Three Torsion in the Class Group of Certain Cyclic Cubic Extensions

Abtien Javanpeykar, Erick Knight, and Peter Stevenhagen

November 14, 2019

Contents

1 Introduction

The goal of this paper is to construct some new governing fields. Classically, governing fields were used to control the 4 and 8-torsion of quadratic fields of the form $F_p = \mathbb{Q}(\sqrt{Np})$ where N is a fixed integer, and p runs over primes in a congruence class mod 4. The basic idea of the theory is to play Kummer theory off of class field theory. There are explicit descriptions of $\mathrm{cl}(F_p)[2]$ and $\mathrm{cl}(F_p)/2$, as well as a usable description of $\mathrm{cl}(F_p)/4$ that let one compute the map from $\mathrm{cl}(F_p)[2] \to \mathrm{cl}(F_p)/2$ or $\mathrm{cl}(F_p)/4$ and then determine what the 4 or 8-torsion of $\mathrm{cl}(F_p)$ is.

This project started when two of the authors realized that the core idea, where one plays Kummer theory off of class field theory, should also work when one considers cyclic cubic extensions of $K = \mathbb{Q}(\zeta_3)$. In this case, we still have a rather quite explicit understanding of the class field theory of K and so there is hope. The initial goal (which has since been realized) is to show, using only the Cheboratev density theorm, that there are infinitely many number fields F with $\mathbb{Z}/9\mathbb{Z} \subset \mathrm{cl}(F)$. Having said that the goal is similar to the 2-power case, the theory for cyclic cubic extensions of K gets significantly more intricate than the theory for quadratic extensions of $\mathbb{Q}$.

To fix notation, F/K will be a cyclic cubic extension, and $\langle\sigma\rangle = \mathrm{Gal}(F/K)$. One has that $\mathrm{cl}(F)$ admits an action of σ. Additionally, $(\sigma^2 + \sigma + 1)[I] = [N(I)] = [(1)]$, as K is a PID. Thus, $\mathrm{cl}(F)$ is an $R_\sigma := \mathbb{Z}[\sigma]/\sigma^2 + \sigma + 1$-module. A point for clarity is in order here: abstractly, $R_\sigma \cong \mathcal{O}_K$, but we find it clearer to think of these rings as being distinct, as they serve very different purposes in the calculations. Since genus theory describes $\mathrm{cl}(F)[1-\sigma]$ and $\mathrm{cl}(F)/(1-\sigma)$, the hope is that we can control $\mathrm{cl}(F)[(1-\sigma)^2]$ or $\mathrm{cl}(F)[(1-\sigma)^3]$.

To make a setup along the lines of the quadratic case, we need to say a few things about the aritmatic of $\mathcal{O}_K$. There is a unique prime dividing 3, namely $\lambda = 1 - \zeta_3$, and this prime will play a key role in the setup of the fields. Every other prime ideal $\mathfrak{p}$ admits a unique generator π such that $\pi \equiv 1 \pmod{\lambda^2}$ (this convention is not quite the typical convention where π is chosen to be 2 $\pmod{\lambda^2}$, but since we will only worry about whether numbers are cubes modulo other numbers, this distinction is not relevant for us). The choice of whether $\pi \equiv 1$, 4, or 7 $\pmod{\lambda^3}$ will play the role of choosing whether $p \equiv 1$ or 3 $\pmod 4$ in the quadratic case. Additionally, one has that $\pi \equiv 1 \pmod{\lambda^3}$ (resp. 4 or 7) if and only if $N(\pi) \equiv 1 \pmod 9$ (resp. 7 or 4). Also of note with this setup is that $K(\sqrt[3]{\beta})$ is unramified at λ if and only if $\beta \equiv \pm 1 \pmod{\lambda^3}$, which highlights the role that this congruence condition plays.

With all that in mind, the goal now becomes the following: fix a congruence class $a \pmod{\lambda^3}$, and choose an element $\alpha \in \mathcal{O}_K$. Let $F_\pi = K(\sqrt[3]{\alpha\pi})$ for $\pi \equiv a \pmod{\lambda^3}$, and let $\langle\sigma_\pi\rangle = \mathrm{Gal}(F_\pi/K)$ (concretely, $\sigma_\pi(\sqrt[3]{\alpha\pi}) = \zeta_3\sqrt[3]{\alpha\pi}$). Then we want to describe $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^2]$ or $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^3]$ as a module over R_{σ_π}, based on splitting conditions of π in various fields. This paper will focus on some of the simplest cases, where $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)] = R_{\sigma_\pi}/(1-\sigma_\pi)$ and so the only question is how much $1-\sigma_\pi$-power torsion is there. Nevertheless, this case will still provide several intricacies.

The main cases we study are summarized in the following theorems.

Theorem 1.1. *Let $\alpha = \zeta_3$, and $\pi \equiv 1 \pmod{\lambda^3}$. Define $F_\pi = K(\sqrt[3]{\alpha\pi})$, and keep notation as above. Then one has the following:*

- *π splits in $K(\zeta_9, \sqrt[3]{3})$ if and only if* $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^2] \cong R_{\sigma_\pi}/(1-\sigma_\pi)^2$.
- *π splits in $K\left(\zeta_9, \sqrt[3]{3}, \sqrt[3]{\frac{1-\zeta_9^4}{1-\zeta_9}}\right)$ and $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) = 1$ implies that* $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^3] = R_{\sigma_\pi}/(1-\sigma_\pi)^3$.

Theorem 1.2. *Choose $\alpha \sim \lambda$ or λ^2. Define $F_\pi = K(\sqrt[3]{\alpha\lambda})$, and keep notation as above. Then one has the following:*

- *π splits in* $K\left(\zeta_9, \sqrt[3]{3}, \sqrt[3]{\frac{1-\zeta_9^4}{1-\zeta_9}}\right))$ *if and only if* $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^2] \cong R_{\sigma_\pi}/(1-\sigma_\pi)^2$.
- *π splits in* $K\left(\zeta_9, \sqrt[3]{3}, \sqrt[3]{\frac{1-\zeta_9^4}{1-\zeta_9}}\right)$ *and* $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) = 1$ *implies that* $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^3] = R_{\sigma_\pi}/(1-\sigma_\pi)^3$.

These two theorems are not enough to show that $\mathbb{Z}/9\mathbb{Z}$ occurs as a class group infinitely often: while calculations seem to suggest that $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) = 1$ should occur infintely often among the relevant conjugacy classes, we currently cannot prove that. However there is another source of examples that will get out from this difficulty.

Theorem 1.3. *Let $\alpha = 10$, and $\pi \equiv 1 \pmod{\lambda^3}$. Define $F_\pi = K(\sqrt[3]{\alpha\pi})$ and keep notation as above. Then one has the following:*

- *π splits in* $K(\sqrt[3]{2}, \sqrt[3]{5})$ *if and only if* $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^2] \cong R_{\sigma_\pi}/(1-\sigma_\pi)^2$.
- *π splits in* $K\left(\sqrt[3]{2}, \sqrt[3]{5}, \zeta_9, \sqrt[3]{\frac{\zeta_3\sqrt[3]{10}-2}{\sqrt[3]{10}-2}}\right)$ *if and only if* $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^3] = R_{\sigma_\pi}/(1-\sigma_\pi)^3$.

Theorem 1.4. *Let $\alpha = 20$, and $\pi \equiv 4 \pmod{\lambda^3}$. Define $F_\pi = K(\sqrt[3]{\alpha\pi})$ and keep notation as above. Then one has the following:*

- *π splits in* $K(\sqrt[3]{2}, \sqrt[3]{5})$ *if and only if* $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^2] \cong R_{\sigma_\pi}/(1-\sigma_\pi)^2$.
- $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^3] \neq R_{\sigma_\pi}/(1-\sigma_\pi)^3$ *for any π.*

Theorem 1.3 realizes the goal of showing that $\mathbb{Z}/9\mathbb{Z}$ occurs infintely often in the class groups of number fields. The key difference here is that in both of these cases, we know that $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) \neq 1$. This may seem counterproductive, but it turns out that it wasn't the vanishing of this cohomology group that was the issue but the fact that either could or couldnt vansh that was the issue. Additionally, one may view the second point of theorem 1.4 as the same as the second point of theorem 1.3: since ζ_9 is in that big field, it is impossible for a prime that is $4 \pmod{\lambda^3}$ to split in it!

2 Genus Theory

Here we will recall some results from genus theory in a form advantageous for our applications. In this section and this section only, F/K will be an arbitrary cyclic extension of number fields of degree d, with $\mathrm{Gal}(F/K) = \langle\sigma\rangle$. The ultimate goal of genus theory is to determine what $\mathrm{cl}(F)[\sigma-1]$ is (or rather, determine as much information as you can in this very general setup). To fix some more notation, S will be the set of primes in K that are ramified in F, I_F will be the group of fractional ideals in F, and Prin_F will be the group of principal ideals in F.

There are short exact sequences of σ-modules:

$$0 \to \mathcal{O}_F^\times \to F^\times \to \mathrm{Prin}_F \to 0, \text{ and}$$

$$0 \to \mathrm{Prin}_F \to I_F \to \mathrm{cl}(F) \to 0.$$

Hilbert's satz 90 says that $H^1(\langle\sigma\rangle, F^\times) = 0$. Additionally, I_F is the direct sum of modules isomorphic to $\mathbb{Z}[\langle\sigma\rangle/H]$, which are all projective as $\mathbb{Z}[\langle\sigma\rangle]$-modules, so $H^1(\langle\sigma\rangle, I_F) = 0$. Consequently, taking cohomology gives the following long exact sequences:

$$0 \to \mathcal{O}_K^\times \to K^\times \to \mathrm{Prin}_F[\sigma-1] \to H^1(\langle\sigma\rangle, \mathcal{O}_F^\times) \to 0$$
$$0 \to H^1(\langle\sigma\rangle, \mathrm{Prin}_F) \to H^2(\langle\sigma\rangle, \mathcal{O}_F^\times) \to H^2(\langle\sigma\rangle, F^\times)$$
$$0 \to \mathrm{Prin}_F[\sigma-1] \to I_F[\sigma-1] \to \mathrm{cl}(F)[\sigma-1] \to H^1(\langle\sigma\rangle, \mathrm{Prin}_F) \to 0.$$

Letting N be the norm from F to K, one has that $H^2(\langle\sigma\rangle, \mathcal{O}_F^\times) = \mathcal{O}_K^\times/N(\mathcal{O}_F)$ and similarly for $H^2(\langle\sigma\rangle, F^\times)$. Thus, we can convert the second exact sequence to:

$$0 \to H^1(\langle\sigma\rangle, \mathrm{Prin}_F) \to H^2(\langle\sigma\rangle, \mathcal{O}_F^\times) \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap N(F^\times)) \to 0.$$

Since $K^\times/\mathcal{O}_K^\times = \mathrm{Prin}_K$, we get that $\mathrm{Prin}_F[\sigma-1]/\mathrm{Prin}_K = H^1(\langle\sigma\rangle, \mathcal{O}_F^\times)$. This gives the following exact sequence:

$$0 \to H^1(\langle\sigma\rangle, \mathcal{O}_F^\times) \to I_F[\sigma-1]/\mathrm{Prin}_K \to \mathrm{cl}(F)[\sigma-1] \to H^2(\langle\sigma\rangle, \mathcal{O}_F^\times) \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap N(F^\times)) \to 0.$$

There is another short exact sequence to compute $I_F[\sigma-1]/\mathrm{Prin}_K$:

$$0 \to \mathrm{cl}(K) \to I_F[\sigma-1]/\mathrm{Prin}_K \to I_F[\sigma-1]/I_K.$$

One clearly has that if $[I] \in I_F[\sigma-1]$, then $N(I) = I^d \in I_K$, and thus one gets that $I_F[\sigma-1]/I_K = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{(1/e_\mathfrak{p})\mathbb{Z}/\mathbb{Z}}$. Finally, a standard calculation in class field theory gives that $h_{2/1}(\mathcal{O}_F^\times) = (\prod_{v|\infty} e_v)/d$ and so putting it all together, one gets the "ambigious class number formula:"

$$\#(\mathrm{cl}(F)[\sigma-1]) = \frac{\#(\mathrm{cl}(K))\prod_v e_v}{d\#(\mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap N(F^\times))}.$$

Some remarks about how these exact sequences will be used. Since we will always be assuming that $K = \mathbb{Q}(\zeta_3)$, we will get to ignore all of the contributions that arise from $\mathrm{cl}(K)$. In these cases, the term $\#(\mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap N(F^\times)))$ is supposed to measure local obstructions to ζ_3 being a norm from F and its easy to show that this is non-zero when you expect it to be. Typically, we can easily construct enough unramified extensions in the cases that there are no local obstructions to ζ_3 being a norm to force $\mathrm{cl}(F)[\sigma-1]$ to be large enough to force $\#(\mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap N(F^\times))) = 1$.

Finally, while this doesn't technically lie in the realm of genus theory, we would be remiss to not explain the notion of Reidi matricies. Genus theory (hopefully) tells you what $\mathrm{cl}(F)[\sigma-1]$ is generated by. As above, you can typically construct enough unramified extensions of the right type, and this tells you what $\mathrm{cl}(F)/\sigma-1$ is. Thus, if you can compute what the map from $\mathrm{cl}(F)[\sigma-1] \to \mathrm{cl}(F)/\sigma-1$ is, then you can determine the structure of $\mathrm{cl}(F)[(\sigma-1)^2]$. This map is called the first Reidi map and we will be leveraging this concept throughout this paper.

3 The $\alpha \in \langle\zeta_3, \lambda\rangle$ cases

This section will be dedicated to studying fields of the form $F_\pi = K(\sqrt[3]{\alpha\pi})$ where α is a non cube in $\langle\zeta_3, \lambda\rangle$ and $\pi \equiv 1 \pmod{\lambda^3}$. For the rest of this section, α will be viewed as a fixed element so as to not cause a mess of notation. These fields are only ramified at λ and π, so one gets that the size of $\mathrm{cl}(K(\sqrt[3]{\alpha\pi})[\sigma_\pi - 1]$ is either 3 or 1 depending on whether ζ_3 is or isn't a norm from $F_\pi^\times$. However, the extension $F_\pi(\sqrt[3]{\pi}) = F_\pi(\sqrt[3]{\alpha})$ is unramified everywhere and invariant under the action of σ_π, so one must have that $\#(\mathrm{cl}(K(\sqrt[3]{\alpha\pi}))[\sigma_\pi - 1]) = 3$ and $\zeta_3 \in N_{F_\pi/K}(F_\pi^\times)$. Consequently, we must have that $\mathrm{cl}(F_\pi)_{\sigma_\pi - 1} = R_{\sigma_\pi}/(\sigma_\pi - 1)^d$ for some d.

Now looking at the long exact sequence above, this says that either $\mathrm{cl}(F_\pi)$ is generated by the primes that are ramified in F_π or $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) \neq 0$. Let $\mathfrak{p}_\pi$ and $\mathfrak{p}_\lambda$ be the primes dividing π and λ in F_π. Moreover, one has that $(\sqrt[3]{\alpha\pi})$ is a principal ideal, so one can write $[\mathfrak{p}_\pi]$ in terms of $[\mathfrak{p}_\lambda]$ in $\mathrm{cl}(F_\pi)$. Thus, we get that either $\mathfrak{p}_\lambda$ generates $\mathrm{cl}(F_\pi)[\sigma_\pi - 1]$ or $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) \neq 0$. Finally, since H^2 for a cyclic group is invariants mod norms, the statement $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) \neq 0$ is the same as $\zeta_3 \in N_{F_\pi/K}(\mathcal{O}_{F_\pi}^\times)$.

Now, let $E_\alpha = K(\sqrt[3]{\alpha})$, and $\langle\tau\rangle = \mathrm{Gal}(E_\alpha/K)$. Additionally, for $i \leq d$, let $F_{\pi,i}/F$ be the unramified extension of F_π whose Galois group is isomorphic to $\mathrm{cl}(F_\pi)/(\sigma_\pi)^i$. Then these fields fit into the following diagram:

$$
\begin{tikzcd}
 & & & \iddots \\
 & & F_{\pi,2} \arrow[dl, dash] \arrow[dd, dash] & \\
 & F_{\pi,1} \arrow[dl, dash] \arrow[dr, dash] & & \\
F_\pi \arrow[dr, dash, "\langle\sigma_\pi\rangle"'] & & E_\alpha \arrow[dl, dash, "\langle\tau\rangle"] & \\
 & K & &
\end{tikzcd}
$$

The prime over λ in E_α is given by $1 - \zeta_9$ if $\alpha = \zeta_3$ or ζ_3^2, $\sqrt[3]{\alpha}$ if $v_\lambda(\alpha) = 1$, and $\sqrt[3]{\alpha^2}/\lambda$ if $v_\lambda(\alpha) = 2$. In all cases, I will denote this element by β_λ.

3.1 Results conditional on $H^2 = 0$

In this section, we will make the following assumption:

Assumption 3.1. $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) = 0$.

Theorem 3.2. *Assume that $\alpha = \zeta_3$ or ζ_3^2 and that assumption 3.1 is true. Then one has the following:*

- *π splits in $K(\zeta_9, \sqrt[3]{3})$ if and only if* $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^2] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^2$.
- *π splits in $K\left(\zeta_9, \sqrt[3]{3}, \sqrt[3]{\frac{1-\zeta_9^4}{1-\zeta_9}}\right)$ if and only if* $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^3] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^3$.

Just to remark: the first condition is equivalent to the condition that $\pi \equiv 1 \pmod{\lambda^4}$.

Proof. Since $\mathrm{cl}(F_\pi)[\sigma_\pi - 1]$ is generated by $[\mathfrak{p}_\lambda]$, asking that $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^2] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^2$ is the same thing as asking that $\mathfrak{p}_\lambda$ splits in $F_{\pi,1}$. But $F_{\pi,1} = F_\pi[\sqrt[3]{\pi}]$, so this is equivalent to asking that λ splits in $K(\sqrt[3]{\pi})$. However, class field theory says that $\mathrm{Gal}(K(\sqrt[3]{\pi})/K) = (\mathcal{O}_K/\pi)^\times \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$, and so this is equivalent to λ being a cube modulo π. But since $\pi \equiv 1 \pmod{()\lambda^3}$, we know that ζ_3 is a cube modulo π. Moreover, $\lambda^2 = -\zeta_3^2 3$, so λ being a cube mod π is the same as 3 being a cube mod π and the first part follows.

Now, assume that π splits in $K(\zeta_9, \sqrt[3]{3})$. Then we have that $F_{\pi,2}/E_\alpha$ is a $(\mathbb{Z}/3\mathbb{Z})^2$-extension, ramified only at π, and Galois over K. Thus, there is a surjection from $V_\pi := (\mathcal{O}_{E_\alpha}/\pi)^\times \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$ onto $\mathrm{Gal}(F_{\pi,2}/E_\alpha)$. Now, $V_\pi = \mathbb{F}_3[\tau]/(\tau^3 - 1)$ as a $\mathbb{Z}[\langle\tau\rangle]$-module, so the only way that the kernel of this surjection has the right size and is $\langle\tau\rangle$-equivariant is if the kernel is $V_\pi[\tau - 1]$. Thus, we have that $\mathrm{Gal}(F_{\pi,2}/E_\alpha) = V_\pi/V_\pi[\tau - 1]$. Now, in order for the prime over λ to split in this field, we need only to check that its image in V_π lies in $V_\pi[\tau - 1]$. But the prime over $1 - \zeta_3$ in E_α is $1 - \zeta_9$, so we need only check that $\frac{1-\zeta_9^4}{1-\zeta_9}$ is a cube modulo π. But that is equivalent to π splitting in $K\left(\zeta_9, \sqrt[3]{3}, \sqrt[3]{\frac{1-\zeta_9^4}{1-\zeta_9}}\right)$.

$1-\zeta_9$ splitting in $F_{\pi,2}$ is equivalent to $\mathfrak{p}_\lambda$ splitting in $F_{\pi,2}$, which in turn is equivalent to $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^3] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^3$. Thus, we get the second part of the theorem. $\square$

Theorem 3.3. *Assume that α is not ζ_3 or ζ_3^2 and that assumption 3.1 is true. Then the following are equivalent:*

1. *π splits in $K(\zeta_9, \sqrt[3]{3})$,*
2. $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^2] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^2$*, and*
3. $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^3] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^3$.

Proof. Clearly, 3 implies 2. We thus need to show that 2 implies 1 and that 1 implies 3.

To that end, assume that $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^2] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^2$. We know that $\mathfrak{p}_\pi$ generates $\mathrm{cl}(F_\pi)[\sigma_\pi - 1]$. Thus, we must have that $\mathfrak{p}_\pi$ is trivial in $\mathrm{cl}(F_\pi)/(\sigma_\pi - 1)\mathrm{cl}(F_\pi)$. This means that $\mathfrak{p}_\pi$ splits in E_α. But we know that π splits in $K(\zeta_9)$, and $E_\alpha(\zeta_9) = K(\zeta_9, \sqrt[3]{3})$. Indeed, this argument is an if and only if, which will be useful in the next part.

Now, assume that π splits in $K(\zeta_9, \sqrt[3]{3})$. Then we have $F_{\pi,2}$ exists. Considerations similar to the ones above show that, if we let $V_\pi = (\mathcal{O}_{E_\alpha}/\pi)^\times \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$, then $\mathrm{Gal}(F_{\pi,2}/E_\alpha) = V_\pi/V_\pi[\tau - 1]$. To get $F_{\pi,3}$ to exist, we need that $\beta_\lambda \in V_\pi[\tau - 1]$. But $\tau(\beta_\lambda)/\beta_\lambda = \zeta_3$, which is a cube in $(\mathcal{O}_{E_\alpha}/\pi)^\times$

since π splits in $K(\zeta_9)$. Thus, we get that $F_{\pi,3}$ exists, or equivalently that $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^3] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^3$. $\square$

3.2 Unconditional Results

Now, we get to results that don't depend on assuming assumption 3.1.

Theorem 3.4. *The following are equivalent:*

- *π splits in $E_\alpha\left(\sqrt[3]{\left(\mathcal{O}_{E_\alpha}^\times\right)^{\tau-1}}\right)$, and*
- $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^2] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^2$.

Remark 3.5. It is a simple caluculation with cyclotomic units to show that, if $\alpha = \zeta_3$ or ζ_3^2, $E_\alpha\left(\sqrt[3]{\left(\mathcal{O}_{E_\alpha}^\times\right)^{\tau-1}}\right) = K(\zeta_3, \sqrt[3]{3})$. Additionally, it is also a fact that, in the other six cases, $E_\alpha\left(\sqrt[3]{\left(\mathcal{O}_{E_\alpha}^\times\right)^{\tau-1}}\right) = K\left(\zeta_9, \sqrt[3]{3}, \sqrt[3]{\frac{1-\zeta_9^4}{1-\zeta_9}}\right)$. However, as of yet, we are unable to come up with a proof of that fact that isn't just "sage says so" in some form.

This theorem also gives the following corollary that controls $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times)$ in some cases.

Corollary 3.6. *Assume that π splits in $K(\zeta_9, \sqrt[3]{3})$ but not $K\left(\zeta_9, \sqrt[3]{3}, \sqrt[3]{\frac{1-\zeta_9^4}{1-\zeta_9}}\right)$.*

- *If $\alpha = \zeta_3$ or ζ_3^2, then $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) = 0$.*
- *In the other six cases for α, one has that $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) \neq 0$.*

Proof of Corollary. In the first case, we have that $F_{\pi,2}$ exists by theorem 3.4. Because π doesn't split in $K\left(\zeta_9, \sqrt[3]{3}, \sqrt[3]{\frac{1-\zeta_9^4}{1-\zeta_9}}\right)$, we have that $\beta_\lambda \neq 0$ in $V_\pi/V_\pi[\tau - 1]$. Thus, we get that $\mathfrak{p}_\lambda$ doesn't split in $F_{\pi,2}$. But this means that $[\mathfrak{p}_\lambda] \neq 0$ in $\mathrm{cl}(F_\pi)$, which forces $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) = 0$.

In the second case, if $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) = 0$, we would have $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^2] \cong R_{\sigma_\pi}/(\sigma_\pi - 1)^2$. But that is equivalent to π splitting in $K\left(\zeta_9, \sqrt[3]{3}, \sqrt[3]{\frac{1-\zeta_9^4}{1-\zeta_9}}\right)$, which is a contradiction. Thus $H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) \neq 0$. $\square$

Proof of Theorem 3.4. Looking at the diagram above, we need to ask whether the field $F_{\pi,2}$ exists. It is an abelian extension of E_α, unramified outside of π, with $\mathrm{Gal}(F_{\pi,2}/E_\alpha) \cong (\mathbb{Z}/3\mathbb{Z})^2$. This implies that there is a surjection from V_π onto $\mathrm{Gal}(F_{\pi,2}/E_\alpha)$. Since $F_{\pi,2}/K$ is Galois, we must have that the kernel of this surjection is $\mathrm{Gal}(E_\alpha/K)$-stable.

If π does not split in E_α, then $\dim(V_\pi) = 1$, so there is no way for $F_{\pi,2}$ to exist. Thus, we will assume that π splits in E_α from now on. We then have as before that $V_\pi = \mathbb{F}_3[\tau]/(\tau^3 - 1)$ as an $\mathbb{F}_3$-vector space with an action of τ, and the only $\mathrm{Gal}(E_\alpha/K)$-stable subspace of dimension 1 is $V_\pi[\tau - 1]$. Class field theory says that the maximal abelian extension of E_α unramified outside of π with Galois group being entirely 3-torsion will have Galois group $V_\pi/\mathcal{O}_{E_\alpha}^\times$. Thus, for $F_{\pi,2}$ to exist, one must have $\mathcal{O}_{E_\alpha}^\times \subset V_\pi[\tau - 1]$, which is equivalent to π splitting in $E_\alpha\left(\sqrt[3]{\left(\mathcal{O}_{E_\alpha}^\times\right)^{\tau-1}}\right)$.

Conversely, if π splits in $E_\alpha\left(\sqrt[3]{\left(\mathcal{O}_{E_\alpha}^\times\right)^{\tau-1}}\right)$, then the above process can be reversed to construct the field $F_{\pi,2}$, showing that $\mathrm{cl}(F_\pi)[(\sigma_\pi - 1)^2] = R_{\sigma_\pi}/(\sigma_\pi - 1)^2$. □

4 The $\alpha = 10$ case

Before stating the main theorem of this section, we need some setup. We will let $\pi \in \mathcal{O}_K$ be a prime with $\pi \equiv 1 \pmod{\lambda^3}$. Additionally, we will let $F_\pi = K(\sqrt[3]{10\pi})$, $\langle\sigma_\pi\rangle = \mathrm{Gal}(F_\pi/K)$, $\mathfrak{p}_2 \subset \mathcal{O}_{F_\pi}$ be the prime dividing 2 (similarly for $\mathfrak{p}_5$ and $\mathfrak{p}_\pi$).

The exact sequence from genus theory gives

$$\langle[\mathfrak{p}_2], [\mathfrak{p}_5], [\mathfrak{p}_\pi]\rangle \to \mathrm{cl}(F_\pi)[1 - \sigma_\pi] \to H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times) \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap F_\pi^\times) \to 0.$$

Because ζ_3 isn't a norm locally at 2 or 5, one gets that $\#(\mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap F_\pi^\times)) = 3$, and hence $\#(H^2(\langle\sigma_\pi\rangle, \mathcal{O}_{F_\pi}^\times)) = 3$ and the map between them is an isomorphism. Consequently, one has that $\mathfrak{p}_2$, $\mathfrak{p}_5$, and $\mathfrak{p}_\pi$ generate $\mathrm{cl}(F_\pi)[1 - \sigma_\pi]$. However, $\mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_\pi = (\sqrt[3]{10\pi})$, we get that $\mathrm{cl}(F_\pi)[1 - \sigma_\pi]$ is generated by $\mathfrak{p}_2$ and $\mathfrak{p}_5$. The ambigious class number formula says that $\#(\mathrm{cl}(F_\pi)[1 - \sigma_\pi]) = 3$, so one has that $\mathrm{cl}(F_\pi)_{1-\sigma_\pi} = R_{\sigma_\pi}/(1 - \sigma_\pi)^d$ for some d.

Some important fields need to be named now. If $d \geq i$, let $F_{\pi,i}$ be the unramified abelian extension of F_π whose Galois group is $\mathrm{cl}(F_\pi)/(1 - \sigma_\pi)^i$. Since $d \geq 1$ always, one has that $F_{\pi,1}$ always exists, and indeed $F_{\pi,1} = F_\pi(\sqrt[3]{10}) = F_\pi(\sqrt[3]{\pi})$. Also, let $E = K(\sqrt[3]{10})$ and $\mathrm{Gal}(E/K) = \langle\tau\rangle$. It is a simple check that $\mathrm{cl}(E)[\tau - 1]$ is trivial, and so there are elements β_2 and β_5 such that $(\beta_2^3) = (2)$, $\beta_5^3 = (5)$, and $\beta_2\beta_5 = \sqrt[3]{10}$. These fields fit into the following incredibly reminiscent diagram:

$$\begin{tikzcd}
& & & \iddots \\
& & F_{\pi,2} \arrow[dl, dash] \arrow[dd, dash] & \\
& F_{\pi,1} \arrow[dl, dash] \arrow[dr, dash] & & \\
F_\pi \arrow[dr, dash, "\langle\sigma_\pi\rangle"'] & & E \arrow[dl, dash, "\langle\tau\rangle"] & \\
& K & &
\end{tikzcd}$$

The aim of this section is to prove the following theorem:

Theorem 4.1. *Keeping notation as above, one has the following:*

- $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^2] = R_{\sigma_\pi}/(1-\sigma_\pi)^2$ *if and only if* π *splits in* $K\left(\sqrt[3]{2}, \sqrt[3]{5}\right) = E\left(\sqrt[3]{\left(\mathcal{O}_E^\times\right)^{\tau-1}}\right)$.
- $\mathrm{cl}(F_\pi)[(1-\sigma_\pi)^3] = R_{\sigma_\pi}/(1-\sigma_\pi)^3$ *if and only if* π *splits in* $E\left(\sqrt[3]{\left(\mathcal{O}_E^\times\right)^{\tau-1}}, \sqrt[3]{\frac{\tau(\beta_2)}{\beta_2}}, \sqrt[3]{\frac{\tau(\beta_5)}{\beta_5}}\right)$.

A few remarks are in order. First off, part of the first part of Theorem 4.1 is that the two presentations of the field are equal. Secondly, one can check that one can choose $2-\sqrt[3]{10}$ for β_2 and hence $\sqrt[3]{10}/(2-\sqrt[3]{10})$ for β_5. Thirdly, it is of note that $\frac{\tau(\beta_2\beta_5)}{\beta_2\beta_5} = \frac{\tau(\sqrt[3]{10})}{\sqrt[3]{10}} = \zeta_3$, which shows that ζ_9 is in the field in the second part of the theorem. Finally, there is nothing special about 2 and 5, and all of the arguments work if you look at fields of the form $K(\sqrt[3]{\alpha\pi})$ where $\alpha \equiv 1 \pmod{\lambda^3}$, cubefree, and divisible by exactly two primes neither of which are equivalent to $1 \pmod{\lambda^3}$.

Proof. First, as noted, one has that $\mathrm{cl}(F_\pi)[1-\sigma_\pi]$ is generated by $\mathfrak{p}_2$ and $\mathfrak{p}_5$. Additionally, one has that $\mathrm{cl}(F_\pi)/(1-\sigma_\pi) \cong \mathrm{Gal}(F_{\pi,1}/F_\pi) \cong \mathrm{Gal}(K(\sqrt[3]{\pi})/K)$. Additionally, $\mathfrak{p}_2$ (or $\mathfrak{p}_5$) splits in $F_{\pi,1}$ if and only if 2 (respectively, 5) splits in $K(\sqrt[3]{\pi})$. That happens if and only if $\left(\frac{\pi}{2}\right)_3 = 1$ (resp. $\left(\frac{\pi}{5}\right)_3 = 1$), which by cubic reciprocity is equvalent to $\left(\frac{2}{\pi}\right)_3 = 1$ (resp. $\left(\frac{5}{\pi}\right)_3 = 1$). Thus, the natural map from $\mathrm{cl}(F_\pi)[1-\sigma_\pi] \to \mathrm{cl}(F_\pi)/(1-\sigma_\pi)$ is the zero map if and only if $\mathfrak{p}_2$ and $\mathfrak{p}_5$ split in $F_{\pi,1}$, which, as noted, is equivalent to π splitting in $K(\sqrt[3]{2}, \sqrt[3]{5})$.

Now, consider the extension $F_{\pi,2}/E$. If this extension exists, we know that its ramified only at π, has Galois group isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$, and is Galois over K. Letting $V_\pi = (\mathcal{O}_E/\pi)^\times \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$, one then has first off that $\dim_{\mathbb{F}_3}(V_\pi) = 3$, which is equivalent to π splitting in E. Additionally, as a $\mathbb{F}_3[\tau]$-module, V_π is a free rank one module, so $\mathrm{Gal}(F_{\pi,2}/E) \cong V_\pi/V_\pi[\tau - 1]$: class field theory provides a surjection from V_π onto $\mathrm{Gal}(F_{\pi,2}/E)$ and there is a unique τ-stable 1-dimensional subspace of V_π. However, one must also have $\mathcal{O}_E^\times$ in the kernel of the surjection, so the image of $\mathcal{O}_E^\times$ in V_π is contained in $V_\pi[\tau - 1]$. But that is equivalent to π splitting in $E\left(\sqrt[3]{(\mathcal{O}_E^\times)^{\tau-1}}\right)$.

Conversely, if π splits in $E\left(\sqrt[3]{(\mathcal{O}_E^\times)^{\tau-1}}\right)$, then one gets that there is an extension of E that is unramified outside of π, Galois over K, and whose Galois group is $(\mathbb{Z}/3\mathbb{Z})^2$. This extension is Galois over F_π of degree 9, and hence abelian, so one gets that $F_{\pi,2}$ exists and thus $\mathrm{cl}(F_\pi)[(1 - \sigma_\pi)^2] = R_\pi/(1 - \sigma_\pi)^2$.

This shows that the two fields $K\left(\sqrt[3]{2}, \sqrt[3]{5}\right)$ and $E\left(\sqrt[3]{(\mathcal{O}_E^\times)^{\tau-1}}\right)$ have the same primes in K that split in them, so they must be the same field. This concludes the proof of the first part of Theorem 4.1.

We will now assume that π splits in $E\left(\sqrt[3]{(\mathcal{O}_E^\times)^{\tau-1}}\right)$. Again, one is interested in whether the map from $\mathrm{cl}(F_\pi)[1 - \sigma_\pi] \to \mathrm{cl}(F_\pi)/(1 - \sigma_\pi)^2$ is the 0 map. This happens if and only if $\mathfrak{p}_2$ and $\mathfrak{p}_5$ split in $F_{\pi,2}$, which is equivalent to (β_2) and β_5 splitting in $F_{\pi,2}$. Now, $\mathrm{Gal}(F_{\pi,2}/E) = V_\pi/V_\pi[\tau - 1]$, so this is equivalent to β_2 and β_5 being in $V_\pi[\tau - 1]$, which is the same as $\frac{\tau(\beta_2)}{\beta_2}$ and $\frac{\tau(\beta_5)}{\beta_5}$ being cubes mod π, which is the same as π splitting in $E\left(\sqrt[3]{(\mathcal{O}_E^\times)^{\tau-1}}, \sqrt[3]{\frac{\tau(\beta_2)}{\beta_2}}, \sqrt[3]{\frac{\tau(\beta_5)}{\beta_5}}\right)$. This concludes the proof of the second part of Theorem 4.1.

$\square$

5 The $\alpha = 20$ case

Now, we will let $\pi \equiv 4 \pmod{\lambda^3}$. Let $F_\pi = K(\sqrt[3]{20\pi})$ and $\langle\sigma_\pi\rangle = \mathrm{Gal}(F_\pi/K)$. As in the previous section, one has that $\#(\mathrm{cl}(F_\pi)[1 - \sigma_\pi]) = 3$ and is generated by $\mathfrak{p}_2$, $\mathfrak{p}_5$, and $\mathfrak{p}_\pi$ with the relation $[\mathfrak{p}_2^2\mathfrak{p}_5\mathfrak{p}_\pi] = [(1)]$, and thus just generated by $\mathfrak{p}_2$ and $\mathfrak{p}_5$. Now, we have the following theorem:

Theorem 5.1. *Keeping notation as above, one has the following:*

- $\mathrm{cl}(F_\pi)[(1 - \sigma_\pi)^2] = R_{\sigma_\pi}/(1 - \sigma_\pi)^2$ *if and only if* π *splits in* $K(\sqrt[3]{2}, \sqrt[3]{5})$.
- $\mathrm{cl}(F_\pi)[(1 - \sigma_\pi)^3] = \mathrm{cl}(F_\pi)[(1 - \sigma_\pi)^2]$*; i.e. there is no primative* $(1 - \sigma_\pi)^3$*-torsion.*

Proof. The proof of the first part is similar to the proof of the first part in theorem 4.1. Since $\mathfrak{p}_2$ and $\mathfrak{p}_5$ generate $\mathrm{cl}(F_\pi)$ and $F_{\pi,1}$ is given by $F_\pi(\sqrt[3]{25\pi}) = F_\pi(\sqrt[3]{2\pi})$, we get that $\mathfrak{p}_2$ (resp. $\mathfrak{p}_5$) splits if and only if 25π (resp. 2π) is a cube mod 2 (resp. 5). But 25 is a cube mod 2 (resp. 2 is a cube mod 5), so this happens if and only if π is a cube mod 2 (resp. 5), which is equivalent to 2 (resp.

5) being a cube mod π by cubic reciprocity. Thus, $\mathfrak{p}_2$ and $\mathfrak{p}_5$ split in $F_{\pi,1}$ if and only if π splits in $K(\sqrt[3]{2}, \sqrt[3]{5})$.

As before, we assume that $F_{\pi,2}$ exists. In this case, one has that the extension $F_{\pi,2}/E$ is given by the same formula as in the proof of theorem 4.1. Thus, in order for $\mathfrak{p}_2$ to split in $F_{\pi,2}$, one needs that $\tau(\beta_2)/\beta_2$ to be a cube mod π. Similarly for $\mathfrak{p}_5$ to split, one needs that $\tau(\beta_5)/\beta_5$ to be a cube mod π. If both of them split, then you get that $\tau(\sqrt[3]{10})/\sqrt[3]{10} = \zeta_3$ is a cube mod π, which means that $\pi \equiv 1 \pmod{\lambda^3}$, a contradiction. Thus, we can't have $\mathfrak{p}_2$ and $\mathfrak{p}_5$ both splitting in $F_{\pi,2}$ and so there can be no primative $(1-\sigma_\pi)^3$-torsion. $\square$

A similar proof gives the following theorem:

Theorem 5.2. *Let π_1, π_2, and π_3 all be congruent to* $4 \pmod{\lambda^3}$, *$F = K(\sqrt[3]{\pi_1\pi_2\pi_3})$, and $\langle\sigma\rangle = \mathrm{Gal}(F/K)$. Then $\mathrm{cl}(F)_{1-\sigma} = R_\sigma/(1-\sigma)$ unless $\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_3}\right)_3 = \left(\frac{\pi_3}{\pi_1}\right)_3$, in which case one gets that $\mathrm{cl}(F)_{1-\sigma} = R_\sigma/(1-\sigma)^2$.*

This is not the most general theorem of this type that can be proven (and in particular, it does not imply theorem 5.1) but stating it when one allows all of the π_is to be 4 or 7 $\pmod{\lambda^3}$ is more hassle than is worth.

6 A few notes about fields over $\mathbb{Q}$

Finally, we will discuss some results about cyclic cubic fields over $\mathbb{Q}$. These results are somewhat similar in nature to those in section 3 although they are much weaker.

Let $p \in \mathbb{Z}$ be a prime such that $p \equiv 1 \pmod 3$. Then there are two fields $F_{p,i}/\mathbb{Q}$ such that $\mathrm{Gal}(F_{p,i}/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ and $F_{p,i}$ is ramified exactly at 3 and p. For most of the remainder of the section, these two fields will behave similarly and we will abuse notation and use F_p to stand in for one of them. As before, we will write σ_p as a generator of $\mathrm{Gal}(F_p/\mathbb{Q})$, and $R_p = \mathbb{Z}[\sigma_p]/(1+\sigma_p+\sigma_p^2)$. Since one again has that $\mathrm{cl}(F_p)[\sigma_p - 1] = R_p/(\sigma_p - 1)$, we are interested in how deep this goes. To that end, we have the following theorem:

Theorem 6.1. *One has that $\mathrm{cl}(F_p)[(\sigma_p-1)^2] \cong R_p/(\sigma_p-1)^2$ if and only if p splits in $\mathbb{Q}(\zeta_9, \sqrt[3]{3})$.*

Proof. The first step in this proof is to compute $H^2(\langle\sigma_p\rangle, \mathcal{O}_{F_p}^\times)$. As before, this is $(\mathcal{O}_{\mathbb{Q}}^\times/N_{F_p/\mathbb{Q}}(\mathcal{O}_{F_p}^\times)$, but unlike before, $\mathcal{O}_{\mathbb{Q}}^\times = \mathbb{Z}^\times = \{\pm 1\}$, so one has that $H^2(\langle\sigma_p\rangle, \mathcal{O}_{F_p}^\times) = 0$ for much simpler reasons. Thus, letting $\mathfrak{p}_3$ and $\mathfrak{p}_p$ denote the primes in F_p lying over 3 and p respectively, we have that $\langle[\mathfrak{p}_3], [\mathfrak{p}_p]\rangle = \mathrm{cl}(F_p)[\sigma_p - 1]$.

Now, there is an explicit description of the field that corresponds to $\mathrm{cl}(F_p)/(\sigma_p - 1)$: letting K_p be the cyclic cubic extension of $\mathbb{Q}$ ramified only at p and K_3 be the cyclic cubic extension ramified only at 3, we have that the compositum K_pK_3/F_p is the field that corresponds to $\mathrm{cl}(F_p)/(\sigma_p - 1)$. Additionally, asking whether $\mathfrak{p}_3$ splits in K_pK_3 is the same thing as asking whether 3 splits in K_p, which is equivalent to 3 being a cube modulo p. Similarly, asking whether $\mathfrak{p}_p$ splits in K_pK_3 is the same thing as asking whether p splits in K_3, which is the same thing as asking that $p \equiv 1 \pmod 9$. Thus, one has that both $\mathfrak{p}_3$ and $\mathfrak{p}_p$ split in K_pK_3 if and only if p splits in $\mathbb{Q}(\zeta_9, \sqrt[3]{3})$. But that happens if and only if the first Reidi map $\mathrm{cl}(F_p)[\sigma_p - 1] \to \mathrm{cl}(F_p)/(\sigma_p - 1)$ is the 0 map, and the theorem follows. $\square$

We were completely unable to find a governing field for the $(\sigma_p - 1)^3$-torsion in this case. Indeed, some numerical calculations showed that the probability that there was $(\sigma_p - 1)^3$-torsion given that there was $(\sigma_p - 1)^2$-torsion tended to 1/9 from above, which as pointed out to us by Hendrik Lenstra, was weakly inconsistent with there being a governing field. (The reason that this is incosnsitent with there being a field is the following: L-function techniques to count primes say that you aren't supposed to give p weight 1 and everything else weight 0, but instead p^n weight $\log(p)$ and everything else weight 0. Generalizing to counting primes whose forbenius is a given conjugacy class in a field, you are supposed to give p^n weight $\log(p)$ if $(Frob_{\mathfrak{p}})^n$ is in that class for some (equivalently any) prime $\mathfrak{p}$ lying over p. The most consistent source of error in passing from the naieve count to the correct one is that the trivial class gets more $\log(p)$ terms than any other class, and so you expect there to be slightly fewer actual primes (instead of prime powers) who split in the field. This is the underlying reason that there are more primes that are $3 \pmod 4$ than primes that are $1 \pmod 4$ up to some constant x for small values of x.)