σ-GROUPS

BÉRANGER SEGUIN

Let p be a prime, let K be a field of characteristic p, and let $\Gamma_K := \mathrm{Gal}(K^{\mathrm{sep}}|K)$.

Definition 1. A *σ-group (over K)* is a topological group $\mathcal{G}$ equipped with a continuous group homomorphism $\sigma\colon \mathcal{G} \to \mathcal{G}$ and with a continuous action of Γ_K, such that:

- the actions of σ and of Γ_K commute, i.e., for any $\tau \in \Gamma_K$ and any $g \in \mathcal{G}$, we have $\tau.\sigma(g) = \sigma(\tau.g)$
- any $g \in \mathcal{G}$ which is fixed under σ is also invariant under the Γ_K-action.

A *morphism of σ-groups* is a continuous group homomorphism which is σ-equivariant and Γ_K-equivariant. An *exact sequence of σ-groups* is an exact sequence of groups in which all maps are morphisms of σ-groups. A *σ-subgroup* is a closed subgroup which is both Γ_K-invariant and σ-invariant.

Definition 2. The σ-group $\mathcal{G}$ is *parametrizing* if the pointed sets $H^1(\langle\sigma^d\rangle, \mathcal{G})$ for any $d \geq 1$ and $H^1(\Gamma, \mathcal{G})$ for any closed subgroup $\Gamma \subseteq \Gamma_K$ (in non-abelian continuous group cohomology) are all trivial.

Definition 3. If $\mathcal{G}$ is a σ-group over K, we define:

- For any separable extension $L|K$, we let $\mathcal{G}(L)$ be the subgroup of $\mathcal{G}$ consisting of elements which are invariant under $\mathrm{Gal}(K^{\mathrm{sep}}|L) \subseteq \Gamma_K$.
- For any $d \geq 1$, we let $\mathcal{G}(\mathbb{F}_{p^d})$ be the subgroup of $\mathcal{G}$ consisting of elements which are invariant under σ^d, and we let $\mathcal{G}(\overline{\mathbb{F}}_p) := \bigcup_{d\geq 1} \mathcal{G}(\mathbb{F}_{p^d})$.

Moreover, if $g \in \mathcal{G}$, we define the *field of definition of g*, denoted by $K(g)$, as being the subfield of K^{sep} fixed under $\mathrm{Stab}_{\Gamma_K}(g)$.

Note that if we have a short exact sequence of σ-groups $1 \to \mathcal{A} \to \mathcal{B} \to \mathcal{C} \to 1$, and if $\mathcal{A}$ is parametrizing, then taking invariants yields short exact sequences of groups $1 \to \mathcal{A}(L) \to \mathcal{B}(L) \to \mathcal{C}(L) \to 1$ for any separable extension $L|K$ (as $H^1(\Gamma_L, \mathcal{A}) = \{1\}$) and $1 \to \mathcal{A}(\mathbb{F}_{p^d}) \to \mathcal{B}(\mathbb{F}_{p^d}) \to \mathcal{C}(\mathbb{F}_{p^d}) \to 1$ (as $H^1(\langle\sigma^d\rangle, \mathcal{A}) = \{1\}$).

Lemma 4. *The condition that $H^1(\langle\sigma^d\rangle, \mathcal{G})$ be trivial is equivalent to the surjectivity of the* multiplicative Artin–Schreier map $\wp_d\colon \mathcal{G} \to \mathcal{G}$, $g \mapsto \sigma^d(g)g^{-1}$.

Proof. A 1-cochain $f\colon \langle\sigma^d\rangle \to \mathcal{G}$ is determined by the element $x := f(\sigma^d) \in \mathcal{G}$, namely we have $f(\sigma^{kd}) = \sigma^{(k-1)d}(x)\sigma^{(k-2)d}(x)\cdots\sigma^d(x)x$, and the condition that this map be a coboundary amounts to the existence of an element $y \in \mathcal{G}$ such that $f(\sigma^k) = \sigma^{kd}(y)y^{-1}$, i.e., such that $\wp_d(y) = x$. □

Lemma 5. *Assume that $\wp_d\colon \mathcal{G} \to \mathcal{G}$ is surjective (i.e., that $H^1(\langle\sigma^d\rangle, \mathcal{G})$ is trivial). If $\mathcal{G}(\overline{\mathbb{F}}_p)$ is torsion, then $\wp_d\colon \mathcal{G}(\overline{\mathbb{F}}_p) \to \mathcal{G}(\overline{\mathbb{F}}_p)$ is surjective.*

Proof. Let $y \in \mathcal{G}(\overline{\mathbb{F}}_p)$, and fix $r \geq 1$ such that $\sigma^r(y) = y$. Pick $x \in \mathcal{G}$ such that $\wp_d(x) = y$, and let $y' = \sigma^{rd}(x)x^{-1}$. We have $y' = \sigma^{(r-1)d}(y)\sigma^{(r-2)d}(y)\cdots\sigma^d(y)y$, so $\sigma^r(y') = y'$. A simple induction on k shows that $\sigma^{krd}(x) = (y')^k x$ for all $k \geq 1$. Since $\mathcal{G}(\overline{\mathbb{F}}_p)$ is torsion, fix $k \geq 1$ such that $(y')^k = 1$, so $\sigma^{krd}(x) = x$, so $x \in \mathcal{G}(\overline{\mathbb{F}}_p)$. □

Definition 6. We denote by $\mathbb{G}_a$ the σ-group K^{sep} equipped with its absolute Frobenius $\sigma\colon x \mapsto x^p$ and its natural Γ_K-action. We say that a σ-group $\mathcal{G}$ is *unipotent* if there exists a sequence of surjective morphisms of σ-groups $\mathcal{G} = \mathcal{G}_1 \twoheadrightarrow \mathcal{G}_2 \twoheadrightarrow \ldots \twoheadrightarrow \mathcal{G}_r = 1$ such that the kernel of $\mathcal{G}_i \twoheadrightarrow \mathcal{G}_{i+1}$ is central in $\mathcal{G}_i$ and isomorphic to $\mathbb{G}_a$.

Lemma 7. *Assume that we have a short exact sequence $1 \to \mathcal{A} \to \mathcal{B} \to \mathcal{C} \to 1$ of σ-groups, with $\mathcal{A}$ and $\mathcal{C}$ parametrizing. Then, $\mathcal{B}$ is parametrizing.*

Proof. Letting Γ be either a closed subgroup of Γ_K or $\langle\sigma^d\rangle$ for some $d \geq 1$, we have the cohomological exact sequence $H^1(\Gamma, \mathcal{A}) \to H^1(\Gamma, \mathcal{B}) \to H^1(\Gamma, \mathcal{C})$ with both ends trivial, implying that $H^1(\Gamma, \mathcal{B})$ is trivial too. □

Proposition 8. *Any unipotent σ-group is parametrizing.*

Proof. By induction, using Lemma 7, the claim reduces to showing that $\mathbb{G}_a = K^{\mathrm{sep}}$ is parametrizing. The triviality of $H^1(\Gamma, K^{\mathrm{sep}})$ for any closed subgroup $\Gamma \subseteq \Gamma_K$ comes from [Ser62, Chap. X, §1, Prop. 1], and the triviality of $H^1(\langle\sigma^d\rangle, K^{\mathrm{sep}})$, which is equivalent to the surjectivity of $\wp_d\colon x \mapsto x^{p^d} - x$ by Lemma 4, comes from the fact that for any $y \in K^{\mathrm{sep}}$, the polynomial equation $x^{p^d} - x = y$ is separable and hence has a solution $x \in K^{\mathrm{sep}}$. □

Proposition 9. *Let $\mathcal{G}$ be a parametrizing σ-group, and let $B(\mathcal{G}(K))$ be the set of σ-conjugacy classes of $\mathcal{G}(K)$ (the σ-conjugacy action is defined by $g.m = \sigma(g)mg^{-1}$). Then, we have a bijection $H^1(\Gamma_K, \mathcal{G}(\mathbb{F}_p)) \simeq B(\mathcal{G}(K))$.*

Proof. Consider an element $[\rho] \in H^1(\Gamma_K, \mathcal{G}(\mathbb{F}_p))$. When seen as an element of $H^1(\Gamma_K, \mathcal{G})$, it is trivial, which means that there exists $\gamma \in \mathcal{G}$ such that $\rho(\tau) = \gamma^{-1}\tau(\gamma)$ for all $\tau \in \Gamma_K$ (uniquely defined up to left-multiplying by an element of $\mathcal{G}(K)$). The fact that ρ takes values in $\mathcal{G}(\mathbb{F}_p)$ implies that $\sigma(\gamma^{-1}\tau(\gamma)) = \gamma^{-1}\tau(\gamma)$, i.e., that $\sigma(\gamma)\gamma^{-1} = \tau(\sigma(\gamma)\gamma^{-1})$, i.e., that $\eta := \wp(\gamma) \in \mathcal{G}(K)$. Taking into account the impact of our choices (of the representative ρ and of the element τ) on the element η yields the map $H^1(\Gamma_K, \mathcal{G}(\mathbb{F}_p)) \to B(\mathcal{G}(K))$, $[\rho] \mapsto [\eta]$.

Conversely, if $\eta \in \mathcal{G}(K)$, then there is $\gamma \in \mathcal{G}$ such that $\eta = \wp(\gamma)$, and then $\tau \mapsto \gamma^{-1}\tau(\gamma)$ defines a continuous group homomorphism $\Gamma_K \to \mathcal{G}(\mathbb{F}_p)$. Taking into account the effect of σ-conjugating η or picking another $\wp$-preimage of η (i.e., right-multiplying γ by an element of $\mathcal{G}(\mathbb{F}_p)$) yields the inverse map $B(\mathcal{G}(K)) \to H^1(\Gamma_K, \mathcal{G}(\mathbb{F}_p))$. □

Example 10. For any $n \geq 1$, and for any field K of characteristic p, the σ-group $\mathcal{G} := \mathrm{GL}_n(K^{\mathrm{sep}})$ equipped with its natural absolute Frobenius and Γ_K-action is parametrizing, with $\mathcal{G}(\mathbb{F}_p) = \mathrm{GL}_n(\mathbb{F}_p)$, $\mathcal{G}(K) = \mathrm{GL}_n(K)$, etc. (The same holds for the unit subgroup of any algebra of the form $R \otimes_{\mathbb{F}_p} K^{\mathrm{sep}}$, where R is an $\mathbb{F}_p$-algebra, cf. [Ser62, Chap. X, §10, Exercise 2].)

For any $n \geq 1$, letting $\mathcal{U}_n(F)$ denote the group of unipotent upper-triangular matrices of size $n \times n$ over a field F, then $\mathcal{G} := \mathcal{U}_n(K^{\mathrm{sep}})$ is a unipotent (hence parametrizing) σ-group with $\mathcal{G}(\mathbb{F}_p) = \mathcal{U}_n(\mathbb{F}_p)$, $\mathcal{G}(K) = \mathcal{U}_n(K)$, etc.

Assume that K is perfect. For any finite p-group G of nilpotency class $< p$ (e.g., abelian), corresponding to some finite Lie $\mathbb{Z}_p$-algebra $\mathfrak{g}$ via the Lazard correspondence, the σ-group $\mathcal{G} := (\mathfrak{g} \otimes W(K^{\mathrm{sep}}), \circ)$ equipped with its natural absolute Frobenius and Γ_K-action is unipotent with $\mathcal{G}(\mathbb{F}_p) = G$, $\mathcal{G}(K) = (\mathfrak{g} \otimes W(K), \circ)$, etc.[1]

Definition 11. A *valued σ-group* $(\mathcal{G}, v)$ is a σ-group $\mathcal{G}$ equipped with a valuation $v\colon \mathcal{G} \to \mathbb{Z} \cup \{+\infty\}$ such that $v(xy) \geq \min(v(x), v(y))$ with equality whenever $v(x) \neq v(y)$, $v(\sigma(x)) = pv(x)$, and $v(x) = +\infty \Leftrightarrow x = 1$. A morphism $f\colon \mathcal{G} \to \mathcal{G}'$ of valued σ-groups is a morphism of σ-groups such that for any $x \in \operatorname{im} f$, we have $v(x) = \max_{y \in f^{-1}(x)} v(y)$. In particular, $v(f(y)) \geq v(y)$ for all $y \in \mathcal{G}$, and if f is injective this is an equality. If we have a fixed valuation on $K^{\mathrm{sep}} = \mathbb{G}_a$, a *unipotent valued σ-group* is a unipotent σ-group for which we can make sure that all the maps in the short exact sequences $1 \to \mathbb{G}_a \to \mathcal{G}_i \to \mathcal{G}_{i+1} \to 1$ are morphisms of valued σ-groups.

If $(\mathcal{G}, v)$ is a valued σ-group, we let $\mathcal{G}(\mathcal{O})$ be the subgroup of elements with $v(x) \geq 0$. Note that $\wp(\mathcal{G}(\mathcal{O})) \subseteq \mathcal{G}(\mathcal{O})$, and $\wp^{-1}(\mathcal{G}(\mathcal{O})) \subseteq \mathcal{G}(\mathcal{O})$. More precisely, $v(\wp(x)) = v(x)$ if $v(x) > 0$, $v(\wp(x)) \geq 0$ if $v(x) = 0$, and $v(\wp(x)) = p \cdot v(x)$ if $v(x) < 0$.

References

[Hug51] N. J. S. Hughes. The use of bilinear mappings in the classification of groups of class 2. *Proceedings of the American Mathematical Society*, 2:742–747, 1951. doi:10.2307/2032075.

[Ser62] Jean-Pierre Serre. *Corps Locaux*. Hermann, Paris, 1962.

[1]In nilpotency class 2, this is possible even in characteristic 2 by tensoring the ($\mathbb{Z}_p$-bilinear, alternating, surjective, nondegenerate) commutator bracket $G/Z(G)^2 \to [G, G]$ with $W(K)$, and using the result of [Hug51]. However, it seems impossible for D_{16} (nilpotency class 3) in characteristic 2, cf. https://mathoverflow.net/q/498286.