A sample computation

Altan Erdnigor

June 27, 2024

Contents

1 Notation

- $p > 2$ a prime number.
- $\mathbf{SL}_3(\mathbb{Z})$ the special linear group over $\mathbb{Z}$.
- Γ_p the pth congruence subgroup of $\mathbf{SL}_3(\mathbb{Z})$.
- $Z_G(x)$ the centralizer of $x \in G$.
-
$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & -p^2 \end{pmatrix} \in \mathbf{SL}_3(\mathbb{Z}) \tag{1}$$
-
$$\tilde{A} = \mathbf{Id} + pA = \begin{pmatrix} 1 & 0 & p \\ p & 1 & 0 \\ 0 & p & 1 - p^3 \end{pmatrix} \in \Gamma_p \tag{2}$$
- If C is a matrix, $\chi_C(\lambda) \coloneqq \det(\lambda \mathbf{Id} - C)$ is the characteristics polynomial.
- $f(t) \coloneqq \chi_A(t) = t^3 + p^2 t^2 - 1$.

2 Intro

In this note we establish the following results:

1. The regularor of $\tilde{A}$ grows as $\approx 3\ln^2(p)$.
   That is, $\mathrm{Reg}(\mathbb{Q}(\alpha)/\mathbb{Q}) \approx 3\ln^2(p)$ for α a root of $\chi_{\tilde{A}}$.

2. The index of the centralizers $[Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) : Z_{\Gamma_p}(\tilde{A})] = 3$ does not depend on p.

This might be interesting.

3 Regulators

We mimic the proofs from a Keigh Conrad's write-up on the Dirichlet unit theorem [1].

Let $\mathbb{Q}(\alpha)$ be the number field obtain by attaching the root of $f(t)$ to $\mathbb{Q}$.

Proposition 3.1. *$\mathbb{Q}(\alpha)/\mathbb{Q}$ is a totally real number field of degree 3.*

Proof. First, $f(t)$ is irreducible as it has no rational roots: $f(1) = p^2 \neq 0, f(-1) = p^2 - 2 \neq 0$.

The discriminant of $f(t)$ equals

$$\mathrm{disc}_f(p) = 4p^6 - 27.$$

The discriminant is always positive $\mathrm{disc}_f(p) > 0$, thus the number field is totally real. □

Proposition 3.2. $\mathbb{Z}[\alpha]^* = \{\pm\alpha^a(1+p\alpha)^b \mid a, b \in \mathbb{Z}\}$.

Note that $\alpha, 1 + p\alpha$ are not necessarily fundamental units in $\mathbb{Q}(\alpha)/\mathbb{Q}$ as we don't claim that the ring of integers of $\mathbb{Q}(\alpha)/\mathbb{Q}$ coincides with $\mathbb{Z}[\alpha]$.

Proof. We have

$$\alpha(\alpha^2 + p^2\alpha) = 1 \tag{3}$$

$$(1 - p\alpha)(1 + p\alpha) = \alpha^3 \tag{4}$$

It shows that $\alpha, 1 + p\alpha$ are indeed units.

Let $\alpha_1 < \alpha_2 < \alpha_3$ be the three different roots of f. We shall compute them approximately.

$$\alpha_1 = -p^2 + O\left(p^{-4}\right),$$
$$\alpha_2 = -p^{-1} + O\left(p^{-4}\right),$$
$$\alpha_3 = p^{-1} + O\left(p^{-4}\right).$$

Remark 3.3. *A computation shows that for $p = 100$ we have*

$$\alpha_1 = -9999.99999999000,$$
$$\alpha_2 = -0.01000000500000625,$$
$$\alpha_3 = 0.00999999500000625.$$

It is not important that p is not a prime in this case as the estimate works for any sufficiently large p.

By the definition of the regulator we have

$$
\begin{aligned}
\operatorname{Reg}(\alpha, p\alpha+1) &= \begin{vmatrix} \ln|\alpha_1| & \ln|\alpha_3| \\ \ln|p\alpha_1+1| & \ln|p\alpha_3+1| \end{vmatrix} \\
&\approx \begin{vmatrix} \ln|-p^2| & \ln|\frac{1}{p}| \\ \ln|-p^3+1| & \ln|2| \end{vmatrix} = \ln(p^2)\ln 2 + \ln(p^3-1)\ln(p) \\
&\approx \ln(p)(3\ln(p)+2\ln 2). \qquad (5)
\end{aligned}
$$

Therefore $\operatorname{Reg}(\alpha, p\alpha+1) > 0$ for all prime p.

Hence $\alpha, p\alpha+1$ are independent units.

Remark 3.4. *For example, for $p = 73$ SageMath computes the regulator to be approximately* $\operatorname{Reg} = 61.1719663782187$.

```
p = Primes().unrank(20) # p = 73
R.<x> = PolynomialRing(QQ)
P = x^3 + p^2 * x^2 - 1
K.<a> = QQ.extension(P)
print(K.regulator())
```

Listing 1: SageMath code

Whereas the above estimate gives 61.1719663782957. *These numbers coincide up to* 10^{-11}.

Another example, for $p = 547$ SageMath computes the regulator to be approximately $\operatorname{Reg} = 127.978045931846$.

```
p = Primes().unrank(100) # p = 547
R.<x> = PolynomialRing(QQ)
P = x^3 + p^2 * x^2 - 1
K.<a> = QQ.extension(P)
print(K.regulator())
```

Listing 2: SageMath code

Whereas the above estimate gives 127.97804593184651. *These numbers coincide up to* 10^{-12}.

It is left to prove that they are fundamental units in $\mathbb{Z}[\alpha]$. By Corollary 5.9 from Conrad it is sufficient to check

$$\frac{16\operatorname{Reg}(\alpha, p\alpha+1)}{(\ln(\operatorname{disc}_f/4))^2} < 2.$$

Substituting, we obtain

$$\frac{16\operatorname{Reg}(\alpha, 2\alpha+1)}{(\ln(\operatorname{disc}_f/4))^2} \approx \frac{16\ln(p)(3\ln(p)+2\ln 2)}{(\ln((4p^6-27)/4))^2}.$$

Asymptotically, the latter equals

$$\xrightarrow{p\to\infty} \frac{48\ln(p)^2}{(\ln(p^6))^2} = \frac{4}{3}.$$

Therefore it is < 2 for big enough p, QED. $\square$

Remark 3.5. *In fact, the function*

$$\frac{16\ln(p)(3\ln(p)+2\ln 2)}{(\ln((4p^6-27)/4))^2}$$

is smaller then 2 *for all* $p > 2.6$*. It monotonously decreases to the asymptotic value* $\frac{4}{3}$*.*

The first several values of $g(p) \stackrel{\text{def}}{=} \frac{16\,\mathrm{Reg}(\alpha,2\alpha+1)}{(\ln(\mathrm{disc}_f/4))^2}$ *are presented in the following*

p	$g(p)$
2	2.3005757200277737
3	0.948774985707828
5	1.7162543373046009
7	0.824986119068219
11	1.5902803808431747
13	1.573545207927126
17	1.5508005143276846
19	1.5425857167054255
23	1.529835319790773
29	1.5163082966042292
31	1.5127547443392193
37	1.5039633069049658
41	1.4992465878896728
43	1.4971456295557026
47	1.4933611793019335
53	1.4885186045113814
59	1.484436992267399
61	1.483211643289589
67	1.4798674282030506
71	1.4778740553564413
73	1.4769381932859227
79	1.4743421857047407
83	1.4727660220987417
89	1.4705979224908206
97	1.4680152465868979
101	1.4668359850881518
103	1.466271166102171
107	1.4651872592939545
109	1.4646667672702098
113	1.4636655275160453
127	1.4605230591156473

Table 1: Values of p and $g(p)$

which we computed using SageMath

```
for i, p in enumerate(Primes()):
    if i > 30:
        break
    R.<x> = PolynomialRing(QQ)
    P = x^3 + p^2 * x^2 - 1
    K.<a> = QQ.extension(P)
    rg = K.regulator()
    print(p, float(16 * rg * ln( p^6 - 27/4 )^(-2)))
```

Listing 3: SageMath code

Remark 3.6. *We just proved that the regulator is approximately*

$$\ln(p)(3\ln(p) + 2\ln 2),$$

which is close to $3\ln^2 p$ *we wanted from the beginning.*

4 Centralizers

Proposition 4.1. *The centralizer of* $\tilde{A}$ *in* $\mathbf{SL}_3(\mathbb{Z})$ *is generated by* $A, pA + \mathbf{Id}$.

$$Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) = \{A^a(pA + \mathbf{Id})^b \mid a, b \in \mathbb{Z}\}.$$

Proof. Since $\tilde{A}$ is regular, its centralizer in $\mathbf{Mat}_3(\mathbb{C})$ is $\mathbb{C}\left\langle \mathbf{Id}, A, A^2 \right\rangle$. Now,

$$\mathbb{C}\left\langle \mathbf{Id}, A, A^2 \right\rangle \cap \mathbf{SL}_3(\mathbb{Z}) \subset \mathbb{Z}\left\langle \mathbf{Id}, A, A^2 \right\rangle = \mathbb{Z}[A].$$

Indeed,

$$\mathbf{Id} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & -p^2 \end{pmatrix}, A^2 = \begin{pmatrix} 0 & 1 & -p^2 \\ 0 & 0 & 1 \\ 1 & -p^2 & p^4 \end{pmatrix}, \tag{6}$$

Considering the first matrix column we see that if a complex combination has integer coefficients, it is in fact integer combination.

Moreover, the centralizer of $\tilde{A}$ is a group, therefore it lies inside the multiplicative group of $\mathbb{Z}[A]$

$$Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) \subset \mathbb{C}\left\langle \mathbf{Id}, A, A^2 \right\rangle \cap \mathbf{SL}_3(\mathbb{Z}) \subset \mathbb{Z}[A]^*.$$

There is an isomorphism of $\mathbb{Z}$-algebras $\mathbb{Z}[A] \simeq \mathbb{Z}[x]/(f(x)) = \mathbb{Z}[\alpha]$. Applying Proposition 3.2 end the proof

$$Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) \subset \mathbb{Z}[A]^* = \{\pm A^a(pA + \mathbf{Id})^b \mid a, b \in \mathbb{Z}\}.$$

□

We are to study the centralizer of $\tilde{A}$ in Γ_p.

$$Z_{\Gamma_p}(\tilde{A}) \subset Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) \cong \mathbb{Z}^2.$$

Proposition 4.2. *The index of the one centralizer inside the other* does not depend on p *and equals* 3.

$$[Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) : Z_{\Gamma_p}(\tilde{A})] = 3.$$

Proof. As $A \pmod{p}$ is equivalent to the cyclic permutation matrix, it follows that $A^3 \in \Gamma_p$.

Thus the smaller centralizer is generated by $A^3, \tilde{A}$

$$Z_{\Gamma_p}(\tilde{A}) = \{A^{3a}(pA + \mathbf{Id})^b \mid a, b \in \mathbb{Z}\},$$

and it is clear that the index is 3. $\square$

References

[1] Keith Conrad. Dirichlet's unit theorem. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/unittheorem.pdf`.