Thm 15.4.6

Let $\mathcal{G}$ be an algebraic group defined over K (e.g. $\mathcal{G} = GL_n, SL_n, \dots$).

Let $\mathcal{V}$ be a variety defined over K (e.g. $\mathcal{V} = \mathbb{A}^n, \dots$).

Consider an algebraic action of $\mathcal{G}$ on $\mathcal{V}$ defined over K.

Consider the $\mathcal{G}(K)$-orbits in $\mathcal{V}(K)$. Fix one such orbit $\mathcal{G}(K)v_0$.

Assuming that $H^1(L|K, \mathcal{G}(L)) = \{*\}$, we have a bijection

$$H^1(L|K, \mathrm{Stab}_{\mathcal{G}(L)}(v_0)) \longleftrightarrow \{\mathcal{G}(K)\text{-orbits in } \mathcal{V}(K) \text{ contained in the } \mathcal{G}(L)\text{-orbit } \mathcal{G}(L)v_0\}$$

$$\{\dots\} = \mathcal{G}(K) \backslash (\mathcal{G}(L)v_0 \cap \mathcal{V}(K))$$

$$(\sigma \mapsto g^{-1}\sigma(g)) \longleftarrow\!\shortmid \quad \mathcal{G}(K)gv_0 \text{ with } g \in \mathcal{G}(L)$$

If the 1-cocycle φ corresponds to the orbit $\mathcal{G}(K)v$, then $\mathrm{Stab}_{\mathrm{Stab}_{\mathcal{G}(L)}(v_0)}(\varphi) \cong \mathrm{Stab}_{\mathcal{G}(K)}(v)$.

Pf 1) Every 1-cocycle $\varphi: \mathrm{Gal}(L|K) \to \mathrm{Stab}_{\mathcal{G}(L)}(v_0)$ is of the form $(\sigma \mapsto g^{-1}\sigma(g))$ for $g \in \mathcal{G}(L)$ because it is a 1-cocycle $\varphi: \mathrm{Gal}(L|K) \to \mathcal{G}(L)$ and $H^1(L|K, \mathcal{G}(L)) = \{*\}$.

2) If $gv_0 \in \mathcal{V}(K)$, then $\underbrace{\sigma(gv_0)}_{=\sigma(g)v_0} = gv_0 \ \forall \sigma \in G$, so $g^{-1}\sigma(g) \in \mathrm{Stab}(v_0) \ \forall \sigma \in G$.

~~3) If $h g_1 v_0 = g_2 v_0$ with $h \in \mathcal{G}(K)$, $g_1, g_2 \in \mathcal{G}(L)$, then~~

Let $S = \mathrm{Stab}_{\mathcal{G}(L)}(v_0)$.

3) $\mathcal{G}(K)\, g_1 v_0 = \mathcal{G}(K)\, g_2 v_0$

$\Leftrightarrow \mathcal{G}(K)\, g_1 S = \mathcal{G}(K)\, g_2 S$

$\Leftrightarrow \exists\, h \in \mathcal{G}(K),\ s \in S : \ g_2 = h g_1 s$

$\Leftrightarrow \exists\, s \in S : \ g_2 s^{-1} g_1^{-1} \in \mathcal{G}(K)$

$\Leftrightarrow \exists\, s \in S : \forall \sigma \in G : \ g_2 s^{-1} g_1^{-1} = \sigma(g_2 s^{-1} g_1^{-1})$

$$\Updownarrow$$

$$s^{-1} g_1^{-1} \sigma(g_1) \sigma(s) = g_2^{-1} \sigma(g_2)$$

$\Leftrightarrow$ The 1-cocycles $(\sigma \mapsto g_1^{-1}\sigma(g_1))$ and $(\sigma \mapsto g_2^{-1}\sigma(g_2))$ lie in the same S-orbit.

4) ...

$\square$

<u>Exe</u> $\mathcal{G} = GL_2$, V = binary cubic forms,

$v_0 = -X^2Y + XY^2$ cubic form with roots $[0:1], [1:0], [1:1] \in \mathbb{P}^1(K)$

By Rmk 15.3.5, $\mathrm{Stab}_{GL_2(K)}(v_0) = \mathrm{Stab}_{GL_2(\bar{K})}(v_0) \cong S_3$.

$\Rightarrow$ trivial action of $\mathrm{Gal}(K^{sep}|K)$

By Cor 15.3.3, the $GL_2(K^{sep})$-orbit is $\{f \in V(K^{sep}) \mid \mathrm{disc}(f) \neq 0\}$.

$\Rightarrow$ The Thm gives a bijection

$$S_3 \backslash \mathrm{Hom}(\Gamma_K, S_3) \longleftrightarrow GL_2(K) \backslash \{f \in V(K) \mid \mathrm{disc}(f) \neq 0\}.$$

Thm 12.2 $\Updownarrow$ $\swarrow$ Thm 15.2.7

$\{$étale deg. 3 ext. of $K\}/\cong$

Ex (Kummer theory)

Let K be a field with $\mathrm{char}(K) \nmid n$ and which contains the n-th roots of unity.

$\mathcal{G} = GL_1 = \mathbb{G}_m \rightsquigarrow \mathcal{G}(L) = L^\times$

$V = \mathbb{A}^1$

Define the action of $\mathcal{G}$ on V by $x \cdot y = x^n y$

$v_0 = 1$

$$\mathrm{Stab}_{\mathcal{G}(K^{sep})}(v_0) = \mathrm{Stab}_{\mathcal{G}(K)}(v_0) = \langle \zeta_n \rangle \cong C_n \quad \text{(cyclic group of order } n\text{)}$$

$\Rightarrow$ triv action

$$\mathcal{G}(K^{sep})\, v_0 = (K^{sep})^{\times n} = (K^{sep})^\times$$

$\Rightarrow$ The Thm gives a bijection

$$\underset{\substack{\text{conjugation}\\ \text{is trivial}\\ \text{because}\\ C_n \text{ is abelian}}}{\cancel{C_n} \backslash} \mathrm{Hom}(\Gamma_K, C_n) \longleftrightarrow \underset{\text{the } x.y = x^n y\text{-action}}{K^\times \backslash} K^\times = \underset{\text{usual action}}{K^{\times n} \backslash} K^\times .$$

15.5. Counting cubic number fields

~~Goal: Thm 15.5.1 $N(T) = \Sigma$~~

~~Overview:~~

~~1. construct fund. dom. for $GL_2(\mathbb{Z}) \circlearrowright$~~

[The goal of this section:]

Thm 15.5.1 For $T \to \infty$,

$$N(T) := \sum_{\substack{L \text{ cubic n.f. up to } \cong \\ |\mathrm{disc}(L)| \le T}} \frac{1}{\#\mathrm{Aut}(L)} \sim \frac{1}{3\zeta(3)} \cdot T.$$

Rmk 15.5.2

~~$\#\mathrm{Aut}(L) = 1$ for 100% of L (ordered~~

a) $\mathrm{Aut}(L) = \begin{cases} C_3 & \text{if } L \text{ is a Galois ext. (with grp } C_3\text{) of } \mathbb{Q} \\ 1 & \text{otherwise} \end{cases}$

b) $$\sum_{\substack{L \text{ cubic n.f.} \\ |\mathrm{disc}(L)| \le T \\ \mathrm{Aut}(L) = C_3}} 1 \sim C \cdot T^{1/2}.$$

Rmk 15.5.3 $\displaystyle\sum_{\substack{L \text{ quadr. n.f.} \\ |\mathrm{disc}(L)| \le T}} \frac{1}{\#\mathrm{Aut}(L)} \sim \frac{1}{2\zeta(2)} \cdot T$, so $\displaystyle\sum_{\substack{L \text{ étale} \\ \mathbb{Q}\text{-alg.} \\ \text{of degree } 3 \\ |\mathrm{disc}(L)| \le T}} \frac{1}{\#\mathrm{Aut}(L)} \sim \left(\frac{1}{3\zeta(3)} + \frac{1}{2\zeta(2)}\right)$

Recall the bijection from Thm 15.2.7:

$$\{\text{cubic ext. } S \text{ of } \mathbb{Z}\}/\cong \;\longleftrightarrow\; GL_2(\mathbb{Z}) \backslash V(\mathbb{Z})$$

$$\mathrm{Aut}_{\mathbb{Z}}(S) \cong \mathrm{Stab}_{GL_2(\mathbb{Z})}(f)$$

$$\mathrm{disc}(S) = \mathrm{disc}(f)$$

Def $V^m(\mathbb{Z}) := \{ f \in V(\mathbb{Z})$ corr. to a cubic ext. S of $\mathbb{Z}$ which is ($\cong$ to) the ring of integers $\mathcal{O}_L$ of an étale $\mathbb{Q}$-alg. L of degree $3 \}$

$$V^i(\mathbb{Z}) := \{ f \in V(\mathbb{Z}) \text{ corr. to an integral domain } S \}$$

$$\underset{\substack{\uparrow \\ \text{Lemma 15.2.10}}}{=} \{ f \in V(\mathbb{Z}) \text{ irreducible over } \mathbb{Q} \}$$

$$V^{mi}(\mathbb{Z}) = V^m(\mathbb{Z}) \cap V^i(\mathbb{Z})$$

$= \{ f \in V(\mathbb{Z})$ corr. to a cubic ext. of S which is ($\cong$ to) the ring of integers $\mathcal{O}_L$ of a cubic number field$\}$.

Rmk 15.5.3 We have a bijection

$$\{\text{cubic number field } L\}/\cong \;\longleftrightarrow\; GL_2(\mathbb{Z}) \backslash V^{mi}(\mathbb{Z})$$

$$\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathrm{Stab}_{GL_2(\mathbb{Z})}(f)$$

$$\mathrm{disc}(L) = \mathrm{disc}(f)$$

Overview of the proof of the Thm:

Step 1: Construct a (nice) fund. dom. α_T for
$$GL_2(\mathbb{Z}) \circlearrowright \{ f \in V(\mathbb{R}) \mid 0 < |\mathrm{disc}(f)| \leq T \}.$$

Rmk 15.5.4
$$N(T) = \sum_{f \in V^{\mathrm{irr}}(\mathbb{Z})} \alpha_T(f)$$

Pf Cor of Lemma 5.1. $\square$

Step 2: Compute the "volume" $V \cdot T = \underbrace{\int_{V(\mathbb{R})} \alpha_T(f)\,df}$.

[proportional to T because $V(\mathbb{R}) = \mathbb{R}^4$ and $\mathrm{disc}(f)$ is a hom. deg. 4 pol. in a,b,c,d]

Def $V^{a\neq 0}(\mathbb{Z}) := \{ f = ax^3 + \ldots \in V(\mathbb{Z}) \mid a \neq 0 \}$

Rmk 15.5.5 $V^{i}(\mathbb{Z}) \subseteq V^{a\neq 0}(\mathbb{Z})$.

Step 3: Show that for any full lattice $\Lambda \subseteq V(\mathbb{Z})$,
$$\sum_{f \in V^{a \neq 0}(\mathbb{Z}) \cap \Lambda} \alpha_T(f) \underset{\Lambda}{\sim} \frac{V}{\mathrm{covol}(\Lambda)} \cdot T \text{ for } T \to \infty.$$

Step 4: Show that
$$\sum_{\substack{f \in V^{a\neq 0}(\mathbb{Z}) \\ f \notin V^{i}(\mathbb{Z})}} \alpha_T(f) = o(T) \text{ for } T \to \infty.$$

Def $V^m(\mathbb{Z}_p) := \{f \in V(\mathbb{Z}_p)$ corr. to a cubic ext. S of $\mathbb{Z}_p$ which is ($\cong$ to) the ring of integers of an étale $\mathbb{Q}_p$-algebra of degree $3\}$.

Rmk 15.5.6

$$V^m(\mathbb{Z}) = \{ f \in V(\mathbb{Z}) \mid f \in V(\mathbb{Z}_p) \ \forall p \}$$

Step 5: Show that $V^m(\mathbb{Z}_p) \subseteq V(\mathbb{Z}_p)$ is given by finitely many congruence conditions (mod powers of p) and compute $W_p := vol(V^m(\mathbb{Z}_p))$.

Step 6: Show that

$$\sum_{f \in V^{a\neq 0}(\mathbb{Z}) \cap V^m(\mathbb{Z})} \alpha_T(f) \sim \underbrace{\prod_p W_p}_{\frac{1}{3\zeta(3)}} \cdot V \cdot T \text{ for } T \to \infty$$

Pf (of Rmk 15.5.6)
Say $f \in V(\mathbb{Z})$ corr. to the ext. S of $\mathbb{Z}$ and L of $\mathbb{Q}$ and S_p of $\mathbb{Z}_p$ and L_p of $\mathbb{Q}_p$. Note that $disc(f) \neq 0$ implies that L is an étale $\mathbb{Q}$-algebra of degree 3.
$\Uparrow$
$f \in V(\mathbb{Z})$ or $f \in V^m(\mathbb{Z}_2)$

Any $\mathbb{Z}$-basis of S is also a $\mathbb{Z}_p$-basis of S_p.

Any $\mathbb{Z}$-basis of $\mathcal{O}_L$ is also a $\mathbb{Z}_p$-basis of L_p.
Let M be the linear map sending a $\mathbb{Z}$-basis of $\mathcal{O}_L$ to a $\mathbb{Z}$-basis of S.
The ring S is an integral ext. of $\mathbb{Z}$ because it is a finitely generated $\mathbb{Z}$-module. $\Rightarrow S \subseteq \mathcal{O}_L \Rightarrow M \in M_{3\times 3}(\mathbb{Z})$

Now, $S = \mathcal{O}_L \Leftrightarrow M \in GL_3(\mathbb{Z}) \Leftrightarrow \det(M) \in \mathbb{Z}^\times$

$S_p = \mathcal{O}_{L_p} \Leftrightarrow M \in GL_3(\mathbb{Z}_p) \Leftrightarrow \det(M) \in \mathbb{Z}_p^\times$.

$f \in V^m(\mathbb{Z})$
$\Updownarrow$
Hence, $S = \mathcal{O}_L \Leftrightarrow S_p = \mathcal{O}_{L_p} \ \forall p \Leftrightarrow f \in V^m(\mathbb{Z}_p) \ \forall p$. $\square$