $\alpha$ be a root of $g$, then we have

$$
\deg g = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [F : \mathbb{F}_p] = n
$$

Thus $g$ divides the right-hand side, and so does $t^{p^n} - t$ because $t^{p^n} - t$ is separable.

Conversely, let $h \in \mathbb{F}_p[t]$ be an irreducible, monic polynomial with degree $d | n$. Let $\beta$ be a root of $h$. Because $[\mathbb{F}_p(\beta) : \mathbb{F}_p] = d$, $\mathbb{F}_p(\beta)$ has order $p^d$, thus we have $\beta^{p^d} = \beta$. Since $d | n$, we have $\beta^{p^n} = (((\beta^{p^d})^{p^d})^{p^d})^{p^d} = \beta$. This shows that every root of $h$ is a root of $t^{p^n} - t$, i.e., $h | t^{p^n} - t$ because $h$ is separable.

Since both sides are monic, we have the desired equality. $\square$

Now we explain how we can count the number of irreducible polynomials in $\mathbb{F}_p[t]$ of a given degree $n$. We will use the following theorem of Möbius.

Theorem 2.6 (Möbius Inversion). Let $f, g : \mathbb{N} \to \mathbb{C}$ and $g(n) = \sum_{d|n} f(d)$. Then we have

$$
f(n) = \sum_{d|n} \mu(d) g \left( \frac{n}{d} \right)
$$

where

$$
\mu(n) = \begin{cases} 
(-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where } p_i's \text{ are distinct primes} \\
1 & \text{if } n = 1 \\
0 & \text{otherwise}
\end{cases}
$$

Theorem 2.7. Let $N_{p,n}$ be the number of irreducible monic polynomials of degree $n$ over $\mathbb{F}_p$. Then

$$
N_{p,n} = \frac{1}{n} \sum_{d|n} \mu(d)p^{\frac{n}{d}}
$$

Proof. We count the degree of both sides in 2.5

$$
p^n = \sum_{d|n} \sum_{\substack{\deg f = d \\ f \in \mathbb{F}_p[t]}} \deg f = \sum_{d|n} dN_{p,d}
$$

Now we apply the Möbius inversion to $f(n) = nN_{p,n}$ and $g(n) = p^n$.

Example 2.8. Let $n = q$ be a prime. Then,

$$
N_{p,q} = \frac{1}{q} \sum_{d|q} \mu(d)p^{\frac{q}{d}} = \frac{p^q - p}{q}
$$

Note that $p^q \equiv p (\text{mod } q)$. 4
3. Chevalley-Waring Theorem

In this section, we let $F$ be a finite field of order $q$ with characteristic $p$.

**Lemma 3.1.** Let $m \in \mathbb{N}$, then,

$$\sum_{x \in F} x^m = \begin{cases} -1 & \text{if } q - 1 \mid m \\ 0 & \text{otherwise} \end{cases}$$

**Proof.** If $q - 1 \mid m$, then $x^m = 1$ for all $x \in F^\times$. Thus, $\sum x^m = q - 1 = -1$. Suppose $q - 1 \nmid m$. Choose a generator of $y \in F^\times$, then $y^m \neq 1$. We have

$$\left( \sum_{x \in F} x^m \right) \left( 1 - y^m \right) = \sum_{x \in F} x^m - \sum_{x \in F} (xy)^m = 0$$

Therefore, $\sum x^m = 0$. $\square$

**Lemma 3.2.** Let $f \in F[t_1, t_2, \ldots, t_n]$ and suppose $\deg f < n(q - 1)$. Then $\sum_{x \in F^n} f(x) = 0$.

**Proof.** It is enough to show this for each monomials $t_1^{u_1} t_2^{u_2} \cdots t_n^{u_n} \in F[t_1, \ldots, t_n]$ with $\sum u_i < n(q - 1)$. We have

$$\sum_{(x_1, \ldots, x_n) \in F^n} x_1^{u_1} \cdots x_n^{u_n} = \prod_{i=1}^{n} \sum_{x_i \in F} x_i^{u_i} = 0$$

by Lemma 3.1 and the fact that $u_i < q - 1$ for some $i$. $\square$

**Theorem 3.3** (Chevalley-Waring). For $i = 1, 2, \ldots, r$, let $f_i \in F[t_1, \ldots, t_n]$ be polynomials satisfying $\sum_i \deg f_i < n$. Let

$$S = \{ x = (x_1, \ldots, x_n) \in F^n \mid f_i(x) = 0 \text{ for all } i \}$$

be the set of common zeros of $f_i$’s. Then, $|S| \equiv 0 \pmod{p}$.

**Proof.** Define

$$g(t_1, \ldots, t_n) = \prod_{i=1}^{r} (1 - f_i(t_1, \ldots, t_n)^{q-1})$$

Since

$$1 - f_i(x_1, \ldots, x_n)^{q-1} = \begin{cases} 1 & \text{if } f_i(x_1, \ldots, x_n) = 0 \\ 0 & \text{if } f_i(x_1, \ldots, x_n) \neq 0 \end{cases}$$

for $(x_1, \ldots, x_n) \in F^n$, we have

$$g(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } (x_1, \ldots, x_n) \in S \\ 0 & \text{if } (x_1, \ldots, x_n) \notin S \end{cases}$$

Note that $\deg g = (q - 1) \sum_i \deg f_i < n(q - 1)$. By Lemma 3.2,

$$|S| \equiv \sum_{x \in F^n} g(x) \equiv 0 \pmod{p}$$

$\square$

**Definition 3.4.** A field $F$ is called quasi-algebraically closed if every nonconstant homogeneous polynomial $f \in F[t_1, \ldots, t_n]$ has a nontrivial zero (i.e., not equal to $(0,0,\cdots,0)$) when $n > \deg f$. 

5
Corollary 3.5. Finite fields are quasi-algebraically closed.

Proof. By Chevalley-Waring, $p$ divides the number of zeros of every homogeneous polynomial $f \in F[t_1, \cdots, t_n]$ with $\deg f < n$. Since we already have a trivial zero, $f$ has a nontrivial zero in $F^n$. □

4. POLYNOMIAL FUNCTIONS

Let $R$ be a ring and $\text{Func}(R, R) = \{ f : R \to R \mid f \text{ is a function}\}$ (we don’t assume any property of $f$) be the ring of functions from $R$ to $R$. The ring structure of $\text{Func}(R, R)$ is given pointwise: $(f + g)(a) = f(a) + g(a)$, $(fg)(a) = f(a)g(a)$. We consider the map

$$\Phi = \Phi_R : R[t] \to \text{Func}(R, R)$$

$$f(t) \mapsto (\Phi(f) : a \mapsto f(a))$$

Definition 4.1. A function $f \in \text{Func}(R, R)$ is called a polynomial function if $f \in \text{Im} \Phi$.

Example 4.2. $\Phi$ is not surjective in general. Let $R = \mathbb{R}$ and consider $\exp \in \text{Func}(\mathbb{R}, \mathbb{R})$ where $\exp(a) = e^a$. For any polynomial $f(t) \in \mathbb{R}[t]$, we have $\lim_{t \to \infty} \frac{e^t}{f(t)} = \infty$, thus $\exp \notin \text{Im} \Phi$.

Example 4.3. $\Phi$ is not injective in general. Let $R = \mathbb{Z}/p\mathbb{Z}$, then we have $x^p = x$ for all $x \in \mathbb{Z}/p\mathbb{Z}$. Therefore, $\Phi(t^p) = \Phi(t)$.

Example 4.4. $\Phi$ is in general not a ring homomorphism. Suppose that $R$ is not commutative, and $ab \neq ba$ for $a, b \in R$. Consider $f(t) = t$, $g(t) = a \in R[t]$. Then, we have $(\Phi(f)(\Phi(g))(b) = (\Phi(f)(b))(\Phi(g)(b)) = ab \neq ab = \Phi(fg)(b)$.

If $R$ is an infinite domain or a finite field, then we can say something more about the function $\Phi$.

Theorem 4.5. If $R$ is an infinite domain, then $\Phi$ is injective.

Proof. Suppose $f(t), g(t) \in R[t]$ and $\Phi(f) = \Phi(g)$. This means we have $(f - g)(a) = 0$ for all $a \in R$. If $f(t) - g(t) \neq 0$, then $f - g$ can have at most $\deg(f - g)$ distinct roots. Since $R$ is infinite, we have $f(t) = g(t)$.

Theorem 4.6. Let $R = \mathbb{F}_q$ be the finite field of order $q$, then we have $\ker \Phi = (t^q - t)$ and $\Phi$ is surjective. Therefore, we have $\mathbb{F}_q[t]/(t^q - t) \cong \text{Func}(\mathbb{F}_q, \mathbb{F}_q)$.

Proof. Note that $|\mathbb{F}_q^\times|$ is a multiplicative group of order $q - 1$. Thus for any $a \in \mathbb{F}_q^\times$, we have $a^{q-1} = 1$. This means $t^q - t \in \mathbb{F}_q[t]$ has all the elements of $\mathbb{F}_q$ as its roots, so $(t^q - t) \subseteq \ker \Phi$. Suppose $g(t) \in \ker \Phi$. By euclidean algorithm, there are $q(t), r(t) \in \mathbb{F}_q[t]$ such that $g(t) = (t^q - t)q(t) + r(t)$ and $r = 0$ or $\deg r < \deg(t^q - t) = q$. Since $g(a) = 0 = a^q - a$ for all $a \in \mathbb{F}_q$, we get $r(a) = 0$ for all $a \in \mathbb{F}_q$ by evaluating $t = a$ to the above equation. If $r \neq 0$, then $r$ can only have $\deg r < q$ distinct roots in $\mathbb{F}_q$. Thus we have $r = 0$ and $g \in (t^q - t)$.

By the first isomorphism theorem, we have

$$\mathbb{F}_q[t]/(t^q - t) \cong \text{Im} \Phi \subseteq \text{Func}(\mathbb{F}_q, \mathbb{F}_q)$$

Now we can compare two sides by counting the number of elements. Note that for any $f(t) \in \mathbb{F}_q[t]$, we can find $r(t) \in \mathbb{F}_q[t]$ such that $f(t) = r(t)$ in $\mathbb{F}_q[t]/(t^q - t)$ and $\deg r < q$ by euclidean
algorithm. Also any $r_1(t) \neq r_2(t) \in \mathbb{F}_q[t]$ with deg $r_1 < q$ and deg $r_2 < q$, we have $\overline{r_1(t)} \neq \overline{r_2(t)}$ in $\mathbb{F}_q[t]/(t^q-t)$ because the difference $r_1 - r_2$ has degree less than $q$, thus cannot be in $(t^q-t)$.

$$|\mathbb{F}_q[t]/(t^q-t)| = \# \text{ of polynomials of degree less than } q \text{ over } \mathbb{F}_q$$

$$= |\{a_0 + a_1t + \cdots + a_{q-1}t^{q-1} \mid a_i \in \mathbb{F}_q\}| = q^q$$

On the other hand, we have

$$|\mathbb{F}_q[t]/(t^q-t)| = |\text{Im } \Phi| \leq |\text{Func}(\mathbb{F}_q, \mathbb{F}_q)| = q^q = |\mathbb{F}_q[t]/(t^q-t)|$$

This shows the surjectivity of $\Phi$. □

**Corollary 4.7.** Any function $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is a polynomial function.

The above corollary is interesting, but doesn’t tell you which polynomial determines the function $f$. There’s a useful formula to find a polynomial defining a function $f$.

Let $F$ be a field (not necessarily finite) and consider the pairs $(x_0, y_0), (x_1, y_1), \ldots, (x_k, y_k) \in F \times F$ where $x_i \neq x_j$ if $i \neq j$. Then we can find a polynomial $L(t) \in F[t]$ such that $L(x_i) = y_i$ for all $i = 0, \ldots, k$ with deg $L \leq k$. We first define

$$l_i(t) = \prod_{j \neq i} \frac{t - x_j}{x_i - x_j} \in F[t]$$

Note that the denominator is not zero by assumption. Then we get

$$l_i(x_j) = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}$$

Now we define $L(t) = \sum_{i=0}^{k} y_i l_i(t)$, then $L(x_i) = y_i$ is satisfied for all $i$. This is called Lagrange interpolation.

**Example 4.8.** Consider $k + 1$ points on the $xy$-plane whose $x$-coordinates are distinct. Then there exists a polynomial in $\mathbb{R}[t]$ with degree at most $k$ whose graph passes through those $k + 1$ points.

**Example 4.9.** Consider the function $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ defined by $f(0) = 3, f(1) = 0, f(2) = 1, f(3) = 1, f(4) = 0$. We apply the method above to find a polynomial in $L_f(t) \in \mathbb{Z}/5\mathbb{Z}[t]$ defining $f$. Firstly, we have

$$l_0(t) = \frac{(t-1)(t-2)(t-3)(t-4)}{(0-1)(0-2)(0-3)(0-4)} = -t^4 + 1$$

Similarly, we can get $l_2(t) = -(t^3-t)(t+2)$ and $l_3(t) = -(t^3-t)(t-2)$. Therefore,

$$L_f(t) = 3l_0(t) + l_2(t) + l_3(t) = 2t^2 + 3$$

We can easily check that we have indeed $L_f(a) = f(a)$ for all $a \in \mathbb{Z}/5\mathbb{Z}$.

A more general thing also holds, and the proof is similar (count the number of elements!).

**Theorem 4.10.** Define $\Phi_n : \mathbb{F}_q[t_1, \ldots, t_n] \to \text{Func}(\mathbb{F}_q^n, \mathbb{F}_q)$ similarly. Then $\Phi_n$ is surjective and ker $\Phi_n = (t_1^q - t_1, t_2^q - t_2, \ldots, t_n^q - t_n)$. Thus we have

$$\mathbb{F}_q[t_1, t_2, \ldots, t_n]/(t_1^q - t_1, t_2^q - t_2, \ldots, t_n^q - t_n) \cong \text{Func}(\mathbb{F}_q^n, \mathbb{F}_q)$$
5. Inverse Galois Problem for $S_p$

We can show that every finite group occurs as a Galois group of some finite Galois extension. Let $G$ be a finite group, then we can consider $G$ as a subgroup of $S_n$ for $n = |G|$. Let $F$ be a field. We define an action of $\sigma \in S_n$ on $F(t_1, \ldots, t_n)$ by

$$\sigma \cdot f(t_1, \ldots, t_n) = f(t_{\sigma(1)}, \ldots, t_{\sigma(n)})$$

for $f, g \in F[t_1, \ldots, t_n]$. Let $e_1 = \sum_i t_i, e_2 = \sum_{i,j} t_it_j, \ldots, e_n = t_1 \cdots t_n$ be the elementary polynomials in $F[t_1, \ldots, t_n]$, then $e_i \in F(t_1, \ldots, t_n)^{S_n}$ for all $i$. (We can actually show that $F(e_1, \ldots, e_n) = F(t_1, \ldots, t_n)^{S_n}$.) Note that we have

$$\text{Gal}(F(t_1, \ldots, t_n)/F(t_1, \ldots, t_n)^{S_n}) = S_n$$

and

$$\text{Gal}(F(t_1, \ldots, t_n)/F(t_1, \ldots, t_n)^G) = G$$

by the following theorem.

**Theorem 5.1.** Let $F$ be a field and $G$ be a finite subgroup of $\text{Aut}(F)$. Then, $F$ is Galois over $F^G$ and $G = \text{Gal}(F/F^G)$. Here $F^G$ means the set of fixed points in $F$ by $G$.

**Proof.** See [2, 48.15].

The following problem is a famous open problem in field theory.

**Problem (Inverse Galois Problem).** For any finite group $G$, is there a field extension $E$ of $\mathbb{Q}$ satisfying $\text{Gal}(E/\mathbb{Q}) = G$?

In this section, we will show that the problem is true for $S_p$ where $p$ is a prime.

**Lemma 5.2.** $S_n = \langle (12), (12 \cdots n) \rangle$ for all $n \geq 3$.

**Theorem 5.3.** Let $p$ be a prime and $f \in \mathbb{Q}[t]$ be an irreducible polynomial of degree $p$. Suppose that $f$ has exactly two nonreal roots in $\mathbb{C}$. Then, $G_f \cong S_p$.

**Proof.** We can consider $G_f$ as a subgroup of $S_p$. Choose a root $\alpha \in \mathbb{C}$ of $f$, then $p = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [G_f]$. Thus, we have a $p$-cycle in $G$. Since $f$ has a pair of complex roots, the complex conjugation is an automorphism of the splitting field of $f$. Therefore, $G$ contains a transposition. Let $\sigma = (ab) \in G$ and $\tau \in G$ be a $p$-cycle. There is an integer $k$ such that $\sigma^k = (ab \cdots) \in G$. We may assume $\sigma = (12)$ and $\tau = (12 \cdots p)$, thus $G_f = S_p$.

**Theorem 5.4.** Let $p$ be a prime. Then there exists an irreducible polynomial $f \in \mathbb{Z}[t]$ of degree $p$ which has exactly two nonreal roots.

**Proof.** Let $g(t) = (t - p)(t - 2p) \cdots (t - (p - 2)p)(t^2 + p) \in \mathbb{Z}[t]$ be a polynomial of degree $p$. Note that the graph of $g$ intersects the $x$-axis $p - 2$ times at $(p, 0), (2p, 0), \ldots, ((p - 2)p, 0)$. Let $m$ be the minimum of the absolute values of negative local minimums of $g$. We can find another prime $q$ satisfying $-m < -\frac{p}{q} < 0$. Then, the graph of $g$ still intersects the line $y = -\frac{p}{q}$ at $p - 2$ points. (Draw the graph of $g$ and check this!) Now we define

$$f(t) = qg(t) + p = q \left( f(t) - \left( -\frac{p}{q} \right) \right)$$

$$= q(t - p)(t - 2p) \cdots (t - (p - 2)p)(t^2 + p) + p$$

$$= a_p t^p + \cdots + a_0$$

8
for some $a_l \in \mathbb{Z}$. Note that $\deg f = p$ and $f$ has exactly two nonreal roots by the observation above. Also we have $p \nmid q = a_p$, $p \mid a_i$ for $i = 0, 1, 2, \ldots, p - 1$, and $p^2 \nmid a_0$. By Eisenstein’s criterion, $f$ is irreducible over $\mathbb{Z}$, thus irreducible over $\mathbb{Q}$.

\section{6. Artin-Schreier Theorem}

We have $[\mathbb{C} : \mathbb{R}] = [\overline{\mathbb{Q}} : \mathbb{Q} \cap \mathbb{R}] = 2$ and $\mathbb{C}, \overline{\mathbb{Q}}$ are algebraically closed. In this section, we will show that if a field $F$ is not algebraically closed and $[\overline{F} : F]$ is finite, then $F$ must look like the cases explained above.

\begin{lemma}
Let $F$ be a field of characteristic $l$ and $a \in F$. Suppose $a \notin F^l$. Then, $t^{lm} - a \in F[t]$ is irreducible for all $m \geq 1$.
\end{lemma}

\begin{proof}
Note that if $\beta^{lm} = a$ for some $\beta \in \overline{F}$, then $t^{lm} - a = (t - \beta)^{lm}$. Suppose $t^{lm} - a = f(t)g(t)$ for $f, g \in F[t] \setminus F$, then $f(t) = (t - \beta)^{lr} = (t^{r} - \beta^{r})^{sl} \in F[t]$ for $(s, l) = 1$ and $r < m$. This shows that $s\beta^{r} \in F$, thus $\beta^{r} \in F$. Therefore, $a = (\beta^{r})^{m-r} \in F^l$.
\end{proof}

\begin{lemma}
Let $F$ be a field where $-1$ is not a square and suppose every element in $F(i)$ is a square in $F(i)$ for $i^2 = -1, i \in \overline{F}$. Then, we have $\text{char } F = 0$ and a sum of squares is also a square in $F$.
\end{lemma}

\begin{proof}
Let $a, b \in F$. There are $c, d \in F$ satisfying $a + bi = (c + di)^2$ by assumption. Thus, we have $a^2 + b^2 = (c^2 + d^2)^2$. By induction, any finite sum of squares in $F(i)$ is also a square in $F(i)$. If $\text{char } F \neq 0$, then $-1$ is a sum of squares $1^2$, thus a contradiction.
\end{proof}

\begin{lemma}
Let $K, F$ be fields. The following are equivalent:

(1) $\text{char } F = p > 0$ and $K/F$ is a cyclic extension with $[K : F] = p$.

(2) $K$ is a splitting field of an irreducible polynomial $t^p - t - a \in F[t]$ for some $a \in F$.
\end{lemma}

\begin{proof}
(1) $\Rightarrow$ (2) Suppose $\text{Gal}(F/K) = \langle \sigma \rangle$. Note that $\text{Tr}_{K/F}(1_F) = p \cdot 1_F = 0$. Thus, there is $v \in K$ satisfying $1_F = v - \sigma(v)$. Let $u = -v$, then $\sigma(u) = u + 1 \neq u$. Therefore $u \notin F$. Let $a = u^p - u$, then $\sigma(a) = \sigma(u^p - u) = (u + 1)^p - (u + 1) = u^p - u = a$

This shows $a \in F$ and $K$ is the splitting field of $t^p - t - a$.

(2) $\Rightarrow$ (1) $\text{Gal}(F/K) = \langle \sigma \rangle$ where $\sigma(a) = a + 1$ for $a \in K$.
\end{proof}

\begin{lemma}
Let $K/F$ be a field extension with $[K : F] = p$. Suppose $\zeta_p \in F$. Then, there is an element $\gamma \in K$ such that $K = F(\gamma)$ and $\gamma^p \in F$.
\end{lemma}

\begin{proof}
Let $\text{Gal}(K/F) = \langle \sigma \rangle$. Since $N_{K/F}(\zeta_p) = \zeta_p^p = 1$, there is $u \in K$ such that $\zeta_p = \frac{u}{\sigma(u)}$ by Hilbert theorem 90. Let $\gamma = u^{-1}$, then $\sigma(\gamma) = \zeta_p \gamma$, and $\sigma(\gamma^p) = \gamma^p \in F$.
\end{proof}

\begin{theorem}[Artin-Schreier]
Let $K/F$ be a field extension and $K = \overline{K}$, $1 < [K : F] < \infty$. Then,

(1) $\text{char } F = 0$ and $K = F(i)$ for some $i \in K$ satisfying $i^2 = -1$

(2) for $a \in F^\times$, exactly one of $a$ or $-a$ is a square in $F$

(3) any finite sum of nonzero squares in $F$ is a nonzero square in $F$.
\end{theorem}

\begin{proof}
(1) We first show that $K/F$ is Galois. Since $K$ is algebraically closed, $K/F$ is normal. If $\text{char } F = 0$, then we’re done since then $K/F$ is separable. Suppose $\text{char } F = l$ for some prime $l$. If $F \neq F^l$, then choose $a \in F \setminus F^l$. By Lemma \ref{6.1}, we will have irreducible polynomials in $F[t]$
of arbitrarily large degree, but this contradicts that \( K = \overline{K} \) and \([K : F]\) is finite. Therefore \( F = F' \) and \( K/F \) is separable, thus Galois.

Now we show that \([K : F] = 2\). If \([K : F] > 2\), then we will have either \( 4 \mid [K : F] \) or \( p \mid [K : F] \) for some odd prime \( p \). Let \( H \) be a subgroup of \( G \) of order 4 or \( p \) (which exists by Sylow’s theorem) and \( E = K^H \).

(Case 1) \([K : E] = p\) and \( \text{char}(E) = p\).

Let \( \text{Gal}(K/E) = \langle \sigma \rangle \). By 6.3, \( K = E(\alpha) \) where \( \alpha \) is a root of the irreducible polynomial \( t^p - t - a \in E[t] \). Because \( K \) is algebraically closed, we can find \( b \in K \) satisfying \( b^p - b = aa^{p-1} \).

We can write \( b = b_0 + b_1\alpha + \cdots + b_{p-1}\alpha^{p-1} \) for some \( b_i \in E \) because \( \{1, \alpha, \cdots, \alpha^{p-1}\} \) is an \( E \)-basis of \( K \). Now we have \( b^p - b = ((b_{p-1})^p - b_{p-1})\alpha^{p-1} + \) (lower degree terms of \( \alpha \)) since \( \alpha^p = \alpha + a \). Note that \( b_{p-1} \) satisfies \( (b_{p-1})^p - b_{p-1} = a \) by comparing the coefficients of \( \alpha^{p-1} \).

This shows that \( t^p - t - a \in E[t] \) is not irreducible. Therefore, this case does not happen.

(Case 2) \([K : E] = p\) and \( \text{char}(E) = l \neq p\).

Let \( \text{Gal}(K/E) = \langle \sigma \rangle \). We have \( \zeta_p \in K \) where \( \zeta_p \) is a \( p \)-th root of unity. Since \( [E(\zeta_p) : E] \mid [K : E] = p \) and \( [E(\zeta_p) : E] = \text{deg}\text{irr}(\zeta_p, E) \leq p - 1 \), we have \( \zeta_p \in E \). Thus by 6.4, \( K = E(\gamma) \) for some \( \gamma^p \in E \). Choose \( \beta \in K \) such that \( \beta^p = \gamma \), then \( \beta^{p^2} \in E \). Since \( \left( \frac{\sigma(\beta)}{\beta} \right)^{p^2} = \left( \frac{\sigma(\gamma)}{\gamma} \right)^{p^2} = 1 \), we have \( \sigma(\beta) = \omega\beta \) where \( \omega \) is a \( p^2 \)-th root of unity. Note that \( \omega^p \) is a \( p \)-th root of unity, thus in \( E \).

We can see that \( \omega^p \neq 1 \) because otherwise we have \( \sigma(\gamma) = \sigma(\beta^p) = \omega^p\beta^p = \gamma \). Therefore, \( \omega^p \) is a primitive \( p \)-th root of unity. Since \( \omega^p = \sigma(\omega^p) = \sigma(\omega)^p \), we have \( \sigma(\omega) = \omega(\omega^p)^k \) for some \( 1 \leq k \leq p - 1 \). Now,

\[
\beta = \sigma^p(\beta) = \omega\sigma(\omega) \cdots \sigma^{p-1}(\omega)\beta = \omega^{1+(1+pk)+\cdots+(1+pk)^{p-1}}\beta
\]

shows that

\[
\sum_{i=0}^{p-1} (1 + pk)^i \equiv \sum_{i=0}^{p-1} (1 + ipk) \equiv 0 \pmod{p^2}
\]

This is equivalent to \( 1 + \frac{p(p-1)}{2}k \equiv 0 \pmod{p} \), but this cannot happen when \( p \) is odd. The only possible case is \( p = 2 \) and \( k \) is odd.

(Case 3) \([K : E] = 4\).

Choose \( E' \) between \( K \) and \( E \) satisfying \([K : E'] = 2\). Note that the arguments in Case 1, 2 can be applied to the case \( p = 2 \). Therefore \( \omega \) is a 4-th root of unity, and \( \sigma(\omega) = \omega^{1+2k} = \omega^3 \neq \omega \) because \( k = 1 \). By the argument in Case 2, \( \omega^2 \) is a primitive 2-th root of unity, i.e., \( \omega^2 = -1 \), and \( K = E'[\omega] \). On the other hand, we have \([K : E(\omega)] = 2\) because \( \omega \) is a root of \( t^2 + 1 \in E[t] \).

By the same argument, \( K \) should be generated by a 4-th root of unity from \( E(\omega) \), but \( E(\omega) \) already have all of them, which is a contradiction.

By considering Case 1-3, we conclude that there is an element \( i \in K \) satisfying \([K : F] = 2\), \( K = F(i) \), \( i^2 = -1 \) and \( \text{char}(F) \neq 2 \). By 6.2, we have \( \text{char}(F) = 0 \).

(2) Suppose \( a \) and \( -a \) are not squares, then \( K = F(\sqrt{a}) = F(\sqrt{-a}) \). Write \( \sqrt{-a} = c_1 + c_2\sqrt{a} \) for \( c_1, c_2 \in F \). By squaring both sides, we get \( -a = c_1^2 + ac_2^2 + 2c_1c_2\sqrt{a} \). This means \( c_1c_2 = 0 \), and thus \( c_1 = 0 \). Hence \(-1 = c_2^2 \) is a square in \( F \), which is a contradiction. The similar argument works when both \( a \) and \(-a \) are squares.
(3) By 6.2 again, we know that any finite sum of nonzero squares in $F$ is also a square in $F$. Suppose $\sum b_i^2 = 0$, $b_i \neq 0$ in $F$. This gives $-1 = \sum_{i>1} \left(\frac{b_i}{b_1}\right)^2$, thus a contradiction. \hfill \Box

Example 6.6. Suppose $\sigma \in \Gal(\overline{Q}/Q)$ has finite order. Let $G = \langle \sigma \rangle$, then $G = \Gal(\overline{Q}/\overline{Q}^G)$ is finite. By Artin-Schreier, we have $|G| = 2$ and $\sigma$ has order 2. In fact, 
$$\Gal(\overline{Q}/Q)_{tor} = \{g\sigma^{-1} \mid g \in \Gal(\overline{Q}/Q)\}$$
where $c$ is the complex conjugation.

7. Infinite Galois Theory

Let $K/F$ be a finite Galois extension of fields. Then by the fundamental theorem of Galois theory, we have the following one-to-one correspondence:
$$\begin{align*}
\{F \leq E \leq K, \text{ intermediate fields}\} & \overset{1-1}\longleftrightarrow \{H \leq \Gal(K/F), \text{ subgroups}\} \\
E & \mapsto \Gal(K/E) \\
K^H & \leftrightarrow H
\end{align*}$$

However, this may fail in an infinite Galois extension.

Consider the infinite Galois extension $\overline{F}_p/F_p$ and let $G = \Gal(\overline{F}_p/F_p)$. Consider the Frobenius map $\phi \in G$ defined by $\phi(x) = x^p$ for $x \in \overline{F}_p$. We have $\langle \phi \rangle \leq G$ and $\overline{F}_p^\phi = F_p^{\phi} = F_p$. We will show that $\langle \phi \rangle \not\leq G$, thus the correspondence in finite extension case fails.

For each $n \in \mathbb{N}$, write $n = \tilde{n}p^{v_p(n)}$ where $(p, \tilde{n}) = 1$. We can find $x_n, y_n \in \mathbb{N}$ such that $1 = \tilde{n}x_n + p^{v_p(n)}y_n$. Define $a_n = \tilde{n}x_n$. Let $m \mid n$, then $a_n - a_m = \tilde{n}x_n - \tilde{m}x_m \equiv 0 \pmod{\tilde{m}}$ because $\tilde{n} \mid \tilde{m}$. Similarly, we can show that $p^{v_p(n)} \mid a_n - a_m$, thus $a_n \equiv a_m \pmod{m}$. Let $\psi_n = \phi^{a_n}|_{\overline{F}_p} \in \Gal(\overline{F}_p/F_p) = \langle \phi \rangle|_{\overline{F}_p}$, then $\psi_n|_{\overline{F}_p} = \phi^{a_n}|_{\overline{F}_p} = \phi^{a_m}|_{\overline{F}_p} = \psi_m$. Therefore, $\psi \in \Gal(\overline{F}_p/F_p)$ defined by $\psi|_{\overline{F}_p} = \psi_n$ for each $n$ is well-defined because $\overline{F}_p = \bigcup_n \overline{F}_{pn}$.

Suppose that $\psi = \phi^{a}$ for some $a \in \mathbb{Z}$, then $\phi^{a_n}|_{\overline{F}_p} = \psi_n = \psi|_{\overline{F}_p} = \phi^{a}|_{\overline{F}_p}$. Therefore we get $a_n \equiv a \pmod{n}$ for all $n \in \mathbb{N}$. In particular, we have $a \equiv a_{p^k} \equiv x_{p^k} \equiv 1 \pmod{p^k}$ for all $k$, thus $a = 1$. However, for a different prime $q \neq p$, $a_q = qx_q \equiv 1 \pmod{q}$. This shows $\psi \not\in \langle \phi \rangle$.

(We can check that $\Gal(\overline{F}_p/F_p) = \langle \phi \rangle$ topologically though.)

We will show that a slightly modified version of the fundamental theorem holds for infinite Galois extensions. We need to define a topology on $\Gal(K/F)$ to state the correspondence.

Definition 7.1. Let $K/F$ be a (possibly infinite) Galois extension of fields. We define a Krull topology (profinite topology) on $G = \Gal(K/F)$ so that for all $\sigma \in G$ and $E/F$ finite Galois, $\{\sigma \Gal(G/E)\}$ is a basis of neighborhoods. Note that this gives a discrete topology on $G$ if $K/F$ is finite.

Remark 7.2. The above definition of Krull topology gives a well-defined topology, and $G$ becomes a compact, Hausdorff, totally disconnected (the only connected components are one-point sets) topological group with respect to the Krull topology.

Remark 7.3. Let $G$ be a topological group. Note that for any $g \in G$, the map $\lambda_g : G \to G$ defined by $\lambda_g(h) = gh$ is a homeomorphism. If $H \leq G$ is an open subgroup, then all the cosets of $H$ are open, thus $H$ is also closed. If $H \leq G$ is a closed subgroup, and $(G : H) < \infty$, then $H$ is also open because it is a complement of finite union of closed cosets.
Theorem 7.4 (Fundamental theorem of infinite Galois theory). Let $K/F$ be a (possibly infinite) Galois extension of fields. Then we have the following one-to-one correspondence:

$$
\{ F \leq E \leq K, \text{ intermediate fields} \} \overset{1-1}{\longleftrightarrow} \{ H \leq \text{Gal}(K/F), \text{ closed subgroups} \}
$$

$$
E \mapsto \text{Gal}(K/E)
$$

$$
K^H \leftrightarrow H
$$

Note that the above gives a one-to-one correspondence between finite extensions of $F$ and open subgroups (thus of finite index) of $\text{Gal}(K/F)$.

Proof. If $E/F$ is finite, then $\text{Gal}(K/E)$ is a basis element of the Krull topology, thus is open. Also it is closed as discussed in the previous remark. For an arbitrary $K/E$, write $E = \bigcup_i E_i$ with $E_i/F$ finite, then

$$
\text{Gal}(K/E) = \bigcap_i \text{Gal}(K/E_i) \subseteq \text{Gal}(K/F)
$$

is closed. This shows that the correspondence $E \mapsto \text{Gal}(K/E)$ is well-defined.

Since $K^{\text{Gal}(K/F)} = E$, this map $E \mapsto \text{Gal}(K/E)$ is injective.

Now we will show that this map is surjective. Consider a subgroup $H$ of $G = \text{Gal}(K/F)$. Clearly, we have $H \leq \text{Gal}(K/K^H)$. Choose $\sigma \in \text{Gal}(K/K^H)$ and a neighborhood of $\sigma$, which is of the form $\sigma \text{Gal}(K/E) \subseteq \text{Gal}(K/K^H)$ with $E/K^H$ finite. Define $r : H \rightarrow \text{Gal}(E/K^H)$ by $r(\rho) = \rho|_E$. $r$ is surjective by the fundamental theorem of finite Galois theory for $E/K^H$ because $E^{r(H)} = K^H = E^{\text{Gal}(E/K^H)}$ gives $r(H) = \text{Gal}(E/K^H)$. Choose $\tau \in H$ such that $r(\tau) = \tau|_E = \sigma|_E$, then $\tau \in H \cap \sigma \text{Gal}(K/E)$. This shows that $H$ is dense in $\text{Gal}(K/K^H)$.

Therefore, for a closed subgroup $H \leq G$, we have $\text{Gal}(K/K^H) = \overline{H} = H$.

The last statement is easy to check. $\square$

Definition 7.5. A profinite group $G$ is a compact, Hausdorff topological group with a basis of neighborhoods of $1 \in G$ consisting of normal subgroups.

Proposition 7.6. Let $G$ be a group. Then the followings are equivalent.

1. $G$ is profinite
2. $G \cong \varprojlim_N G/N$
   \[ N \leq G \text{ open} \]
3. $G$ is an inverse limit of finite groups with discrete topology.

Example 7.7. A Galois group $G = \text{Gal}(K/F)$ is a profinite group. Since a subgroup $N \leq G$ is open if and only if $N = \text{Gal}(K/E)$ for some $E/F$ finite Galois, we have

$$
\text{Gal}(K/F) = \varprojlim_{N \leq G \text{ open}} G/N = \varprojlim_{E/F \text{ finite Galois}} \text{Gal}(K/F)/\text{Gal}(K/E) = \varprojlim_{E/F \text{ finite Galois}} \text{Gal}(E/F)
$$

Example 7.8. Note that $\mathbb{F}_p = \bigcup_n \mathbb{F}_{p^n}$. Therefore, we have

$$
\text{Gal}(\mathbb{F}_p/\mathbb{F}_p) = \varprojlim_n \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}
$$

Example 7.9. Let $\mathbb{Q}^{ab}$ be the maximal abelian extension (the composite of all abelian extensions) of $\mathbb{Q}$. By Kronecker-Weber theorem, we have $\mathbb{Q}^{ab} = \bigcup_n \mathbb{Q}(\mu_n)$. Therefore, we have

$$
\text{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \varprojlim_n \text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times
$$
References


