DOES $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ HAVE UNIQUE PRIME FACTORIZATION?

JONATHAN HANKE

Abstract. These are notes for my 7-minute PROMYS counselor mini-mini-course marathon talk on August 8, 2014 giving four proofs answering the question "Does $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ have unique prime factorization?".

1. Setup and Statement of Unique Prime Factorization

Let $\alpha := \frac{1+\sqrt{-23}}{2}$ and $K := \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-23})$. We say that $u \in \mathbb{Z}[\alpha]$ is a **unit** if u has a multiplicative inverse in $\mathbb{Z}[\alpha]$. We say that an element $a \in \mathbb{Z}[\alpha]$ is **irreducible** if any factorization of $a = bc$ with $b, c \in \mathbb{Z}[\alpha]$ implies that either b or c is a unit. We say that $\mathbb{Z}[\alpha]$ has **unique prime factorization** if any two factorizations of an non-zero element $x \in \mathbb{Z}[\alpha]$ as a product of irreducible elements of $\mathbb{Z}[\alpha]$ can be transformed into each other by taking unit multiples and reordering.

The **class group** of K is defined to be the group of non-zero ideals of $\mathbb{Z}[\alpha]$ under multiplication modulo the principal ideals in $\mathbb{Z}[\alpha]$, and the **class number** h_K is defined to be the cardinality of the (finite) class group. In terms of class numbers, it is known [1, Thrm 24, p128] that $h_K = 1 \iff \mathbb{Z}[\alpha]$ has unique prime factorization.

2. Proof by counterexample

Consider the possible factorizations of $6 = 2 \cdot 3$ in $\mathbb{Z}[\alpha]$. We know that the norm of $x + y\alpha \in \mathbb{Z}[\alpha]$ is given by

$$N_{K/\mathbb{Q}}(x + y\alpha) = (x + y\alpha)(x + y\overline{\alpha}) = x^2 + xy + 6y^2$$

and so we also see that $N_{K/\mathbb{Q}}(\alpha) = \alpha \cdot \overline{\alpha} = 6$. This gives the two distinct factorizations

$$6 = 2 \cdot 3 = \alpha \cdot \overline{\alpha}$$

which do not differ by unit multiples (since the only units in $\mathbb{Z}[\alpha]$ are ± 1). Computing the norms of the factors gives

$$N_{K/\mathbb{Q}}(2) = 4 \qquad N_{K/\mathbb{Q}}(3) = 9 \qquad N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\overline{\alpha}) = 6$$

so any common factorization that refines these two factorizations must use elements β with $N_{K/\mathbb{Q}}(\beta) = 2$ or 3. However the quadratic norm form $x^2 + xy + 6y^2$ doesn't represent 2 or 3, so no such common refinement exists, proving the failure of unique prime factorization in $\mathbb{Z}[\alpha]$.

Date: August 15, 2014.

3. Proof by binary quadratic forms

We can compute the class number h_K of the ring of integers $\mathbb{Z}[\alpha]$ of K by the theorem of Dedekind that associates the ideal classes (i.e. the non-zero ideals modulo principal ideals) with the $SL_2(\mathbb{Z})$-equivalence classes of binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $b^2 - 4ac = -23$ since the field discriminant of K is $\Delta_K = -23$. (See [1, Thrm 6, p204; §7, p207] for more details.) These can be enumerated from the usual reduction theory inequalities

$|b| < \sqrt{\frac{|\Delta_K|}{4}}$ and $|b| \leq a \leq c$ where we require $b > 0$ when $|b| = a$ or $a = c$. This gives that there are three $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of forms of discriminant -23, namely

$$\mathrm{BQF}(-23) := \{x^2 \pm xy + 6y^2, 2x^2 + xy + 3y^2, 2x^2 - xy + 3y^2\},$$

so we have that the class number $h_K = |\mathrm{BQF}(-23)| = 3$. Since $h_K = 3 \neq 1$ we know that its ring of integers $\mathbb{Z}[\alpha]$ doesn't have unique prime factorization.

4. Proof by class number formula

From the analytic class number formula [2, Theorem 1, eq (4.3), p344], there is a class number formula that applies to imaginary quadratic fields $K := \mathbb{Q}(\sqrt{-d})$ when $-d < 0$ and $-d \equiv 1 \pmod 4$ is squarefree, given by

$$h_K = \frac{1}{-d} \sum_{j=1}^{d-1} j \left(\frac{-d}{j} \right).$$

Using Jacobi symbol quadratic reciprocity this can be rewritten as

$$h_K = \frac{1}{-d} \sum_{j=1}^{d-1} j \left(\frac{j}{d} \right)$$

and evaluated by knowing the quadratic character of all elements of $(\mathbb{Z}/23\mathbb{Z})^\times$. When $-d = -23$ we know that $g = 5$ is a generator for $(\mathbb{Z}/23\mathbb{Z})^\times$ and so the group of squares is generated by $5^2 \equiv 2 \pmod{23}$, giving us the list of squares

$$\langle 2 \rangle = \{2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1\} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

With this the class number formula evaluates to

$$\begin{aligned} h_K &= \frac{1}{-23} \sum_{j=1}^{22} j \left(\frac{j}{23} \right) \\ &= \frac{1}{-23} [1 + 2 + 3 + 4 - 5 + 6 - 7 + 8 + 9 - 10 - 11 \\ &\qquad +12 + 13 - 14 - 15 + 16 - 17 + 18 - 19 - 20 - 21] \\ &= \frac{1}{-23}(-69) = 3. \end{aligned}$$

Since $h_K = 3 \neq 1$, we know that $\mathbb{Z}[\alpha]$ does not have unique prime factorization.

5. Proof by class field theory

Notice that $-23 = 4a^3 - 27b^2$ has an integer solution by setting $a = b = 1$. Since the discriminant of the cubic polynomial $f(x) = x^3 - ax + b$ is $4a^3 - 27b^2$, this meant that the cubic field $L := \mathbb{Q}[\beta]$ where β is a root of the irreducible polynomial $g(x) := x^3 - x + 1$ has field discriminant $\Delta_L = -23$. Since $\Delta_L < 0$ we see that not all roots of $g(x)$ are real, so the extension $L/\mathbb{Q}$ is not Galois. Its Galois closure $M := L^{\mathrm{GC}}$ is therefore a degree 6 Galois extension of $\mathbb{Q}$ with Galois group S_3.

Now there is a unique subgroup $C_3 \subset S_3$ of order 3 (i.e. generated by the 3-cycle (123)), and by Galois theory its fixed subfield

$$M^{C_3} := \{x \in M \mid \sigma(x) = x \text{ for all } \sigma \in C_3\} \subset M$$

is a quadratic extension of $\mathbb{Q}$. Since M is ramified only at the primes of $\mathbb{Z}$ which ramify in L, we see that only the prime 23 ramifies in M, and since there are no unramified quadratic extensions of $\mathbb{Q}$ with discriminant 1, we see that 23 must also ramify in M^{C_3}, and that this is the only prime which ramifies in M^{C_3}, so $M^{C_3} = K$.

By considering the factorization of 23 in L, we see that it must factor as $\mathfrak{p}_1^2\,\mathfrak{p}_2$ and that it must factor in a similar way in each of the conjugates of L in M, so 23 factors in M as $23 = \mathfrak{p}_1^2\,\mathfrak{p}_2^2\,\mathfrak{p}_3^2$ which shows that the extension M/K is unramified. Therefore since M/K is a Galois extension with abelian Galois group C_3 we see that it is contained in the Hilbert class field $\mathrm{HCF}(K)$ which has degree $[\mathrm{HCF}(K) : K] = h_K$. However since $[L : K] = 3$ we know that $3 = [L : K] \mid [\mathrm{HCF}(K) : K] = h_K$ so $3 \mid h_K$. Therefore $h_K \neq 1$ and so $\mathbb{Z}[\alpha]$ doesn't have unique prime factorization!

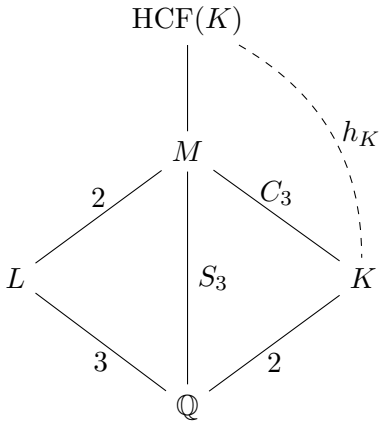

Figure: Tower of fields diagram

For more reading about these kinds of constructions, see for example [3] and [4].

References

[1] Harvey Cohn: *Advanced Number Theory*, Dover Publications, Mineola NY, 1962.
[2] Z.I. Borevich and I.R. Shafarevich: *Number Theory*, Academic Press, New York, 1966.
[3] Henri Cohen and Anna Morra: *Counting Cubic Extensions with given Quadratic Resolvent*, `arxiv.org/pdf/1003.1869v1.pdf`, March 2010.
[4] Guillermo Mantilla-Soler: *Integral Trace Forms associated to Cubic Extensions*, `arxiv.org/pdf/1104.4598v1.pdf`, April 2011.