Notes for the 8th talk in the seminar on Galois module theory

Alessandro Cobbe

1 K-groups

Here I follow the PhD thesis of Manuel Breuning.

Let A be a ring and $\mathcal{P}(A)$ the category of f.g. projective A-modules.

$K_0(A)$ is the Groethendieck group of $\mathcal{P}(A)$.

Generators: $\forall P \in \mathcal{P}(A)$, its isomorphism class (P).

Relations: $(P) - (P') - (P'')$ for each exact sequence $0 \to P' \to P \to P'' \to 0$.

Notation: $[P]$.

$K_1(A)$. Let us consider the category of pairs (P, f) with $P \in \mathcal{P}(A)$ and f automorphism of P. (Morphisms are defined in the obvious way.) The isomorphism classes are denoted by $((P, f))$.

Generators: $((P, f))$.

Relations: $((P, f)) - ((P', f')) - ((P'', f''))$ if $0 \to (P', f') \to (P, f) \to (P'', f'') \to 0$ exact and $((P, fg)) - ((P, f)) - ((P, g))$ for all $P \in \mathcal{P}(A)$ and automorphisms f, g of P.

Notation: $[P, f]$. Alternative description: Whitehead group. Define $\mathrm{GL}_n(A) \to \mathrm{GL}_{n+1}(A)$ by $M \mapsto \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$. Let $\mathrm{GL}(A) = \varinjlim \mathrm{GL}_n(A)$ and let $\mathrm{GL}(A)' = [\mathrm{GL}(A), \mathrm{GL}(A)]$ be the commutator subgroup. Then $K_1(A) \cong \mathrm{GL}(A)/\mathrm{GL}(A)'$. The isomorphism is obtained as follows: let $[P, f] \in K_1(A)$, let Q be such that $P \oplus Q = F$ is free, then $f \oplus \mathrm{id}$ is represented by a matrix $M \in \mathrm{GL}(A)$. For the proof that this is a well-defined map and an isomorphism, see [CR, Thm. 40.6].

$K_0(A, \varphi)$, where $\varphi : A \to B$ is a ring homomorphism. Category of triples (P, f, Q), where $P, Q \in \mathcal{P}(A)$ and $f : B \otimes_A P \to B \otimes_A Q$ is an isomorphism of B-modules. A morphism is a pair of morphisms $u : P \to P'$ and $v : Q \to Q'$ such that $f' \circ (\mathrm{id}_B \otimes u) = (\mathrm{id}_B \otimes v) \circ f$.

Generators: $((P, f, Q))$.

Relations: $((P, f, Q)) - ((P', f', Q')) - ((P'', f'', Q''))$ for each short exact sequence $0 \to ((P', f', Q')) \to ((P, f, Q)) \to ((P'', f'', Q'')) \to 0$ (i.e. $0 \to P' \to P \to P'' \to 0$ and $0 \to Q' \to Q \to Q'' \to 0$ both exact); $((P, gf, R)) - ((P, f, Q)) - ((Q, g, R))$ with $P, Q, R \in \mathcal{P}(A)$ and $f : B \otimes P \to B \otimes Q$, $g : B \otimes Q \to B \otimes R$ isomorphisms.

Notation: $[P, f, Q]$.

For any ring homomorphism $\varphi : A \to B$ there is an exact sequence

$$K_1(A) \xrightarrow{\varphi_*} K_1(B) \xrightarrow{\partial^1_{A,\varphi}} K_0(A, \varphi) \xrightarrow{\varphi^0_{A,\varphi}} K_0(A) \xrightarrow{\varphi_*} K_0(B).$$

Here $\varphi_*([P, f]) = [B \otimes_A P, \mathrm{id}_B \otimes f]$, $\partial^1_{A,\varphi}([M]) = [A^n, M, A^n]$ for $M \in \mathrm{GL}(B)$, $\partial^0_{A,\varphi}([P, f, Q]) = [P] - [Q]$, $\varphi_*([P]) = [B \otimes_A P]$.

2 Realizable classes

Let K be a number field and G a finite group. Denote by $R(\mathcal{O}_K[G])$ the set of those classes in $\mathrm{Cl}(\mathcal{O}_K[G])$ which are realizable as Galois-module classes of rings of integers $\mathcal{O}_L$ in tame G-Galois extensions L/K.

Conjecture 2.1 (McCulloh)**.** *$R(\mathcal{O}_K[G])$ is always a subgroup of $\mathrm{Cl}(\mathcal{O}_K[G])$.*

Let G be a direct product of n cyclic groups of order l and let C be a cyclic group of order $l^n - 1$. Then G is isomorphic to the additive group of the finite field F_{l^n}, C to its multiplicative group. Via these isomorphisms there is an action of C on G via multiplication.

For $\delta \in C$, let $t(\delta)$ denote the least non-negative residue $\pmod l$ of $\mathrm{Tr}(\delta)$, where $\mathrm{Tr} : F_{l^n} \to F_l$ is the trace. Let

$$\theta = \sum_{\delta \in C} t(\delta)\delta^{-1} \in \mathbb{Z}[C],$$

and

$$\mathcal{I} = \mathbb{Z}[C](\theta/l) \cap \mathbb{Z}[C]$$

be the Stickelberger ideal of $\mathbb{Z}[C]$.

Theorem 2.2 (McCulloh)**.** *If G is elementary abelian,*

$$R(\mathcal{O}_K[G]) = \mathrm{Cl}^0(\mathcal{O}_K[G])^{\mathcal{I}},$$

where $\mathrm{Cl}^0(\mathcal{O}_K[G])$ is the kernel of the map $\mathrm{Cl}(\mathcal{O}_K[G]) \to \mathrm{Cl}(\mathcal{O}_K)$ induced by the augmentation map $\mathcal{O}_K[G] \to \mathcal{O}_K$.

In 1987 McCulloh extended this result to abelian groups G, but we do not give a pricise formulation here.

Theorem 2.3 (Agboola-McCulloh)**.** *Suppose that G is of odd order, that $|G|$ is coprime to the class number of K and that K contains no non-trivial $|G|$-th roots of unity. Then $R(\mathcal{O}_K[G])$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_K[G])$.*

Note that they actually associate to number field extensions elements of $K_0(\mathcal{O}_K[G], K^c)$, where K^c is the algebraic closure of K.

3 Mayer-Vietoris sequence

Let

$$\begin{array}{ccc} A & \xrightarrow{f_1} & A_1 \\ \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle g_1} \\ A_2 & \xrightarrow{g_2} & \bar{A} \end{array}$$

be a fiber product of ring homomorphisms, which means

$$A \cong \{(a_1, a_2) \in A_1 \oplus A_2 : \ g_1(a_1) = g_2(a_2)\}.$$

Theorem 3.1 (Milnor)**.** *If g_1 or g_2 is surjective, then there is a Mayer-Vietoris sequence:*

$$\begin{aligned} K_1(A) &\xrightarrow{(f_1,f_2)} K_1(A_1) \times K_1(A_2) \xrightarrow{g_1 \times (1/g_2)} K_1(\bar{A}) \\ &\xrightarrow{\partial} K_0(A) \xrightarrow{(f_1,f_2)} K_0(A_1) \times K_0(A_2) \xrightarrow{g_1 - g_2} K_0(\bar{A}). \end{aligned}$$

Proof. See [CR, Thm. 42.13]. □

Our situation. Let K be a number field, G an elementary abelian group of order l^n, $\Sigma = \sum_{\delta \in G} \delta$.

$$\begin{array}{ccc} \mathcal{O}_K[G] & \xrightarrow{\phi} & \mathcal{O}_K[G]/\mathcal{O}_K\Sigma = \Gamma \\ \downarrow{\scriptstyle \varepsilon} & & \downarrow{\scriptstyle \bar{\varepsilon}} \\ \mathcal{O}_K & \xrightarrow{\bar{\phi}} & \overline{\mathcal{O}_k} = \mathcal{O}_K/l^n\mathcal{O}_K \end{array}$$

Let us extract a piece of the Mayer-Vietoris exact sequence

$$K_1(\Gamma) \times K_1(\mathcal{O}_K) \xrightarrow{\bar{\varepsilon} \times (1/\bar{\phi})} K_1(\overline{\mathcal{O}_K}) \xrightarrow{\partial} K_0(\mathcal{O}_K[G])$$

It can be shown that $K_1(\Gamma) \cong \Gamma^*$, $K_1(\mathcal{O}_K) \cong \mathcal{O}_K^*$ and $K_1(\overline{\mathcal{O}_K}) \cong \overline{\mathcal{O}_K}^*$ (see [CR, Thm. 40.31]). Main idea: Gauß elimination and the fact that elementary matrices are trivial in K^1-groups. It can also be shown that $\partial(\bar{s}) = [(s, \Sigma)]$, where $(s, \Sigma) = s\mathcal{O}_K[G] + \Sigma\mathcal{O}_K[G]$ is called a Swan-module and is locally free. All their classes generate the Swan-subgroup $T \subseteq \mathrm{Cl}(\mathcal{O}_K[G])$. We get

$$\Gamma^* \times \mathcal{O}_K^* \xrightarrow{\bar{\varepsilon} \times (1/\bar{\phi})} \overline{\mathcal{O}_K}^* \xrightarrow{\partial} T \to 0,$$

i.e.:

$$T \cong \overline{\mathcal{O}_K}^* / \mathcal{O}_{\mathrm{K}}^* \bar{\varepsilon}(\Gamma^*) \tag{1}$$

4 Swan modules and Hilbert-Speiser number fields

Here we follow the paper by [Greither, Replogle, Rubin, Srivastav].

Note that T is a $\mathbb{Z}[C]$-submodule of D, the subgroup of the class group consisting of those classes that become trivial under extension of scalars to the maximal order. Actually C acts trivially on T since $\delta \in C$ acts as an automorphism of G, so it maps $s\mathcal{O}_K[G]$ and $\mathcal{O}_K\Sigma$ to itself.

Proposition 4.1. *Assume G is elementary abelian of order $l^n > 2$, then $T^{l^{n-1}(l-1)/2} \subseteq R \cap D$.*

Proof.

$$\varepsilon(\theta) = \sum_{\delta \in C} t(\delta) = l^{n-1} \sum_{a=1}^{l-1} a = l^n(l-1)/2$$

and $N_C(\theta/l) = \varepsilon(\theta/l)N_C = l^{n-1}(l-1)/2N_C \in \mathcal{I}$. Then

$$\varepsilon(l^{n-1}\theta - N_C(\theta/l)) = l^n l^{n-1}(l-1)/2 - (l^{n-1}(l-1)/2)(l^n-1) = l^{n-1}(l-1)/2.$$

Note that $D \subseteq \mathrm{Cl}^0(\mathcal{O}_K[G])$, because the map induced by augmentation commutes with extension of scalars to the maximal order. Since C acts trivially on T, $T^{\mathcal{I}} = T^{\varepsilon(\mathcal{I})}$,

$$T^{l^{n-1}(l-1)/2} \subseteq T^{\mathcal{I}} \subseteq D^{\mathcal{I}} \subseteq \mathrm{Cl}^0(\mathcal{O}_K[G])^{\mathcal{I}} \cap D = R \cap D.$$

□

Lemma 4.2. *If $\gamma \in \Gamma^*$ then $\bar{\varepsilon}(\gamma)^{l^n-1} \in \mathrm{Im}(\mathcal{O}_K^*) \subseteq \mathcal{O}_K/l^n\mathcal{O}_K$.*

Proof. Let e be the identity of G, then

$$0 \to (\mathcal{O}_K\Sigma)^C \to (\mathcal{O}_K[G])^C \to \Gamma^C \to H^1(C, \mathcal{O}_K\Sigma)$$

$$0 \to \mathcal{O}_K\Sigma \to \mathcal{O}_K e \oplus \mathcal{O}_K\Sigma \to \Gamma^C \to \mathrm{Hom}(C, \mathcal{O}_K\Sigma) = 0$$

Hence $\phi : \mathcal{O}_K e \to \Gamma^C$ is an isomorphism (in the paper they claim that $\bar{\varepsilon}$ induces an isomorphism). Let $N : \Gamma^* \to (\Gamma^*)^C$ be the norm $N(\gamma) = \prod_{\delta \in C} \gamma^\delta$. Then

$$\bar{\varepsilon}(\gamma)^{l^n-1} = \bar{\varepsilon}(N(\gamma)) \subseteq \mathrm{Im}(\mathcal{O}_K^*).$$

□

Theorem 4.3. *There is a natural surjcetive map*

$$T \to V_{l^n}^{l^n-1} = ((\mathcal{O}_K/l^n\mathcal{O}_K)^*/\mathrm{Im}(\mathcal{O}_K^*))^{l^n-1}.$$

Proof. By (1), $T \cong \overline{\mathcal{O}_K}^*/\mathcal{O}_{\mathrm{K}}^*\bar{\varepsilon}(\Gamma^*) \cong V_{l^n}/(\bar{\varepsilon}(\Gamma^*)/\mathrm{Im}(\mathcal{O}_K^*))$. To conclude: raise to the power $l^n - 1$ and use the lemma. □

Definition 4.4. *A number field K is Hilbert-Speiser if each finite tame abelian extension N/K has a trivial Galois-module structure.*

Theorem 4.5 (Hilbert-Speiser)**.** *$\mathbb{Q}$ is a Hilbert-Speiser field.*

Proof. This is the tame case in Leopoldt's Theorem. □

Theorem 4.6 (Greither-Replogle-Rubin-Srivastav)**.** *$\mathbb{Q}$ is the only Hilbert-Speiser field.*

Proof. Strategy: for each $K \neq \mathbb{Q}$ one finds a prime l such that V_l is divisible by some prime q, which does not divide $l-1$. Then $V_l^{(l-1)^2/2}$ is non-trivial. By Theorem 4.3

$$T^{(l-1)/2} \to V_l^{(l-1)^2/2}$$

is surjective, so also $T^{(l-1)/2}$ must be non-trivial. But by Proposition 4.1

$$T^{(l-1)/2} \subseteq R \cap D.$$

Hence R is non-trivial. □