Corollary. *For each $s \in S$ there exists a representation*

$$s = \sum_{i=0}^{n-1} r_i \alpha^i,$$

where $r_i \in R$ and n is the degree of corresponding residue class field extension.

Proof. We can choose $N = \{\sum_{i=0}^{n-1} r_i \alpha^i \mid r_i \in R\}$ in Nakayama's lemma as well. □

In the continuation we suppose that the maximal ideal of R is a principal ideal generated by element p. If there is another element q that generates the ideal pR, then p can be written $p = r_1 q$ and $q = r_2 p$, consequently $p = r_1 r_2 p$. If either r_1 or r_2 were not a unit, then we would get a contradiction by multiplying by p sufficiently many times. We can now assume that the generator of $\mathfrak{r}$ is fixed. Let d be the (uniqely determined) nilpotency degree of the generator p. First we see that all nonzero elements of R have a representation $r = up^m$, where u is a unit and exponent m is uniquely determined. In fact, if $r \in R^*$, then the representation is given by $r = rp^0$, and the exponent of p cannot be anything else than 0. If $r \notin R^*$, then r is in maximal ideal and therefore of form $r = r_1 p$. If r_1 is not a unit, we can continue the procedure to finally obtain $r = r_k p^k$, where r_k is a unit. The procedure stops before $k = d$, since we assumed r to be nonzero. The uniqueness of the exponent follows easily; if $u_1 p^m = u_2 p^n$, where $m < n$, multiplying by p^{d-n} we see that $u_1 p^{d-(n-m)} = 0$ which contradicts the definition of nilpotency degree.

Definition. The mapping $R \setminus 0 \to \{0, 1, \ldots, d-1\}$ $r = up^k \to k$ is called a *(exponent) valuation* of R, and the exponent in representation is said to be the *order* of r with respect to p. Note that this definition must not make any sense unless speaking about local ring with principal maximal ideal.

Lemma II.4.3. *Let R be local ring whose maximal ideal $\mathfrak{r}$ is principal, $\mathfrak{r} = pR$ and let d be the nilpotency degree of p. All the proper ideals of R are*

$$0 = p^d R \subset p^{d-1} R \subset \ldots \subset p^2 R \subset pR.$$

Further, the inclusions are proper.

Proof. Let J be any proper ideal, and m be the least value of any element in J. Since J is proper, $m \geq 1$. Choose an element such that $j = up^m \in J$. It follows that $p^m = u^{-1} j \in J$ and therefore $p^m R \subseteq J$. Pick then any element k in J. Then $k = u_1 p^n$, where $n \geq m$, so $k = u_1 p^{n-m} p^m \in p^m R$. Then $J \subseteq p^m R$ as well. The fact that all inclusions above are strict follows from the fact that the nilpotency degree of $\mathfrak{r} = pR$ is also d, and d is the smallest integer such that $p^{d-1} R = p^d R$ (see corollary II.3). □

Let R be as above, and S be an unramified extension of R. Then the maximal ideal of S, $\mathfrak{s}$, is also generated by p, this follows from the facts that clearly $pS \subseteq \mathfrak{s}$, but also

$$\mathfrak{s} = \mathfrak{r}S = \{\sum r_i s_i \mid r_i \in \mathfrak{r}, s_i \in S\} = \{p \sum r'_i s_i \mid r'_i \in R, s_i \in S\} \subseteq pS.$$

Therefore, the nilpotency degree of $\mathfrak{s}$ is also d, and the ideals of S are given in the same fashion as the ideals of R. Furthermore, the valuation is extended to S the range unchanged.

Let us now study the natural chain of projections:

$$S \cong S/\mathfrak{s}^d \longrightarrow S/\mathfrak{s}^{d-1} \longrightarrow \ldots \longrightarrow S/\mathfrak{s}^2 \longrightarrow S/\mathfrak{s} = \mathbb{F},$$

each projection is defined by

$$\pi_i : S/\mathfrak{s}^i \to S/\mathfrak{s}^{i-1} : \pi_i(s + \mathfrak{s}^i) = s + \mathfrak{s}^{i-1}.$$

The kernel of π_i consists clearly of those elements where $s \in \mathfrak{s}^{i-1}$. It is natural to denote this set by $\mathfrak{s}^{i-1}/\mathfrak{s}^i$. We get an isomorphism

$$(S/\mathfrak{s}^i)/(\mathfrak{s}^{i-1}/\mathfrak{s}^i) \cong S/\mathfrak{s}^{i-1}$$

and consequently $\left|S/\mathfrak{s}^i\right| = \left|\mathfrak{s}^{i-1}/\mathfrak{s}^i\right| \cdot \left|S/\mathfrak{s}^{i-1}\right|$. Now we can compute the cardinality of S:

$$\begin{aligned} |S| &= \left|S/\mathfrak{s}^d\right| = \left|\mathfrak{s}^{d-1}/\mathfrak{s}^d\right| \cdot \left|S/\mathfrak{s}^{d-1}\right| \\ &= \left|\mathfrak{s}^{d-1}/\mathfrak{s}^d\right| \left|\mathfrak{s}^{d-2}/\mathfrak{s}^{d-1}\right| \cdot \ldots \cdot \left|\mathfrak{s}^1/\mathfrak{s}^2\right| \left|S/\mathfrak{s}\right|. \end{aligned}$$

But this is not all we can say about the cardinality of S. We can see that each set $\mathfrak{s}^{i-1}/\mathfrak{s}^i$ becomes a vector space over the residue class field $S/\mathfrak{s}$, the scalar multiplication defined by

$$(c + \mathfrak{s})(v + \mathfrak{s}^i) = cv + \mathfrak{s}^i.$$

The definition is independent from the choise of representative, since if $c_1 = c_2 + s$, where $s \in \mathfrak{s}$, we have

$$(c_1 + \mathfrak{s})(v + \mathfrak{s}^i) = c_1 v + \mathfrak{s}^i = c_2 v + sv + \mathfrak{s}^i = c_2 v + \mathfrak{s}^i = (c_2 + \mathfrak{s})(v + \mathfrak{s}^i),$$

because $s \in \mathfrak{s}$ and $v \in \mathfrak{s}^{i-1}$. Therefore, the cardinality of $\mathfrak{s}^{i-1}/\mathfrak{s}^i$ is a power of $|\mathbb{F}|$. Here we needed not the fact that S is a principal ideal ring, and as a by-product we get

Corollary. *The cardinality of a finite local ring is a prime power.*

When S is a principal ideal ring each vector space $\mathfrak{s}^{i-1}/\mathfrak{s}^i = p^{i-1}S/p^iS$ is of dimension one; the dimension is at most one, since each element in $p^{i-1}S$ is of form sp^{i-1}. The dimension is at least one, since the inclusion $p^iS \subset p^{i-1}S$ is strict. Consequently $\left|p^{i-1}S/p^iS\right| = |\mathbb{F}|$ and $|S| = |\mathbb{F}|^d$.

Theorem II.4.4. *Assume that S/R is an unramified extension and that R is a principal ideal ring. Then $S = R[\alpha]$ consists precicely of elements of form $\sum_{i=0}^{n-1} r_i\alpha^i$, where r_i is in R. The representation is unique. The cardinality of S is $|S| = |R|^n$, where n is the degree of the correspondening residue class field extension.*

Proof. It has been observed that $|S| = |\mathbb{F}|^d$. Similary $|R| = |\mathbb{K}|^d$. The claims follow from the fact $|\mathbb{F}| = |\mathbb{K}|^n$. $\square$

Theorem II.4.5 (Unramified extensions of principal ideal rings). *Let R be a local principal ideal ring. The ring extension S/R is unramified if and only if there exists a basic irreducible monic polynomial $f \in R[X]$ such that $S \simeq R[X]/\langle f(X)\rangle$.*

Proof. Assume first that f is monic basic irreducible. We will show that $R[X]/\langle f\rangle$ is a local unramified extension of R (here R is assumed to be embedded in the quotient ring). Let $n = \deg f$. First we fix the set of representatives to be all polynomials in $R[X]$ of degree at most $n-1$. This set we can always obtain, since f is monic and the division algorthim can be used. We claim that the maximal ideal of $R[X]/\langle f\rangle$ consists precisely of those elements, whose representative has coefficients in $\mathfrak{r}$. Note that by lemma II.3.6 this property will be preserved even if we had begun with another set of representatives. It is obvious that the set descibed is a proper ideal. Suppose now that it is properly contained in an ideal J. Choose an element $g + \langle f\rangle \in J \setminus \mathfrak{r}[X] + \langle f\rangle$, and denote $g = a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$. By the choise of g at least one of the coefficients is not in $\mathfrak{r}$ and consequently $\pi g \neq 0$. Because πf were assumed to be irreducible, and $\deg \pi g < \deg \pi f$ (f is monic polynomial of degree n), we have $g.c.d(\pi f, \pi g) = 1$ and also $g.c.d(f, g) = 1$. Then there are polynomials λ_1 and λ_2 in $R[X]$ such that $\lambda_1 g + \lambda_2 f = 1$. Therefore

$$1 + \langle f\rangle = \lambda_1 g + \langle f\rangle$$

is in J, consequently $J = R[X]/\langle f\rangle$.

Assume now that S is an unramified extension of R. Let α and n be as in theorem II.4.2, and $\overline{f}$ be the minimal polynomial of $\overline{\alpha}$. Mapping $\pi : R[X] \to \mathbb{K}[X]$ is surjective, so we take a lift of $\overline{f}$, say $h \in R[X]$. We can also assume that h is chosen to be monic polynomial of degree $n = \deg \overline{f}$. By corollary of lemma II.4.2 we have a representation

$$h(\alpha) = \sum_{i=0}^{n-1} h_i\alpha^i,$$

where $h_i \in R$. Projecting modulo $\mathfrak{s}$ we obtain

$$0 = \overline{f}(\overline{\alpha}) = \pi h_0 + \pi h_1\overline{\alpha} + \ldots + \pi h_{n-1}\overline{\alpha}^{n-1},$$

so all coeffifients πh_i are zero, since $\overline{f}$ was the minimal polynomial of $\overline{\alpha}$. Further, the coefficients h_i are in $\mathfrak{s} \cap R = \mathfrak{r}$. Let

$$g(X) = h_0 + h_1X + \ldots + h_{n-1}X^{n-1}$$

and $f(X) = h(X) - g(X)$. We see that $f(\alpha) = h(\alpha) - h(\alpha) = 0$ and $\pi f = \pi h - \pi g = \overline{f}$ is irreducible as a minimal polynomial, so f is basic irreducible. Finally we introduce a substitution morphism

$$F : R[X]/\langle f(X)\rangle \to S, \quad F(p(X) + \langle f(X)\rangle) = p(\alpha).$$

It is clear that F is a morphism. Since $f(\alpha) = 0$, the value of F is independent of the choise of the representative. Furthermore, it was shown in corollary of II.4.2 that F is surjective. It is obvious that $|R[X]/\langle f(X)\rangle| = |R|^n$. Then F is injective by theorem II.4.4 $\square$

EXAMPLE. Let $R = \mathbb{Z}_4$ and $f(X) = X^2 + 2$. Then f has no zeros in $\mathbb{Z}_4$, and the quotient ring

$$S = \mathbb{Z}_4[X]/\langle X^2 + 2\rangle \cong \{a + b\alpha \mid a, b \in \mathbb{Z}_4, \alpha^2 = 2\}$$

is easily verified that $S/\alpha S \cong \mathbb{F}_2$. However, S is not unramified, the phenomenon that 2 divides into proper factors in S, $2 = \alpha^2$ is called *ramification* of 2. Note also that $\pi(X^2 + 2) = X^2$, so $X^2 + 2$ is not basic irreducible.

II.5 Galois theory briefly.

In this chapter we assume that S and R are finite local commutative rings and that R is a principal ideal ring and a subring of S. Let H be the group of automorphisms of S. For any subgroup of H, say G we let

$$\mathrm{Inv}(G) = \{s \in S \mid \sigma(s) = s \text{ for all } \sigma \in H\}.$$

It is obvious that $\mathrm{Inv}(G)$ is a subring of S.

DEFINITION. $\mathrm{Inv}(G)$ is called the *invariant ring* of group G.

DEFINITION. Ring S is called a *Galois extension* of R if S is an unramified extension of R and the *Galois group* G of extension S/R is the subgroup of H satisfying $\mathrm{Inv}(G) = R$. Then we write $G = \mathrm{Gal}(S/R)$. The automorphisms fixing all elements in R are also called R-automorphisms

Assume now that S is a Galois extension of R. Let the maximal ideals of S and R be $\mathfrak{s}$ and $\mathfrak{r}$ respectively. We also denote $\mathbb{F} = S/\mathfrak{s}$ and $\mathbb{K} = R/\mathfrak{r}$. The projection $\pi : S \to \mathbb{F}$ can be restricted to R, so we use the same notation for projection $\pi : R \to \mathbb{K}$.

Lemma II.5.1. *Let f be a polynomial in ring $R[X]$ Assume that $\pi f \neq 0$ and that πf has a simple zero $\overline{\alpha}$ in $\mathbb{K}$. Then polynomial f has exactly one zero $\alpha \in R$ such that $\pi\alpha = \overline{\alpha}$.*

Proof. By assumption πf has a linear factor $X - \overline{\alpha}$, denote $\pi f = (X - \overline{\alpha})\overline{h}$. Then $g.c.d(X - \overline{\alpha}, \overline{h}) = 1$, since $\overline{\alpha}$ is a simple zero. By Hensel's lemma f can be factored in ring $R[X]$ to get $f = h_1 h_2$, where $\pi h_1 = X - \overline{\alpha}$ and $\pi h_2 = \overline{h}$. Let h be any lift of $\overline{h}$ and α' any lift of $\overline{\alpha}$. Then

$$f = (X - \alpha' + g_1)(h + g_2),$$

where g_1 and g_2 are in $\mathfrak{r}[X]$. We see directly that $\deg(\pi(X-\alpha'+g_1))=1$. By lemma II.3.7 there is a monic polynomial of degree one, say $p=X-\alpha$ and a unit such that

$$X-\alpha'+g_1=up=u(X-\alpha).$$

Now $\pi(X-\alpha'+g_1)=X-\pi\alpha'=X-\overline{\alpha}$ and $\pi u(X-\alpha)=\overline{c}(X-\pi\alpha)$. Therefore $\overline{c}=1$ and $\pi\alpha=\overline{\alpha}$. Now we see that

$$f=u(X-\alpha)(h+g_2)=(X-\alpha)\underbrace{u(h+g_2)}_{g}$$

has α as a zero.

Assume that there is an other zero of f, say β, which satisfies $\pi\beta=\overline{\alpha}$. Then $0=f(\beta)=(\beta-\alpha)g(\beta)$, and $\pi g(\beta)=\overline{h}(\overline{\alpha})\neq 0$, since α was supposed to be a simple zero. It follows that $g(\beta)$ is a unit, and consequently $\beta=\alpha$. $\square$

DEFINITION. Let S and R be as before. If $\sigma: S\to S$ is an R-morphism, we say that $\overline{\sigma}: S/\mathfrak{s}\to S/\mathfrak{s}$ given by

$$\overline{\sigma}(s+\mathfrak{s})=\sigma(s)+\mathfrak{s}$$

is *induced* by sigma. Now $\overline{\sigma}$ is well-defined, since σ fixes all elements of R, espcesially the generator of the maximal ideal, so if $s_1-s_2=ps$, where s is any element of S and p generates the maximal ideal, we also see that

$$\sigma(s_1)-\sigma(s_2)=\sigma(s_1-s_2)=\sigma(ps)=\sigma(p)\sigma(s)=p\sigma(s)\in\mathfrak{s}.$$

It is clear that $\overline{\sigma}$ is also a morphism.

Let the residue class fields be $\mathbb{K}=R/\mathfrak{r}$ and $\mathbb{F}=S/\mathfrak{s}$. If σ_1 and σ_2 are R-automorphisms of S, then $\overline{\sigma_2\sigma_1}=\overline{\sigma}_1\overline{\sigma}_2$ and $\overline{\sigma}_1$ and $\overline{\sigma}_2$ are $\mathbb{K}$-automorphisms of $\mathbb{F}$. This is easy to verify, for example

$$\overline{\sigma_1\sigma_2}(s+\mathfrak{s})=\sigma_1\sigma_2(s)+\mathfrak{s}=\overline{\sigma}_1(\sigma_2(s)+\mathfrak{s})=\overline{\sigma_1}(\overline{\sigma_2}(s+\mathfrak{s}))$$

and

$$\overline{\sigma}((r+\mathfrak{s})(s+\mathfrak{s}))=\overline{\sigma}(rs+\mathfrak{s})=\sigma(rs)+\mathfrak{s}=r\sigma(s)+\mathfrak{s}=(r+\mathfrak{s})(\overline{\sigma}(s+\mathfrak{s}).$$

Briefly, the mapping $\mathrm{Aut}_R(S)\to\mathrm{Aut}_{\mathbb{K}}(\mathbb{F}):\sigma\mapsto\overline{\sigma}$ is a morphism.

Theorem II.5.2 (Lifting theorem). *Let S be an unramified extension of R with maximal ideal $\mathfrak{s}$ and residue class field $\mathbb{F}=S/\mathfrak{s}$. For each $\mathbb{K}$-automorphism $\tilde{\sigma}$ there exists unique R-automorphism of S that induces $\tilde{\sigma}$.*

Proof. Let $\mathbb{F}=\mathbb{K}[\overline{\alpha}]$ and $\overline{f}$ be the minimal polynomial of $\overline{\alpha}$ over $\mathbb{K}$. By theorem II.4.5 there exists a basic irreducible polynomial $f\in R[X]\subseteq S[X]$ such that $\pi f=\overline{f}$ $S\cong R[X]/\langle f\rangle$, and by lemma II.5.1 there is unique α in S such that $f(\alpha)=0$ and $\pi\alpha=\overline{\alpha}$. Indeed, S becomes a free R-module generated by $\{1,\alpha,\alpha^2,\dots,\alpha^{n-1}\}$.

Let $\tilde{\sigma} : \mathbb{F} \to \mathbb{F}$ be any $\mathbb{K}$-automorphism. Denote $\tilde{\sigma}(\overline{\alpha}) = \overline{\alpha}_0$. Then also $\overline{f}(\overline{\alpha}_0) = 0$, and by lemma II.5.1 there exists unique α_0 in S such that $f(\alpha_0) = 0$ and $\pi\alpha_0 = \overline{\alpha}_0$. Define now $\sigma(\alpha) = \alpha_0$ and extend this by

$$\sigma(r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{n-1}) = r_0 + r_1\alpha_0 + \ldots + r_{n-1}\alpha_0^{n-1}.$$

It is obvious that σ becomes a morphism, and even an automorphism. The latter is verified by the fact that $R[\alpha_0]$ becames also a free R-module generated by the set $\{1, \alpha_0, \alpha_0^2, \ldots, \alpha_0^{n-1}\}$. Further,

$$\overline{\sigma}(\overline{\alpha}) = \overline{\sigma}(\alpha + \mathfrak{s}) = \sigma(\alpha) + \mathfrak{s} = \alpha_0 + \mathfrak{s} = \overline{\alpha}_0 = \tilde{\sigma}(\overline{\alpha}),$$

so σ induces the original $\overline{\sigma}$.

Assume on contrary, that there is an other R-morphism σ_1 that induces $\tilde{\sigma}$. Then

$$0 = \sigma_1(f(\alpha)) = f(\sigma_1(\alpha)),$$

so $\beta = \sigma_1(\alpha)$ is a zero of f. By assumption

$$\pi\alpha_0 = \overline{\alpha}_0 = \tilde{\sigma}(\overline{\alpha}) = \tilde{\sigma}(\alpha + \mathfrak{s}) = \overline{\sigma}_1(\alpha + \mathfrak{s}) = \beta + \mathfrak{s} = \pi\beta.$$

By lemma II.5.1 $\alpha_0 = \beta$ and consequently $\sigma_1 = \sigma$. □

Theorem II.5.3. *Let S be an unramified extension of R. Then S is a Galois extension of R with Galois group isomorphic to the Galois group of corresponding residue class field extension.*

Proof. The mapping $\mathrm{Aut}_R(S) \to \mathrm{Aut}_{\mathbb{K}}(\mathbb{F}) : \sigma \mapsto \overline{\sigma}$ is a morphism, and it is surjective and injective by theorem II.5.2. □

Definition Galois ring $GR(p^e, m)$ is a Galois extension extension of prime ring $\mathbb{Z}_{p^e}$ of degree m.

A slight modification in lifting theorem shows that Galois extension of of a prime ring of degree m is uniquely determined up to isomorphism.

If $GR(p^m, d)$ is a Galois extension of degree m of $\mathbb{Z}_{p^e}$ with Galois group generated by automorphism σ (σ is also called Frobenius-automorphism), we can define the *trace* of an element by

$$T(s) = s + \sigma(s) + \sigma^2(s) + \ldots + \sigma^{m-1}(s).$$

It is clear that $\sigma(T(s)) = T(s)$, so $T(s)$ always belongs to the bottom ring. The *characters* of the additive group of S are obtained by choosing a primitive p^e:th root of unity, say ω and defining

$$e(s) = \omega^{T(s)}.$$

Above the power is understood in a natural way.

II.6 More about Galois rings.

Now we fix a prime number p and a prime ring $\mathbb{Z}_{p^e}$. As we saw before, $\mathbb{Z}_{p^e}$ is local ring with principal maximal ideal $p\mathbb{Z}_{p^e}$. Recall that any element can be written as $a = up^i$ with unique exponent of p, and so p determines an (exponent) valuation on $\mathbb{Z}_{p^e}$. Obviously unit u must not be unique. It also is obvious that the quotient field is $\mathbb{F}_p \cong \mathbb{Z}_{p^e}/p\mathbb{Z}_{p^e}$. We will fix the set of representatives modulo $p\mathbb{Z}_{p^e}$ to be

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

Such a set is called *transversal*. Then $\mathbb{Z}_{p^e}$ is disjoint union of cosets $p\mathbb{Z}_{p^e}$, $1+p\mathbb{Z}_{p^e}$, $2+p\mathbb{Z}_{p^e}$, $\ldots$, $p-1+p\mathbb{Z}_{p^e}$, so each element has a representation of form $a = u_0+a_1p$, with unique $u_0 \in T$. Furthermore, a_1 has a representation $u' = u_1+a_2p$ with unique $u_1 \in T$. Substituting this we get $a = u_0 + u_1p + a_2p^2$. Continuing this procedure we obtain a representation

$$a = u_0 + u_1p + u_2p^2 + \ldots + u_{e-1}p^{e-1},$$

where $u_i \in T$. This representation is unique by construction, when T remains fixed. It is obvious that the least index i where $u_i \neq 0$ is the order of a with respect to exponent valuation.

The Galois extension of $\mathbb{Z}_{p^e}$ of degree m is equipped with a generating element α. It is clear that alpha is a root of unity over $\mathbb{Z}_{p^e}$. The construction of extesion of degree m can be done as follows:

Let $n = p^m - 1$. Then the polynomial $X^n - 1$ decomposes into pairwise coprime factors in $\mathbb{F}_p$, in fact, these factors are all monic irreducible polynomials $\neq X$ over $\mathbb{F}_p$ whose degree divides m. Furthermore, there is a factor of degree m, say $\overline{h}$ that has got a primitive n:th root as a zero. Let us denote this root by $\overline{\zeta}$. We can lift the decomposition of $X^n - 1$ in $\mathbb{F}_p$ into $\mathbb{Z}_{p^e}$ by Hensel's lemma and choose the factor h that corresponds $\overline{h}$. Then we can form the Galois ring $GR(p^e, m)$:

$$GR(p^e, m) = \mathbb{Z}_{p^e}[X]/\langle h \rangle.$$

There exists unique $\zeta \in GR(p^e, m)$ that satisties both $f(\zeta) = 0$ and $\pi\zeta = \overline{\zeta}$. The element ζ is also a primitive n:th root of unity over $\mathbb{Z}_{p^e}$; since clearly $\zeta^n = 1$, and if $\zeta^k = 1$ with $k < m$, we would have $\overline{\zeta}^k = 1$ also. Each element in $GR(p^e, m)$ has unique representation

$$a = a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{m-1}\zeta^{m-1}.$$

So $GR(p^e, m) = \mathbb{Z}_{p^e}[\zeta]$, and we can also say that Galois rings are obtained by adoining a root of unity to the prime ring.

Definition. The set $\mathcal{T} = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$ is called the *set of Teichmüller representatives* or briefly *Teichmüller set*.