Cyclic Extensions of Fields and SO_2

Connor Lane

August 2024

1 Introduction

Let k be a characteristic field (characteristic $\neq 2$) and $C : x^2 - \alpha y^2 = 1$ with $\alpha \in k$ be an algebraic variety with distinguished point $O = (1, 0)$. We can put a group law on C with identity O as follows. Define a symmetric bilinear form $\omega : k^2 \times k^2 \to k$ by

$$\omega\left(\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}, \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}\right) = v_1 w_1 + \alpha v_2 w_2$$

Let K/k be an extension of k, and define $\mathrm{O}_2(\omega, K)$ as the set of 2×2 matrices with entries in K that preserve ω. Define $SO_2(\omega, K)$ as the kernel of $\det : \mathrm{O}_2(\omega, K) \to \{\pm 1\}$. Note that we can then view $\mathrm{SO}_2(\omega)$ (and $\mathrm{O}_2(\omega)$) as group varieties over k. We define a map $\varphi : C \to \mathrm{SO}_2(\omega)$ by

$$\varphi(x, y) = \begin{pmatrix} x & \alpha y \\ y & x \end{pmatrix}$$

this map is an isomorphism of varieties and induces a group structure on C via the group structure on $\mathrm{SO}_2(\omega)$.

Because of this isomorphism, we will use $\mathrm{SO}_2(\omega)$ and C interchangeably. In particular, we will use C when it is convenient to have a group written additively.

We fix the following notation conventions for Galois cohomology: $H^i(K/k, A) = H^1(\mathrm{Gal}(K/k), A)$, $H^i(k, A) = H^i(\mathrm{Gal}(\bar{k}/k), A)$, and we use $\hat{H}^i$ to denote Tate's augmented cohomology groups.

Finally, I will remark that more elementary (read: no group cohomology) introductions to some of these ideas can be found in a blog post on my website and in these slides I made for the Rose-Hulman undergraduate math conference.

2 The group structure of SO_2

Our first goal is to understand the group structure of $\mathrm{SO}_2(\omega)$. To do this, we define a ring (variety) A_ω

$$A_\omega(K) = \left\{ \begin{pmatrix} x & \alpha y \\ y & x \end{pmatrix} : x, y \in K \right\}.$$

As a variety, A_ω is simply $\mathbb{A}^2_k$, however it has a different ring structure in general. For notational convenience, we define

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad J = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}.$$

As rings, we have a natural isomorphism

$$K[X]/(X^2 - \alpha) \simeq A_\omega(K) \qquad 1 \mapsto I, \quad X \mapsto J.$$

Lemma 1. *When α is not a square in K, we get an isomorphism $K[\sqrt{\alpha}] \simeq A_\omega(K)$. When α is a square, we get an isomorphism $K \oplus K \simeq A_\omega(K)$*

Proof. The case where α is not square follows from the definition of adjoining an element. The case where it is a square follows from Chinese remainder theorem. $\square$

This yields another intepretation of A_ω: it's a $k(\sqrt{\alpha})/k$-form of $k \oplus k$. (In general, by $k(\sqrt{\alpha})/k$-form of X we mean some object Y defined over k whose base change to $k(\sqrt{\alpha})$ is isomorphic to X.)

We have an exact sequence

$$1 \longrightarrow \mathrm{SO}_2(\omega, K) \longrightarrow A_\omega^\times(K) \xrightarrow{\det} K^\times$$

The image of the last map is precisely the subset of $K^\times$ that can be written as $x^2 - \alpha y^2$ for $x, y \in K$, so in particular it is surjective when K is algebraically closed.

When α is not a square in K, we get a natural action of $\mathbb{Z}/2\mathbb{Z}$ on $A_\omega(K)$ induced by the action of $\mathrm{Gal}(K(\sqrt{\alpha})/K)$ on $K(\sqrt{\alpha}) \simeq A_\omega(K)$. We wish to generalize this action to the case where α is a square. For the group $G = (e, \sigma)$, define

$$^\sigma(xI + yJ) = xI - yJ.$$

We note that this agrees with the action of the Galois group when α is not square. For $M \in A_\omega(K)$, we have $M + {}^\sigma M = \mathrm{Tr}(M)$ and $M^\sigma M = \det(M)$.

Lemma 2. *With all notation as previously established, $H^1(G, A_\omega^\times(K)) = 1$.*

Proof. When α is not a square, this is Hilbert's theorem 90 by 1 and the discussion proceeding this lemma.

Now assume α is a square. Let $f : G \to A_\omega^\times$ be a 1-cocycle, We wish to show that f is a 1-coboundary. By the definition of a cocycle, we have

$$f(e) = f(ee) = f(e)^e(f(e)) = f(e)^2$$

Since $A_\omega^\times(K)$ is a group, we obtain $f(e) = I$. Now

$$I = f(\sigma\sigma) = f(\sigma)^\sigma f(\sigma).$$

If we let $f(\sigma) = aI + bJ$, we get $I = (aI + bJ)(aI - bJ) = a^2 I - \alpha b^2 I$ so $a^2 - \alpha b^2 = 1$. Now define $t = f(e) + f(\sigma)$. Then for $g \in \{e, \sigma\}$

$$^g t = {}^g f(e) + {}^g f(g) = f(ge)f(g)^{-1} + f(gg)f(g)^{-1} = f(g)^{-1}t$$

when $t \in A_\omega^\times$, we obtain $f(g) = {}^g t t^{-1}$ so f is a coboundary. Now suppose t is not a unit. Then $\det(t) = 0$ so we obtain

$$\begin{aligned} 0 &= \det(f(e) + f(\sigma)) = \det(I + aI + bJ) = \det((1+a)I + bJ) \\ &= ((1+a)I + bJ)((1+a)I - bJ) = (1+a)^2 I - \alpha b^2 I = a^2 I - \alpha b^2 I + 2aI + I = 2aI + 2I \end{aligned}$$

therefore $a = -1$, which along with $a^2 - \alpha b^2 = 1$ implies $b = 0$.

This means we have only one possible cocycle that is not a coboundary (the one given by $f(e) = I$ and $f(\sigma) = -I$.) However, there are at least two coboundaries. This implies that all cocycles are coboundaries and $H^1(G, A_\omega^\times) = 1$. $\square$

Now we can establish a nice description of $\mathrm{SO}_2(\omega, k)$.

Theorem 1. *We have an exact sequence*

$$1 \longrightarrow K^\times \longrightarrow A_\omega^\times(K) \xrightarrow{[e]-[\sigma]} \mathrm{SO}_2(\omega, K) \longrightarrow 1$$

Proof. By periodicity and Lemma 2, we have $\hat{H}^{-1}(G, A_\omega^\times(K)) \simeq H^1(G, A_\omega^\times(K)) \simeq 1$, so the map $x \mapsto {}^e x - {}^\sigma x$ is a surjection from $A_\omega^\times(K)$ to $\ker(\det) = \mathrm{SO}_2(\omega, K)$. On the other hand, the kernel of $x \mapsto {}^e x - {}^\sigma x$ is precisely $(A_\omega^\times(K))^G = IK^\times$. $\square$

Corollary 1. *We have isomorphisms of abelian groups*

$$\mathrm{SO}_2(\omega, K) \simeq \begin{cases} K(\sqrt{\alpha})^\times / K^\times & \alpha \textit{ is not square} \\ K^\times & \alpha \textit{ is square} \end{cases}$$

Proof. Combine Lemma 1 and Theorem 1. $\square$

3 The Galois Module Structure of SO_2.

Let K/k be a Galois extension of fields. We wish to describe the structure of $A_\omega(K)$ as a ring with a $\mathrm{Gal}(K/k)$ action.

Lemma 3. *Let α be a square in k. Then the isomorphism*

$$A_\omega(K) \simeq K \oplus K$$

commutes with the Gal(K/k) action.

Proof. The isomorphism $A_\omega(K) \simeq K[X]/(X^2 - \alpha)$ commutes with the Galois action, so it remains to show that the isomorphism

$$K[X]/(X^2 - \alpha) \simeq K \oplus K$$

commutes with the Galois action. More explicitly, this isomorphism is given by the maps

$$K[X]/(X^2 - \alpha) \xrightarrow{\text{proj}} K[X]/(X - \sqrt{\alpha}) \oplus K[X]/(X + \sqrt{\alpha}) \xrightarrow{\mathrm{ev}_\alpha, \mathrm{ev}_{-\alpha}} K \oplus K$$

The first map is a quotient map and trivially commutes with the Galois action. For the second pair of maps, note that for $\sigma \in \mathrm{Gal}(K/k)$ we have $\mathrm{ev}_\alpha({}^\sigma X) = \mathrm{ev}_\alpha(X) = \alpha = {}^\sigma\alpha$. Similarly, for $x \in K$ we have $\mathrm{ev}_\alpha({}^\sigma x) = {}^\sigma x$. Since X and K generate $K[X]$, and the evaluation map commutes with the action on these elements, it must commute with the action on all of $K[X]$. $\square$

From this, we obtain the

Corollary 2. *If α is a square in k and K/k is a galois extension,* $\mathrm{SO}_2(\omega, K) \simeq K^\times$ *as Galois modules.*

Proof. By lemma 3, we obtain an isomorphism of Galois modules $A_\omega^\times(K) \simeq K^\times \oplus K^\times$. Then by theorem 1, we have an exact sequence of Galois modules

$$1 \longrightarrow K^\times \longrightarrow K^\times \oplus K^\times \xrightarrow{[e]-[\sigma]} \mathrm{SO}_2(\omega, K) \longrightarrow 1$$

The first map is the diagonal embedding, so $\mathrm{SO}_2(\omega, K) \simeq K^\times$ as Galois modules. $\square$

Our goal is to obtain an explicit description of $H^1(k, \mathrm{SO}_2(\omega, \bar{k}))$. For this, we need the following lemma.

Lemma 4. $H^1(k, A_\omega(\bar{k})) = 0$.

Proof. If α is square, this follows from 3. Otherwise, assume α is not a square. Let $K = k(\sqrt{\alpha})$, then by inflation-restriction, we have

$$0 \longrightarrow H^1(K/k, A_\omega^\times(K)) \longrightarrow H^1(k, A_\omega^\times(\bar{k})) \longrightarrow H^1(K, A_\omega^\times(\bar{K})) = 0$$

so we have isomorphisms between the first two cohomology groups. We are now reduced to computing $H^1(K/k, A_\omega(K))$, and to do this we want to understand the structure of $A_\omega(K)$ as a $\mathrm{Gal}(K/k)$ module.

We work with the representation $A_\omega(K) \simeq K[X]/(X^2 - \alpha)$. Let $aX + b \in K[X]/(X^2 - \alpha)$, and let $\sigma \in \mathrm{Gal}(K/k)$ be the nontrivial element. Then

$$\mathrm{ev}_{\sqrt{\alpha}}(\sigma(aX + b)) = \mathrm{ev}_{\sqrt{\alpha}}(\sigma(a)X + \sigma(b)) = \sigma(a)\sqrt{\alpha} + \sigma(b) = \sigma(a)\sigma(-\sqrt{\alpha}) + \sigma(b) = \sigma(\mathrm{ev}_{-\sqrt{\alpha}})(aX + b)$$

Writing $p \in K[X]/(X^2 - \alpha)$ as (p_+, p_-) where $p_\pm = \mathrm{ev}_{\pm\sqrt{\alpha}}(p)$, we have

$$\sigma(p_+, p_-) = (\sigma(p_-), \sigma(p_+))$$

This description yields an isomorphism of $\mathrm{Gal}(K/k)$ modules $A_\omega(K)^\times \simeq \mathrm{ind}_{\mathrm{Gal}(K/k)} K^\times$. Therefore $H^1(K/k, A_\omega(K)^\times) = 0$ and therefore $H^1(k, A_\omega(K)) = 0$. $\square$

With this, we can now compute the cohomology of $\mathrm{SO}_2(\omega, \bar{k})$. First, we introduce a

Definition 1. *The set represented by ω, written* $\mathrm{rep}\,\omega$, *is* $\{x^2 - \alpha y^2 : x, y \in k\} \cap k^\times$.

Theorem 2. $H^1(k, \mathrm{SO}_2(\omega, \bar{k})) = k^\times / \operatorname{rep}\omega$. *When α is a square in k, this group is trivial.*

Proof. We have the exact sequence

$$0 \longrightarrow \mathrm{SO}_2(\omega, \bar{k}) \longrightarrow A_\omega^\times(\bar{k}) \xrightarrow{\det} \bar{k}^\times \longrightarrow 0$$

Taking the long exact sequence in cohomology, we get by 3

$$A_\omega^\times(k) \xrightarrow{\det} k^\times \longrightarrow H^1(k, \mathrm{SO}_2(\omega, \bar{k})) \longrightarrow H^1(k, A_\omega^\times(\bar{k})) = 0$$

so $H^1(k, \mathrm{SO}_2(\omega, \bar{k})) = k^\times / \det(A_\omega^\times(k))$. But $\det(xI + yJ) = x^2 - \alpha y^2$ is an arbitrary element of $\operatorname{rep}\omega$, so we obtain the isomorphism.

When α is a square, we have $H^1(k, \mathrm{SO}_2(\omega, \bar{k})) = H^1(k, \bar{k}^\times) = 0$ by corollary 2 and theorem 90. □

Theorem 3. *Let n be an odd integer and k a field that contains the n-torsion of C. Then there is a canonical isomorphism*

$$\delta : C(k)/nC(k) \simeq \hom_{cts}(G_k, C[n])$$

Proof. Consider the Kummer exact sequence on C

$$0 \longrightarrow C[n] \longrightarrow C(\bar{k}) \xrightarrow{[n]} C(\bar{k}) \longrightarrow 0$$

Taking cohomology we obtain

$$C(k) \xrightarrow{[n]} C(k) \xrightarrow{\delta} H^1(k, C[n]) \longrightarrow H^1(k, C(\bar{k})) \xrightarrow{[n]} H^1(k, C(\bar{k}))$$

Since $H^1(k, C(\bar{k})) = H^1(k, \mathrm{SO}_2(\bar{k}))$ is 2-torsion by Theorem 2, $[n]$ is an isomorphism. This implies $H^1(k, C[n]) \to H^1(k, C(\bar{k}))$ is the zero map and therefore δ is a surjection. Exactness at $C(k)$ yields the isomorphism. □