Element $\overline{\zeta}$ clearly generates the multiplicative group of the corresponding extension field $\mathbb{F}_{p^m}$. Then we can choose $\mathcal{T}$ to be the set of representatives modulo $pGR(p^e, m)$, and get for each element $b \in GR(p^e, m)$ unique representation

$$b = t_0 + pt_1 + p^2 t_2 + \ldots + p^{e-1} t_{e-1},$$

Where each $t_i \in \mathcal{T}$. Again, the least index where $t_i \neq 0$ is the order of b with respect to exponent valuation. We see now that the multiplicative stucture of the residue class field $\mathbb{F}_{2^m}$ can be embedded in the Galois ring $GR(p^e, m)$ by $0 \mapsto 0$, $\overline{\zeta}^i \mapsto \zeta^i$.

As seen in former chapter, the automorphism group of $GR(p^e, m)$ is generated by σ which is defined by

$$\sigma(\zeta) = \zeta^p,$$

and extending this in the only possible way:

$$\sigma(b) = t_0^p + pt_1^p + p^2 t_2^p + \ldots + p^{e-1} t_{e-1}^p,$$

where b is as above.

The case $p = 2$, $e = 2$ is important in the applications. The bottom ring is then $\mathbb{Z}/4\mathbb{Z} := \mathbb{Z}_4$. Extension of degree m is obtained as explained above: find a primitive irreducible polynomial $\overline{h}$ over $\mathbb{F}_2$. This polynomial is a factor of $X^{2^m-1} - 1$ (in $\mathbb{F}_2[X]$), and it can be lifted to be a factor of $X^{2^m-1} - 1$ in $\mathbb{Z}_4[X]$ by Hensel's lemma. A more useful algorithm for finding the lift over $\mathbb{Z}_4[X]$ is given by Graeffe's method [Uspensky: Theory of equations]. The method is as follows:

Let $h_2(X) = e(X) - d(X)$, where $e(X)$ contains only even powers and $d(X)$ only odd powers of X. The basic irreducible lift of $\overline{h}$ is then obtained by

$$h(X^2) = \pm(e^2(X) - d^2(X)).$$

The root of h is then adjoined to $\mathbb{Z}_4$ to obtain $GR(4, m)$. This root, ζ, is a primitive n:th root of unity over $\mathbb{Z}_4$, where $n = 2^m - 1$. Each element in $GR(4, m)$ can then be represented in the form

$$b = b_0 + b_1\zeta + b_2\zeta^2 + \ldots + b_{m-1}\zeta^{m-1},$$

or in the form

$$b = t_0 + 2t_1,$$

where $t_0, t_1 \in \mathcal{T}$. The former representation corresponds to the additive representation in field extensions and the latter to the multiplicative representation. The latter one is of special interest: the generator of the automorphism group is obtained by

$$\sigma(t_0 + 2t_1) = t_0^2 + 2t_1^2,$$

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

as shown in the lifting theorem (II.5.2). Furthermore, the natural projection is given by

$$\pi(t_0 + 2t_1) = \bar{t}_0.$$

The multiplicative representation also reveals an interesting connection to a general ring theoretic construction: Let mapping $f : GR(4, m) \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ be defined by

$$f(t_0 + 2t_1) = (\bar{t}_0, (\bar{t}_1)^2)$$

It is clear that f is bijective mapping, since $\alpha \mapsto \alpha^2$ is a permutation of the field $\mathbb{F}_{2^m}$. We will now define a ring addition and multiplication on the set $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with help of f:

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = f(f^{-1}(\alpha_1, \beta_1) + f^{-1}(\alpha_2, \beta_2))$$
$$(\alpha_2, \beta_1) \cdot (\alpha_2, \beta_2) = f(f^{-1}(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2)).$$

It is straightforward to verify that these operations become

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2 + \alpha_1\alpha_2)$$
$$(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (\alpha_1\alpha_2, \alpha_1^2\beta_2 + \alpha_2^2\beta_1).$$

Ring $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ equipped with operations defined above is called the ring of *Witt vectors* of length 2 over $\mathbb{F}_{2^m}$. Witt vectors can be defined over arbitrary ring and of arbitrary length [Nathan Jacobson: Basic Algebra II], but the arithmetics becomes very complicated when the length or the characterisric increases. In short lengths the approach by using Witt vectors is very useful.

Let us investigate a little bit how the general structure of local ring is reflected to the multiplicative representation. It is clear that the elements of form $2t_1$ are exactly all nilpotents. Moreover, all elemets ζ^i are clearly units. Since a sum of a unit and a nilpotent is a nilpotent, we see that all the elements of form $\zeta^i + 2t_1$ are units. There are $n \cdot (n + 1) = (2^m - 1) \cdot 2^m$ such elements, and because $|GR(4, m)^*| = |GR(4, m)| - |2GR(4, m)| = 4^m - 2^m = 2^m(2^m - 1)$, we see that these elements are *all* units. We have obtained:

Theorem II.6.1. *The unit group of $GR(4, m)$ is of form $\mathcal{E} \times \mathcal{H}$, where $\mathcal{E} = \mathcal{T} \setminus 0$ and $\mathcal{H} = 1 + 2\mathcal{E}$.*

Proof. The existence and the uniqueness of the representation of a unit in form $u = \zeta^i(1 + 2t)$ follows directly from the multiplicative representation. □

Note that $(\mathcal{H}, \cdot)$ is isomorphic to $(\mathbb{F}_{2^m}, +)$, isomorphism $\mathbb{F}_{2^m} \to \mathcal{H}$ given by $0 \mapsto 1$ and $\bar{\zeta}^i \mapsto 1 + 2\zeta^i$.

Next we will study a closely related topic, namely the rings of p-adic integers.

III. p-adic theory briefly

III.1. On the foundations.

The multiplicative group of rational numbers $\mathbb{Q}$ is known to be direct product of group $\{-1, 1\}$ and of a free abelian group generated by prime numbers $\mathbb{P}$. That is, each $r \in \mathbb{Q}$ has unique representation of form

$$r = \pm \prod_{p_i \in \mathbb{P}} p_i^{a_i},$$

Where $a_i \in \mathbb{Z}$, p_i runs over all primes and only a finite number of exponents a_i are nonzero.

Now we fix a prime number p. If r is any rational number, the exponent a_i of p in the representation above is said to be the *p-order* of r, let us denote this exponent $\mathrm{ord}_p(r)$. Mapping $\mathbb{Q} \to \mathbb{Z} : r \to \mathrm{ord}_p(r)$ is called *(exponent) valuation* of $\mathbb{Q}$. We shall also pick a symbol ∞ that is not in $\mathbb{Z}$ and agree that $a < \infty$ for all $a \in \mathbb{Z}$ and that $\mathrm{ord}_p(0) = \infty$.

Definition. If $\mathrm{ord}_p(r) \geq 0$, then r is said to be rational p-adic integer.

Example. Let $r = \frac{50}{7} = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^{-1} \cdot 11^0 \cdot 13^0 \cdot \ldots$. $\mathrm{ord}_2(r) = 1$, $\mathrm{ord}_3(r) = 0$, $\mathrm{ord}_5(r) = 2$, $\mathrm{ord}_7(r) = -1$, and $\mathrm{ord}_p(r) = 0$ for $p > 7$. r is not a 7-adic integer, but is a p-adic integer for all $p \neq 7$.

By using p-order we can define a *p-adic valuation* of $\mathbb{Q}$: Choose a fixed real number $0 < \rho < 1$ and define $|r|_p = \rho^{\mathrm{ord}_p(r)}$. We agree on that $\rho^\infty = 0$. It is easily verified that this is really a valuation, i.e. $|\cdot|_p$ satisfies the following conditions:

(V1) $|r|_p \geq 0$ and $|r| = 0$ if and only of $r = 0$.

(V2) $|r_1 r_2|_p = |r_1|_p |r_2|_p$.

(V3) $|r_1 + r_2|_p \leq |r_1|_p + |r_2|_p$.

The absolute value defines also a valuation, and in the thery of p-adic numbers the absolute value of a rational number r is often denoted by $|r|_\infty$. The p-adic valuation satisfies a condition even stronger than (V3), namely

(V3') $|r_1 + r_2| \leq \max\{|r_1|_p, |r_2|_p\}$.

A valuation satifying (V3') is called *non-Archimedian* valuation. The field $\mathbb{Q}$ becomes a metric space, when we define $d_p(x, y) = |x - y|_p$. This p-adic metric is even an *ultrametric*, that is, $d_p(x, z) \leq \max\{d_p(x, y), d_p(y, z)\}$ for all x, y and z. From the theory of metric spaces we know that for each metric space V there is a *completion* of V, i.e. a metric space where V can isometrically embedded and which is complete in the sense that each Cauchy-sequence converges in that space. Furthermore, V is dense in then completion. In the case of $\mathbb{Q}$ equipped with p-adic metric the completion is called the *field of p-adic numbers* and denoted by $\mathbb{Q}_p$. The valuation can also be extended to the completion with range unchanged, in fact, for a chosen $\alpha \in \mathbb{Q}$ there exists a sequence a_1, a_2, ... in $\mathbb{Q}$ converging to α, and we can define

$$|\alpha|_p = \lim_{i \to \infty} |a_i|_p$$

It can easily be shown that there exists an index N such that $|a_i|_p = |\alpha|_p$ for $i \geq N$. It is an easy exercise to show by using the properties of ultrametric that a sequence

$$S_n = \sum_{i=0}^{n} c_i$$

converges if and only if $|c_i|_p$ tends to zero as i tends to infinity. In the sequence

$$S_n = \sum_{i=0}^{n} a_i p^i$$

where $0 \leq a_i \leq p-1$ the value of a general term is $\left|a_i p^i\right|_p$ is either 0 or $\rho^i \xrightarrow{i\to\infty} 0$, and therefore the sequence converges. Next we classify the p-adic numbers with respect to the value.

Definition. A p-adic number a is said to be

1) a *p-adic integer*, if $\mathrm{ord}_p(a) \geq 0$, and
2) a *p-adic unit*, if $\mathrm{ord}_p(a) = 0$.

The set of p-adic integers will unconventionally be denoted by $\mathbb{Z}_{p^\infty}$, and the set of p-adic units by $\mathbb{U}_{p^\infty}$. Furthermore, we will denote

$$\mathbb{M}_{p^\infty} = \{a \in \mathbb{Q}_p \mid \mathrm{ord}_p(a) > 0\}.$$

It is easy to see that $\mathbb{Z}_{p^\infty}$ forms a subring of $\mathbb{Q}$, and that $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}_{p^\infty}$. Moreover, $\mathbb{U}_{p^\infty}$ is the unit group of $\mathbb{Z}_{p^\infty}$. It is also easy to see that $\mathbb{Z}_{p^\infty}$ is a local ring with maximal ideal $\mathbb{M}_{p^\infty}$. A similar argumentation as in lemma II.4.3 gives us the structure of the ideals of $\mathbb{Z}_{p^\infty}$; all of them are given by

$$0 \subset \ldots \subset p^3\mathbb{Z}_{p^\infty} \subset p^2\mathbb{Z}_{p^\infty} \subset p\mathbb{Z}_{p^\infty} = \mathbb{M}_{p^\infty} \subset \mathbb{Z}_{p^\infty}.$$

III.2. Representing the p-adic numbers.

Let $\mathrm{ord}_p(a) = n$. Then $\mathrm{ord}_p(\frac{a}{p^n}) = n - n = 0$, so $\frac{a}{p^n}$ is a p-adic unit, let us denoite $u = \frac{a}{p^n}$. Therefore each nonzero p-adic number can be written as $a = up^n$, where u is a unit and $n = \mathrm{ord}_p(a)$. Furthermore, the exponent of p is unique; this can be verified by counting orders in both sides of $up^n = vp^m$, and since all elements here are in field, we can cancel p^n in $up^n = vp^n$ to obtain

Proposition III.1.1. *Each nonzero p-adic number α can be represented uniquely in the form $\alpha = up^n$, where u is a unit and $n = \mathrm{ord}_p(\alpha)$.*

The quotient field $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$, and the set of representatives modulo p can be chosen to be

$$T = \{0, 1, 2, \ldots, p-1\}.$$

It can (easily) be shown, that also $\mathbb{Z}_{p^\infty}/p\mathbb{Z}_{p^\infty} \cong \mathbb{F}_p$, and the set above is suitable to represent the cosets modulo $p\mathbb{Z}_{p^\infty}$. So for each p-adic integer α there exists a representation $\alpha = u_0 + p\alpha_1$, where $u_0 \in T$. Applying the same procedure to α_1 and so on we obtain a representation for a p-adic number by a convergent series

$$\alpha = u_0 + u_1 p + u_2 p^2 + u_3 p^3 \ldots ,$$

$u_i \in T$. In general, any p-adic number can be represented as a convergent series like above, but also negative powers of p can be included;

$$\alpha = u_{-n}p^{-n} + u_{-n+1}p^{-n+1} + \ldots + u_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + \ldots ,$$

$u_i \in T$, $u_{-n} \neq 0$. It is also obvious that $\mathrm{ord}_p(\alpha) = -n$ above.

III.3. Some further connections.

The *value group* of a p-adic number field $\mathbb{Q}_p$ is the additive group of all possible orders of nonzero elements in $\mathbb{Q}_p$ and (exponent) valuation is a group morphism from $\mathbb{Q}_p^*$ onto the value group. We have seen that in $\mathrm{ord}_p(p^n) = n$, so we see that the value group of $\mathbb{Q}_p$ is $\mathbb{Z}$. The additive group of integers is always a subgroup of the value group of any extension of $\mathbb{Q}_p$. Let us suppose that $\mathbb{F}/\mathbb{Q}_p$ is a finite field extension. It can be shown that the p-adic valuation can be uniquely extended to $\mathbb{F}$. Suppose that the value groups of $\mathbb{F}$ and $\mathbb{Q}_p$ are G and $\mathbb{Z}$ respectively. In the extension field $\mathbb{F}$ the consepts of integer ring and the unit group of the integer ring can be defined exactly in the same fashion as in $\mathbb{Q}_p$:

$$\mathbb{Z}_{\mathbb{F}} = \{\alpha \in \mathbb{F} \mid \mathrm{ord}_p(\alpha) \geq 0\}$$
$$\mathbb{U}_{\mathbb{F}} = \{\alpha \in \mathbb{F} \mid \mathrm{ord}_p(\alpha) = 0\}$$

The index $e = [G : \mathbb{Z}]$ is said to be the *ramification index* of the extension. The extension $\mathbb{F}/\mathbb{Q}_p$ is *ramified*, if $e > 1$ and *unramified*, if $e = 1$. As in the theory of Galois rings, the maximal ideal of the integer ring of $\mathbb{F}$ is generated by p. Moreover, when the extension is unramified, the residue class field exntension is of the same degree than the extension of $\mathbb{Q}_p$: Let $n = [\mathbb{F} : \mathbb{Q}_p]$. Then $\mathbb{Z}_{p^\infty}/p\mathbb{Z}_{p^\infty} \cong \mathbb{F}_p$, and $\mathbb{Z}_{\mathbb{F}}/p\mathbb{Z}_{\mathbb{F}} \cong \mathbb{F}_{p^n}$. In general case the connection is given by $n = ef$, where e is the ramification index and f is degree of the residue class field extension.

It can be shown that each p-adic number field has an unramified extension of arbitrary degree m, and that this extension is unique up to isomorphism. Furthermore, this extension is obtained by adjoining the n:th root of unity, where $n = p^m - 1$.

Another formulation of Hensel's lemma holds in p-adic number fields. Here we denote the projection $\mathbb{Z}_{p^\infty} \to \mathbb{Z}_{p^\infty}/p\mathbb{Z}_{p^\infty} \cong \mathbb{F}_p$ by π as usual.