Lemma 8.34

If $P \in \operatorname{Spec} R$, then $PS \neq S$.

Proof: Can assume $P \neq 0$. Since $P \neq P^2$, there is $\pi \in P \setminus P^2$. Then $(\pi) \subseteq P \Rightarrow P \mid (\pi)$
$\Rightarrow (\pi) = PI$ for an ideal I with $P \nmid I \Rightarrow P + I = R$ by maximality of P
Can write $1 = b + r$ for some $b \in P$, $r \in I \Rightarrow r \notin P$ and $rP \subseteq IP = (\pi)$.
If $PS = S$, then $rS = rPS \subseteq \pi S \Rightarrow r = \pi x$ for some $x \in S$. Since $x = \frac{r}{\pi} \in Q(R) = K$,
so $x \in S \cap K = R$ (Lemma 8.33) $\Rightarrow r = \pi x \in P$ ↯ $\square$

Corollary 8.35

If $P \in \operatorname{Spec} R$, then

$$PS = \prod_{i=1}^{r} Q_i^{e_i}$$

For unique prime ideals $Q_i \in \operatorname{Spec} S$, unique $r > 0$ and $e_i > 0$.
By Lemma 8.32 the Q_i are precisely the prime ideals lying over P.
In particular, over each prime ideal of P there is a prime ideal of S, and there are only finitely many such prime ideals.

The picture is

$$\begin{tikzcd} \operatorname{Spec} S \arrow[d, two heads, "\text{surjective}"'] & Q \arrow[d, mapsto] \\ \operatorname{Spec} R & Q \cap R \end{tikzcd}$$

This picture is actually true for any finite ring extension. But in general, we can't say much about how many primes are lying over a prime and how "big" they are. For Dedekind domains there is a beautiful relation.

Def 8.36

Let
$$PS = \prod_{i=1}^{r} Q_i^{e_i}.$$
The exponent e_i is called the ramification index.

The dimension
$$f_i := [S/Q_i : R/P]$$
Since $R \subseteq S$ is finite, $R/P \subseteq S/Q_i$ is finite. It is called a residue field extension

is called the inertia degree.

Thm 8.37

For any $P \in \operatorname{Spec} R$ the following fundamental equation holds:
$$\sum_{i=1}^{r} e_i f_i = n \ (= \dim_K L)$$

Proof: Chinese Remainder Theorem gives
$$S/PS \simeq \prod_{i=1}^{r} S/Q_i^{e_i}.$$
Set $k := R/P$. If we can show that
$$\dim_k S/PS = n \quad \text{and} \quad \dim_k S/Q_i^{e_i} = e_i f_i \ \forall i,$$
then we are done.

First part: let $\omega_1, \dots, \omega_m$ be such that $\overline{\omega_1}, \dots, \overline{\omega_m} \in S/PS$ is an R/P-basis.

We will show that $\omega_1, \dots, \omega_m$ is a K-basis of $L \Rightarrow m = n$.

Suppose, $\omega_1 \dots \omega_m$ would be linearly dependent over K. Then they are also linearly dependent over R, so $a_1\omega_1 + \dots + a_m\omega_m = 0$ for some $a_i \in R$, not all zero.

Let $I := (a_1, \dots, a_m) \subseteq R$. Recall from Lemma 8.14 that $I \subsetneq IP^{-1}$. Applying $(-)^{-1}$ yields $I^{-1} \supsetneq I^{-1}P$ (recall that every non-zero ideal is invertible). Hence, there is $a \in I^{-1}$ with $a \notin I^{-1}P$. Since $a \in I^{-1} \Rightarrow aI \subseteq R \Rightarrow aa_i \in R \ \forall i$.

Since $a \notin I^{-1}P \Rightarrow aI \nsubseteq P \Rightarrow$ not all aa_i are contained in P.

Hence, when reducing $a_1\omega_1 + \dots + a_m\omega_m = 0 \mod P$, we get a relation
$$\overline{a_1}\,\overline{\omega_1} + \dots + \overline{a_m}\,\overline{\omega_m} = 0 \in S/PS,$$

not all $\bar{a}_i = 0$. Contradiction to $\bar{\omega}_1, \dots, \bar{\omega}_m$ being a basis. Hence, $\omega_1, \dots, \omega_m$ are linearly independent over K.

Still need to show that $\omega_1, \dots, \omega_m$ span L. Set $M := R\cdot\{\omega_1, \dots, \omega_m\}$ and $N := S/M$ as R-module. We have $M/P = R/P \cdot \{\omega_1, \dots, \omega_m\} = S/PS$, hence $S = M + PS$, hence

$$N = S/M = {}^{PS}/_{M} = P\,S/M = PN.$$

Since S is a finitely generated R-module, so is N. Let $\alpha_1, \dots, \alpha_s$ be a generating system. The $N = PN$ implies

$$\alpha_i = \sum_j a_{ij}\alpha_j \quad \text{for some } a_{ij} \in P.$$

Let $A := (a_{ij}) - 1_s \Rightarrow A \cdot (\alpha_1, \dots, \alpha_s)^t = 0$

$$\Rightarrow 0 = \operatorname{adj}(A) A \cdot (\alpha_1, \dots, \alpha_s)^t = d(\alpha_1, \dots, \alpha_s)^t, \quad d := \det(A)$$

$$\Rightarrow dN = 0 \Rightarrow dS \subseteq M = R\cdot\{\omega_1, \dots, \omega_m\}.$$

Since $a_{ij} \in P \ \forall i,j \Rightarrow \det(A \bmod P) = (-1)^s \neq 0 \Rightarrow \det(A) \neq 0$

$$\Rightarrow S \subseteq R \cdot \left\{\frac{\omega_1}{d}, \dots, \frac{\omega_m}{d}\right\} \Rightarrow L = K \cdot \{\omega_1, \dots, \omega_m\}.$$

We have now proven that $\dim_k S/PS = n$.

<u>Second part</u>: Need to show that $\dim_k S/Q_i^{e_i} = e_i f_i$. We have a chain

$$S/Q_i^{e_i} \supsetneq Q_i/Q_i^{e_i} \supsetneq Q_i^2/Q_i^{e_i} \supsetneq \dots \supsetneq Q_i^{e_i-1}/Q_i \supsetneq 0$$

of R/P-vector spaces. In the proof of Prop 8.24 we have shown that

$$\dim_{S/Q_i} Q_i^j/Q_i^{j+1} = 1 \ \forall j$$

Hence,

$$\dim_k S/Q_i^{e_i} = e_i \cdot \dim_k S/Q_i = e_i \cdot f_i. \quad \square$$

Observe: the smaller the inertia degree, the more P splits into different primes.
We introduce some terminology to describe how P splits in S.

Def 8.38

With notation as above, P is called:

- non-split if $r = 1$
- split if $r > 1$
- totally split if $r = n$ ($\Leftrightarrow e_i = 1 = f_i \ \forall i$)

Q_i is called:

- unramified (over P) if $e_i = 1$ and the residue field extension $R/P \subseteq S/Q_i$ is separable (the latter is always true for number fields since R/p is finite).
- ramified if not unramified

P is called:

- unramified if all Q_i unramified
- ramified if not unramified
- totally ramified if a ramification index is equal to n
- inert non-split and unramified ($\Leftrightarrow PS$ is prime)

Questions: How do we compute the factorization of PS into prime ideals?
How do we find the primes which are unramified, inert, etc.?

8.5 Geometric interlude

Let k be a commutative ring and let $I \subseteq k[X_1, \dots, X_n]$ be an ideal.
For a k-algebra R define

$$Z_I(R) := \{ x = (x_1, \dots, x_n) \in R^n \mid f(x) = 0 \ \forall f \in I \} \subseteq R^n,$$

the zero set of I over R. Let $A := k[X_1, \dots, X_n]/_I$.
Any $x \in Z_I(R)$ defines a k-algebra morphism $\varphi_x : A \to R$, $\bar{f} \mapsto f(x)$
(this is the morphism induced by $X_i \mapsto x_i$).
Conversely, any k-algebra morphism $\varphi : A \to R$ defines a zero $x_\varphi := (\varphi(\bar{X}_1), \dots, \varphi(\bar{X}_n))$ of I.
We thus have a natural bijection

$$Z_I(R) \simeq \mathrm{Hom}_{k\text{-Al}}(A, R).$$

Now, consider the case where $R = K$ is a field. Any k-algebra morphism

$\varphi: A \to K$ defines a prime ideal $P_\varphi := \varphi^{-1}(0)$ of A with

$$\underbrace{Q(A/P_\varphi)}_{\substack{\text{field of fractions}\\ \text{of } A/P_\varphi}} \hookrightarrow K$$

Different morphisms $\varphi: A \to K$, $\varphi': A' \to K'$ can define the same prime ideal, namely if there is a diagram

$$\begin{tikzcd}
 & K'' & \\
K \arrow[ur] & & K' \arrow[ul] \\
 & A \arrow[ul, "\varphi"] \arrow[ur, "\varphi'"'] &
\end{tikzcd}$$

$\rightsquigarrow$ consider equivalence relation on $\coprod_{\substack{K \supseteq k\\ \text{field}}} \mathrm{Hom}_{k\text{-Alg}}(A,K)$.

Conversely, any prime ideal P of A defines such a class by

$$\varphi_P : A \twoheadrightarrow A/P \hookrightarrow Q(A/P).$$

<u>Summary</u>: Field valued solutions of $I \mathrel{\hat{=}}$ prime ideals of A

(This is the beginning of algebraic geometry.)