Reminder:

Consider a maximal ideal $\mathfrak{p} \subset A$. Then $\mathfrak{p}B$ is a non-zero ideal of B and therefore has a prime factorization

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

$$\begin{array}{ccccc} \mathfrak{q}_i & \subset & B & \subset & L \\ | & & | & & | \\ \mathfrak{p} & \subset & A & \subset & K \end{array}$$

with distinct maximal ideals $\mathfrak{q}_i \subset B$ and integral exponents $e_i \geqslant 1$.

Proposition 6.2.1: (a) The ideals $\mathfrak{q}_i$ are precisely the prime ideals of B above $\mathfrak{p}$.

(b) For each i the residue field $k(\mathfrak{q}_i)$ is a finite extension of the residue field $k(\mathfrak{p})$.

(c) Letting f_i denote the degree of this residue field extension, we have

$$\boxed{\sum_{i=1}^{r} e_i f_i = n.}$$

Proposition 6.2.4: Suppose that $B = A[\beta]$ and let $f \in A[X]$ be the minimal polynomial of β above K. Set $\bar{f} := f \bmod \mathfrak{p}$ and write $\bar{f} = \prod_{i=1}^{r} \bar{f}_i^{e_i}$ with inequivalent irreducible factors $\bar{f}_i \in k(\mathfrak{p})[X]$ and integral exponents $e_i \geqslant 1$. Choose $f_i \in A[X]$ with $f_i = f_i \bmod \mathfrak{p}$. Then $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$ with the prime ideals $\mathfrak{q}_i := \mathfrak{p}B + f_i(\beta)B$.

Throughout the following we impose the

Assumption: The residue field $k(\mathfrak{p})$ is perfect.

Example 6.2.6: Take $L=\mathbb{Q}(\sqrt{d}\,)$ with $d\in\mathbb{Z}\smallsetminus\{1\}$ squarefree. Then an odd prime p of $\mathbb{Z}$ with

$$\left(\frac{d}{p}\right) = \begin{cases} 0 & \text{is (totally) ramified in } \mathcal{O}_L,\\ 1 & \text{is (totally) decomposed in } \mathcal{O}_L,\\ -1 & \text{is (totally) inert in } \mathcal{O}_L.\end{cases}$$

If $\mathcal{O}_L=\mathbb{Z}[\sqrt{d}] \Rightarrow \mathcal{O}_L \cong \mathbb{Z}[X]/(X^2-d)$

$\Rightarrow \mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{F}_p[X]/(X^2-d)$

$2\beta = 1+\sqrt{d}$ | $\beta^2-\beta+\frac{1-d}{4}=0$

$(2\beta-1)^2=d$

If $\mathcal{O}_L=\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \cong \mathbb{Z}[X]/(X^2-X+\frac{1-d}{4})$

$\Rightarrow \mathcal{O}_L/p\mathcal{O}_L = \mathbb{F}_p[X]/(X^2-X+\frac{1-d}{4}) \underset{p \text{ odd}}{\cong} \mathbb{F}_p[Y]/(Y^2-d)$

$\left(\frac{d}{p}\right)=0 \iff p\mid d \iff p\cdot\mathcal{O}_L=\mathfrak{q}^2$ for $\mathfrak{q}=(p,\sqrt{d})$.

$\left(\frac{d}{p}\right)=1 \iff d\equiv a^2$ for $a\in\mathbb{Z}\smallsetminus p\mathbb{Z}$ $\rightsquigarrow (X^2-d)=(X-a)(X+a)$

$\Rightarrow p\mathcal{O}_L=\mathfrak{q}\mathfrak{q}'$, $\mathfrak{q}=(p,\sqrt{d}-a)$, $\mathfrak{q}'=(p,\sqrt{d}+a)$

$\left(\frac{d}{p}\right)=-1 \iff X^2-d$ irred. in $\mathbb{F}_p$ $\Rightarrow p\mathcal{O}_L=\mathfrak{q}$ prime.

qed

Proposition 6.2.7: For any a prime $\mathfrak{r}\subset C$ above $\mathfrak{q}\subset B$ above $\mathfrak{p}\subset A$ we have

$$e_{\mathfrak{r}|\mathfrak{p}} = e_{\mathfrak{r}|\mathfrak{q}}\cdot e_{\mathfrak{q}|\mathfrak{p}} \quad\text{and}\quad f_{\mathfrak{r}|\mathfrak{p}} = f_{\mathfrak{r}|\mathfrak{q}}\cdot f_{\mathfrak{q}|\mathfrak{p}}.$$

$$\begin{array}{ccccccc} M & \supset & C & \supset & \mathfrak{r} & & k(\mathfrak{r})\\ | & & & & & & \|\\ L & \supset & B & \supset & \mathfrak{q} & & k(\mathfrak{q})\\ | & & & & & & \|\\ K & \supset & A & \supset & \mathfrak{p} & & k(\mathfrak{p}) \end{array}$$

Proof:

$\mathfrak{p}B = \prod_i \mathfrak{q}_i^{e_i}$

$\forall i: \ \mathfrak{q}_i C = \prod_j \mathfrak{r}_{ij}^{e_{ij}}$ $\Rightarrow \mathfrak{p}C = \prod_{i,j} \mathfrak{r}_{ij}^{e_{ij}\cdot e_i}$

numbering dep. for fixed i.

$\forall i\neq i'$, $\forall j,j'$: $\mathfrak{r}_{ij}\cap B=\mathfrak{q}_i\neq\mathfrak{q}_{i'}=\mathfrak{r}_{i'j'}\cap B$

$\Rightarrow \mathfrak{r}_{ij}\neq\mathfrak{r}_{i'j'}$.

qed

6.3 Decomposition group

From now until §6.5 we assume in addition that L/K is galois with Galois group Γ.

Lemma 6.3.1: For any prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and any ideal $\mathfrak{a}$ of a ring we have

$$\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i \quad \Longleftrightarrow \quad \exists\, i \colon \mathfrak{a} \subset \mathfrak{p}_i.$$

Proof: "$\Leftarrow$" clear. For "$\Rightarrow$" we prove: If $\forall i: \mathfrak{a} \not\subset \mathfrak{p}_i$ then $\mathfrak{a} \not\subset \bigcup_i \mathfrak{p}_i$.

$n = 0$: $\mathfrak{a} \not\subset \emptyset$ ✓.

$n = 1$ clear.

$n-1 \rightsquigarrow n \geq 2$: Can assume $\forall j: \mathfrak{a} \not\subset \bigcup_{i \neq j} \mathfrak{p}_i$.

$\rightsquigarrow$ Select $a_j \in \mathfrak{a} \setminus \bigcup_{i\neq j} \mathfrak{p}_i$.

If some $a_j \notin \mathfrak{p}_j$ then done. So can assume $a_j \in \mathfrak{p}_j \setminus \bigcup_{i \neq j} \mathfrak{p}_i$

Then $\forall k$: $\prod_{j \neq k} a_j \in \Big(\prod_{j\neq k} \mathfrak{p}_j\Big) \setminus \mathfrak{p}_k$. $\Big|$ $\Rightarrow \forall j \neq k: a_j \notin \mathfrak{p}_k$.

$\Rightarrow \forall i$: $\underbrace{\sum_k \Big(\prod_{j\neq k} a_j\Big)}$ $\notin \mathfrak{p}_i$ $\Rightarrow$

$\Rightarrow$ $\in \mathfrak{a} \setminus \bigcup_i \mathfrak{p}_i$ done.

qed.

$$\begin{array}{ccccc} \Gamma \circlearrowright L & \supset & B & \supset & \mathfrak{q} \\ | & & | & & | \\ K & \supset & A & \supset & \mathfrak{p} \end{array}$$

Theorem 6.3.2: (a) The group Γ acts on B and on the set of prime ideals of B.

(b) The group Γ acts transitively on the set of prime ideals $\mathfrak{q} \subset B$ above $\mathfrak{p}$.

Proof: (a) ✓ (b) $\quad \forall \gamma \in \Gamma \quad \mathfrak{q} \cap A = {}^{\gamma}\mathfrak{q} \cap A$

Take $\mathfrak{q}, \mathfrak{q}' \subset B$ above $\mathfrak{p}$.

$$\forall y \in \mathfrak{q}' : \underbrace{Nm_{L/K}(y)}_{\in A} = \underbrace{\prod_{\gamma \in \Gamma}}{}^{\gamma}y = \Big(\prod_{\gamma \neq 1} {}^{\gamma}y\Big) \cdot y \in \mathfrak{q}' \cap A = \mathfrak{p} \subset \mathfrak{q}$$

$\Rightarrow \exists \gamma : {}^{\gamma}y \in \mathfrak{q}$.

i.e. $y \in {}^{\gamma^{-1}}\mathfrak{q}$.

$$\Rightarrow \mathfrak{q}' \subset \bigcup_{\gamma \in \Gamma} {}^{\gamma^{-1}}\mathfrak{q} \overset{6.3.1}{\Longrightarrow} \exists \gamma \in \Gamma : \mathfrak{q}' \subset {}^{\gamma^{-1}}\mathfrak{q}.$$

$\Rightarrow \mathfrak{q}' = {}^{\gamma^{-1}}\mathfrak{q}$ $\qquad$ qed.

Definition 6.3.3: The stabilizer of $\mathfrak{q}$ is called the *decomposition group of* $\mathfrak{q}$:

$$\Gamma_{\mathfrak{q}} := \{\gamma \in \Gamma \mid \forall x \in \mathfrak{q}\colon {}^{\gamma}x \in \mathfrak{q}\}.$$

Proposition 6.3.4:

(a) The numbers $e := e_{\mathfrak{q}|\mathfrak{p}}$ and $f := f_{\mathfrak{q}|\mathfrak{p}}$ depend only on $\mathfrak{p}$.

(b) We have $\mathfrak{p}B = \prod_{[\gamma]\in\Gamma/\Gamma_{\mathfrak{q}}} {}^{\gamma}\mathfrak{q}^{e}$.

(c) We have $n = r \cdot e \cdot f$.

(d) For any $\gamma \in \Gamma$ we have $\Gamma_{\gamma\mathfrak{q}} = {}^{\gamma}\Gamma_{\mathfrak{q}}$.

Also: $r = [\Gamma : \Gamma_{\mathfrak{q}}]$

$ef = |\Gamma_{\mathfrak{q}}|$.

Pf: $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i} = \prod_{[\gamma]\in\Gamma/\Gamma_{\mathfrak{q}}} {}^{\gamma}\mathfrak{q}^{e_1}$

$\mathfrak{q} = \mathfrak{q}_1$,

$\forall \gamma \in \Gamma$: $\left.\begin{array}{l} B \xrightarrow{\sim} B \\ \mathfrak{q} \xrightarrow{\sim} {}^{\gamma}\mathfrak{q} \end{array}\right\} \Rightarrow B/\mathfrak{q} \xrightarrow{\sim} B/{}^{\gamma}\mathfrak{q}$

$n = \sum_{i=1}^{r} e_i f_i = r \cdot e_1 \cdot f_1 = ref$.

qed

Proposition 6.3.5:

(a) We have $\Gamma_{\mathfrak{q}} = 1$ if and only if $\mathfrak{p}$ is totally split in B.

(b) We have $\Gamma_{\mathfrak{q}} = \Gamma$ if and only if there is a unique prime $\mathfrak{q} \subset B$ above $\mathfrak{p}$.

Pf (a) $\Gamma_{\mathfrak{q}} = 1 \iff r = n \iff \mathfrak{p}B = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ with distinct $\mathfrak{q}_i$.

(b) $\Gamma_{\mathfrak{q}} = \Gamma \iff \mathfrak{p}B = \mathfrak{q}^e$ for $\mathfrak{q}$ prime. $\quad n = ef$.

$\iff r = 1 \iff$

qed.

Proposition 6.3.6: Set $L' := L^{\Gamma_{\mathfrak{q}}}$ and $B' := B \cap L'$ and $\mathfrak{q}' := \mathfrak{q} \cap B'$.

(a) Then $\mathfrak{q}$ is the unique prime of B above $\mathfrak{q}'$ and $\mathfrak{q}'B = \mathfrak{q}^e$.

(b) We have $e_{\mathfrak{q}|\mathfrak{q}'} = e$ and $f_{\mathfrak{q}|\mathfrak{q}'} = f$ and $e_{\mathfrak{q}'|\mathfrak{p}} = f_{\mathfrak{q}'|\mathfrak{p}} = 1$.