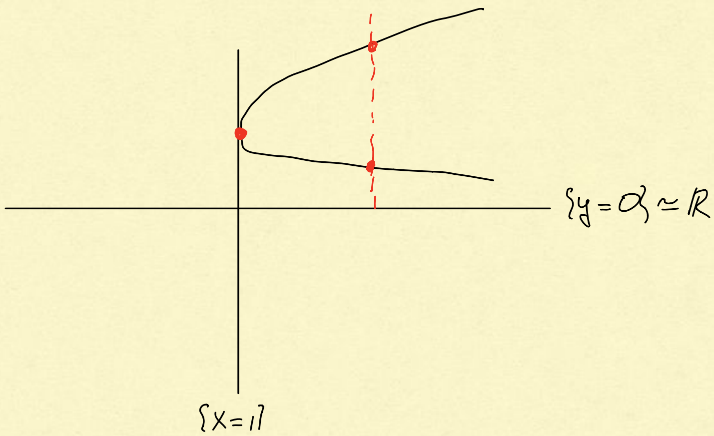
Lecture 22 (22.1.)

Consider $f := (Y-2)^2 - (X-1) \in \mathbb{R}[X,Y]$.

Picture of $Z_f(\mathbb{R})$:



The ring $A = \mathbb{R}[X,Y]/(f)$ is a Dedekind domain: noetherian (✓), one-dimensional (picture), and integrally closed (no singularities, picture).

We have $\mathbb{R}[X] \hookrightarrow A$. In fact, A is the integral closure of $\mathbb{R}[X]$ in $Q(A)$.

The morphism

$$\begin{array}{ccc} \operatorname{Spec} A & & Q \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathbb{R}[X] & & Q^{-1} \end{array} \quad \text{corresponds to the projection} \quad \begin{array}{c} Z_f(\mathbb{R}) \\ \downarrow \\ \mathbb{R} \end{array}$$

Over each $a > 1$ there are precisely two distinct points, namely $(a, 2+\sqrt{a-1})$ and $(a, 2-\sqrt{a-1})$. These two points correspond to the prime ideals

$$M_{a\pm} := (X-a,\ Y-2 \pm \sqrt{a-1}) \in \operatorname{Spec} A$$

These are precisely the primes over

$$(X-a) \in \operatorname{Spec} \mathbb{R}[X]$$

$\Rightarrow$ $(X-a)$ unramified in A, $(X-a) = M_{a+} \cdot M_{a-}$ in A

But for $a=1$, there is only one point, namely $(1,2)$. The corresponding prime is

$$\mathcal{M}_1 := (X-1, Y-2),$$

$\Rightarrow (X-1)$ ramified in A, $(X-1) = \mathcal{M}_1^2$.

8.6 Computing factorizations

Let's get serious again.
Setup as before. Since $K \subseteq L$ is separable, there is a primitive element $\Theta \in S$, i.e. $L = K(\Theta)$, see Thm 2.23. Recall (see Exercise 4.2) that we do not necessarily have $S = R[\Theta]$. In the number field case, S is a free R-module and the index $[S : R[\Theta]]$ is finite. To measure this defect in the general setting, we introduce the following.

Def 8.39

The conductor of $R[\Theta]$ in S is

$$\mathfrak{F} := \mathfrak{F}_{S|R[\Theta]} := \{\alpha \in S \mid \alpha S \subseteq R[\Theta]\}.$$

Lemma 8.40

$\mathfrak{F}$ is an ideal in both $R[\Theta]$ and S. It is the largest ideal with this property. Moreover, $\mathfrak{F} \neq 0$.

Proof: If $\alpha \in \mathfrak{F}$ then $\alpha = \alpha \cdot 1 \in R[\Theta]$ by definition, so $\mathfrak{F} \subseteq R[\Theta]$.
If $\alpha, \beta \in \mathfrak{F}$, clearly $(\alpha+\beta)S \subseteq \alpha S + \beta S \subseteq R[\Theta]$. If $\alpha \in \mathfrak{F}$ and $\beta \in S$, then $\beta\alpha S = \alpha\beta S \subseteq \alpha S \subseteq R[\Theta] \Rightarrow \beta\alpha \in \mathfrak{F}$. $\Rightarrow \mathfrak{F}$ ideal.
If I is an ideal in both S and in $R[\Theta]$, then $xS \subseteq I \subseteq R[\Theta]$ $\forall x \in I$, so $I \subseteq \mathfrak{F}$.

Recall that S is a finitely generated R-module, so $S = R \cdot \{\alpha_1, \dots, \alpha_n\}$.
Since $L = K(\Theta)$, we can write $\alpha_i = \sum \frac{r_{ij}}{r'_{ij}} \Theta^j$ for some $r_{ij} \in R$, $r'_{ij} \in R \setminus \{0\}$.
Let $r := \prod_{i,j} r'_{ij} \in R \setminus \{0\}$. Then $r\alpha_i \in R[\Theta]$ $\forall i \Rightarrow rS \subseteq R[\Theta] \Rightarrow r \in \mathfrak{F}$. $\square$

Remark 8.41

In the number field case, we have $[S : R[\Theta]] \in \mathfrak{F}$.

Let $\mu \in R[X]$ be the minimal polynomial of $\Theta \in S$ over R.

Thm 8.42 (Dedekind)

Let $0 \neq P \in \operatorname{Spec} R$ be such that PS is coprime to the conductor $\mathfrak{F} = \mathfrak{F}_{S|R[\Theta]}$

Let

$$\overline{\mu} = \overline{\mu}_1^{e_1} \cdot \ldots \cdot \overline{\mu}_r^{e_r}$$

be the factorization of $\overline{\mu}$ over $R/P[X]$ into pairwise coprime irreducibles $\overline{\mu}_i$.

Let $\mu_i \in R[X]$ be a monic representative of $\overline{\mu}_i$. The the ideals

$$Q_i := (P, \mu_i(\Theta))_S \qquad \text{(ideal in } S \text{ generated by } P \text{ and } \mu_i(\Theta))$$

are precisely the prime ideals of S lying over P. Their inertia degrees are

$$f_i(P) = \deg \overline{\mu}_i$$

and

$$PS = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}.$$

is the factorization.

Proof:

Since prime ideals in S over $P \mathrel{\hat{=}}$ prime ideas in S/PS, we can transfer the problem to S/PS. Set $R' := R[\Theta]$ and $\overline{R} := R/P$. We have the following situation

$$\begin{tikzcd}
S \arrow[r, two heads] & S/PS \\
R' = R[\Theta] \arrow[u, dash] \arrow[r, two heads] & R'/PR' \arrow[u, dash] \\
R \arrow[u, dash] \arrow[r] & R/P \arrow[u, dash]
\end{tikzcd}$$

We will show that we have canonical isomorphisms

$$S/PS \simeq R'/PR' \simeq \overline{R}[X]/(\overline{\mu})$$

The latter ring is easy to understand. The first isomorphism needs the coprime

assumption: we have $PS + \mathfrak{F} = S$. Since $\mathfrak{F} \subseteq R' \subseteq S \Rightarrow PS + R' = S$
$\Rightarrow R' \longrightarrow S/_{PS}$ is surjective. The kernel is $R' \cap PS$.

We show that $R' \cap PS = PR'$.

Since PS coprime to $\mathfrak{F} \Rightarrow P$ coprime to $\mathfrak{F} \cap R$ (would otherwise get a divisor in S)

$\Rightarrow P + (\mathfrak{F} \cap R) = R \Rightarrow PR' + \mathfrak{F} = R'$

$$\Rightarrow R' \cap PS = (PR' + \mathfrak{F})(R' \cap PS) \subseteq PR'(R' \cap PS) + \mathfrak{F}(R' \cap PS)$$
$$\subset PR' + \mathfrak{F}PS \subseteq PR' + P\mathfrak{F}S \subseteq PR' + PR' \subseteq PR'$$

The second isomorphism comes from the surjective morphism $R[X] \longrightarrow \overline{R}[X]/(\overline{p})$.
The kernel is (P, p). Since $R' = R[\Theta] \simeq R[X]/(p)$, it follows that

$$R'/_{PR'} \simeq R[X]/_{(P,p)} \simeq \overline{R}[X]/_{(\overline{p})}.$$

Combined, we have an isomorphism $S/_{PS} \simeq \overline{R}[X]/(\overline{p})$. The inverse is given explicitly by $\overline{g} \longmapsto g(\Theta) \bmod PS$.

Let's look at $\overline{R}[X]/(\overline{p})$. From Chinese Remainder Theorem we get

$$A := \overline{R}[X]/(\overline{p}) = \overline{R}[X]/\left(\prod_{i=1}^{r} \overline{p}_i^{\,e_i}\right) \simeq \prod_{i=1}^{r} \overline{R}[X]/(\overline{p}_i)^{e_i}.$$

Easy observations:

1. The prime ideals in A are the principal ideals $(\overline{p_i})$
2. $[A/(\overline{p}_i) : \overline{R}] = \deg \overline{p_i}$
3. $(0) = (\overline{p}) = \bigcap_{i=1}^{r} (\overline{p}_i)^{e_i}$.
4. $\sum_{i=1}^{r} \deg \overline{p}_i \cdot e_i = \dim_{\overline{R}} A$, moreover $\dim_{\overline{R}} A = \deg p = n$ (p monic)

Now, transfer this to $\overline{S} := S/_{PS}$ using the isomorphism $\overline{g} \longmapsto g(\Theta) \bmod PS$.

1. The prime ideals in $\overline{S}$ are the ideals $\overline{Q}_i := (p_i(\Theta) \bmod PS)$
2. $[\overline{S}/\overline{Q}_i : \overline{R}] = \deg \overline{p_i}$
3. $(0) = \bigcap_{i=1}^{r} \overline{Q}_i^{\,e_i}$.

Transfer to S by taking preimages:

1. The prime ideals in S over P are precisely the ideals $Q_i := (P, p_i(\theta))_S$
2. $f_i = [S/Q_i : R/P] = \deg \bar{p}_i$
3. $PS \supseteq \bigcap_{i=1}^{r} Q_i^{e_i} = \prod_{i=1}^{r} Q_i^{e_i} \Rightarrow PS$ divides $\prod_{i=1}^{r} Q_i^{e_i}$

ideals pairwise coprime

Since we have $\sum_{i=1}^{r} e_i f_i = n$ by 4 above, we must have $PS = \prod_{i=1}^{r} Q_i^{e_i}$.

$\square$

The condition PS coprime to $\mathfrak{F}$ excludes only finitely many P. Here is a helpful criterion:

<u>Lemma 8.43</u>

In the number field case, Thm 8.42 applies to all P with $[S:R[\theta]] \notin P$.
This is satisfied if $d_{R[\theta]} \notin P$ discriminant of $R[\theta]$, easily computable

<u>Proof</u>: Since P is maximal, $P + ([S:R[\theta]]) = R$. We have $[S:R[\theta]] \in \mathfrak{F}$ (Remark 8.41), hence $PS + \mathfrak{F} = S$. Recall that

$$d_{R[\theta]} = [S:R[\theta]]^2 d_S,$$

so, if $d_{R[\theta]} \notin P$, also $[S:R[\theta]] \notin P$. $\square$

<u>Remark 8.44</u>

What do we do if PS is not coprime to $\mathfrak{F}$? Try to change θ!
You can find examples of this in Exercise 11.1.
There's also a more systematic approach, see lecture next week.