How to describe all cubic Galois extensions?

Juliusz Brzeziński and Ulf Persson.

Mathematical Sciences
Chalmers and Gothenburg University
S–41296 Göteborg, Sweden
jub@chalmers.se, ulfp@chalmers.se

1 Introduction

Every quadratic field extension of the rational numbers is a field $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer different from 1. Moreover, the fields corresponding to different d are different, that is, they are not isomorphic as fields. Of course, the number $\sqrt{d}$ generating the extension is a zero of the polynomial $X^2 - d$. This well-known description of the quadratic fields over the rational numbers is very satisfactory. Is it possible to describe in a similar way all cubic extensions of the rational numbers?

Trying to find such a description, we note that there are two types of cubic extensions K of $\mathbb{Q}$. If the degree $[K : \mathbb{Q}] = 3$, then the automorphism group $G(K/\mathbb{Q})$ whose order must divide 3, consists of either 1 or 3 elements. In the context of Galois theory, it is more interesting to look at cubic Galois extensions, that is, cubic extensions which are splitting fields of cubic polynomials. This will be our purpose. We want to describe all cubic Galois extensions, that is, the fields K such that $|G(K/\mathbb{Q})| = [K : \mathbb{Q}] = 3$. Usually, such extensions are called **cubic cyclic fields**, since the Galois group $G(K/\mathbb{Q})$ is, of course, cyclic of order 3.

We would like to have a similar description as in the case of quadratic extensions, which means that we want to construct a list of some simple cubic polynomials in such a way that different polynomials define different (non-isomorphic) cubic Galois fields and every such field can be obtained as a splitting field of a cubic polynomial belonging to our list. Moreover, when a cubic Galois field is given as a splitting field of a cubic polynomial, we would like to have a possibility to find a polynomial belonging to our list, which defines this field. Let us notice that there exist different solutions of this problem and rather vast list of references (see [C], 6.4.2 and the references), so our purpose is to present the topic in an easily accessible way.

Before we start, let us note that we can not expect an equally simple answer as in the case of quadratic fields. If we take $K = \mathbb{Q}(\sqrt[3]{d})$, where d is a cube-free integer different from ± 1, then K is not a Galois extension of $\mathbb{Q}$, since $X^3 - d$, which is the minimal polynomial of $\sqrt[3]{d}$ has zeros $\varepsilon^i \sqrt[3]{d}$, where $\varepsilon = \frac{-1+\sqrt{-3}}{2}$ is the primitive 3rd root of 1 and $i = 0, 1, 2$. Two of these numbers are non-real and, consequently, not in the field K. In the next section, we discuss how to construct all cyclic cubic fields.

2 Cyclic cubic fields

A cyclic cubic field K can be generated over $\mathbb{Q}$ by any non-rational number $x \in K$. In fact, the field $\mathbb{Q}(x)$ is then bigger than $\mathbb{Q}$ and must be equal to K, since there are no subfields between $\mathbb{Q}$ and K. The minimal polynomial of x has degree 3. As usual, we can choose a generator x such that its minimal polynomial has the form $\varphi(X) = X^3 - pX + q$, where p, q are integers. Denoting by x_1, x_2, x_3 the zeros of this polynomial, the discriminant of $\varphi(X)$ is the number $\Delta(\varphi) = [(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)]^2 = 4\,p^3 - 27\,q^2$. Computing the discriminant, one can decide whether the splitting field of $\varphi(X)$ is cyclic or not (see the article on cubic and quartic equations in this volume):

Proposition 2.1. *The splitting field of an irreducible polynomial $\varphi(X) = X^3 - pX + q$ over $\mathbb{Q}$ is cyclic if and only if its discriminant $\Delta(\varphi) = 4\,p^3 - 27\,q^2$ is a rational square.*

Assuming that p, q are integers, the discriminant of an irreducible polynomial whose splitting field is cyclic must be a square of an integer. For such a polynomial the coefficient p must be positive. One of the the zeros of any cubic polynomial over $\mathbb{Q}$ must be real. Therefore, all zeros are real, since the splitting field is generated by the real zero. We shall denote by $\delta(\varphi)$ the square root of $\Delta(\varphi)$ and call it the **reduced discriminant**.

Example 1. It is easy to check that the polynomial $\varphi(X) = X^3 - 3X + 1$ is irreducible over $\mathbb{Q}$. We have $\Delta(\varphi) = 9^2$, so the splitting field of $\varphi(X)$ is cyclic. Let x be any zero. Then $K = \mathbb{Q}(x)$ is the splitting field. It is not difficult to check that the remaining two zeros of $\varphi(X)$ are $x^2 - 2$ and $2 - x - x^2$.

Unfortunately, it is impossible to give a description of the splitting fields of cyclic cubics using only the four arithmetical operations and extractions of roots if we only use the real numbers. This is a consequence of a rather unexpected property of cubic equations with 3 real zeros – in order to get a formulae for the zeros, it is necessary to use complex numbers. This phenomenon, known as Casus Irreducibilis, created many problems for mathematicians in the old ages. However, it suggests that looking for a classification of cubic cyclic extensions, it may be convenient to use complex numbers. In fact, it appears that the description of cyclic cubic extensions simplifies dramatically if we only allow the 3rd root of 1 and extend the cyclic cubic fields over $\mathbb{Q}$ to the cyclic cubic fields over the field of **Eisenstein numbers** $\mathbb{Q}(\varepsilon)$, where ε is the primitive 3rd root of 1. In the next section, we discuss the Eisenstein integers in order to apply them in classification of the cubic cyclic extensions of rational numbers.

3 The Eisenstein integers

The Eisenstein integers, also known as Eulerian integers, are the numbers $a + b\varepsilon$, where a, b are integers and $\varepsilon = \frac{-1+\sqrt{-3}}{2}$ is the primitive 3rd root of 1. These numbers form the ring of integers $\mathbb{Z}[\varepsilon]$ in the quadratic field $E = \mathbb{Q}(\sqrt{-3})$. In general,

the algebraic integers in any algebraic number field are the zeros of polynomials with integer coefficients and the highest coefficient equal 1. All integers in any algebraic number field form a ring. Probably the best known such ring of integers bigger than the rational integers $\mathbb{Z}$ is the ring of Gaussian integers $\mathbb{Z}[i]$ in the field $\mathbb{Q}(i)$. The Eisenstein integers, like the Gaussian, have unique factorization into Eisenstein primes. The Eisenstein primes π are the numbers $\pi = p$, where p is a prime number such that $p = 2 \pmod 3$ or the numbers $\pi = a + b\varepsilon$ such that

$$\mathrm{Nr}(a + b\varepsilon) = (a + b\varepsilon)(a + b\bar{\varepsilon}) = a^2 - ab + b^2$$

is a prime number (in $\mathbb{Z}$). For example, the numbers $2, 5, 2+\varepsilon$, $1+3\varepsilon$ are Eisenstein primes. The primes of the first type, that is, the "old" prime numbers which also are Eisenstein primes, are called **inert**. The new primes π such that $\mathrm{Nr}(\pi) = p = 1 \pmod 3$ will be called **split Eisenstein primes**. They split the old primes into a product of two different prime factors, for example, $7 = (1 + 3\varepsilon)(1 + 3\bar{\varepsilon})$. The only integer prime, which, up to a sign, is a square of an Eisentstein integer is the prime 3. We have, $3 = -(\sqrt{-3})^2 = -(1 + 2\varepsilon)^2$. The units in the ring of Eisenstein integers, that is, the numbers $\eta \in \mathbb{Z}[\varepsilon]$ such that η^{-1} is also an Eisenstein integer are exactly $\pm 1, \pm\varepsilon, \pm\varepsilon^2$ ($\varepsilon^2 = -1 - \varepsilon$). Notice that only ± 1 are cubes of units. The unusually high number of units in the rings of Gauss and Eisenstein integers makes these rings very special among the rings of integers in the quadratic number fields whose integers normally have only two units: ± 1. The Gauss integers have four: $\pm 1, \pm i$, and the Eisenstein integers, as we have seen, six.

The following result, whose proof can be found in several textbooks, for example, in [IR], p.13, gives the most important property of the Eisenstein integers. It is usually proved using the fact that the Eisenstein integers form an Euclidean ring with respect to the usual Euclidean norm (the square of the absolute value):

Theorem 3.1. *The ring of Eisenstein integers is a unique factorization domain.*

The theorem says that if $\alpha \in \mathbb{Z}[\varepsilon]$ and α is neither 0 or a unit, then $\alpha = \pi_1 \cdots \pi_k$, where π_i are Eisenstein primes and the factorization is unique up to the order of the factors and possible modifications of them by units. Recall that a modification by a unit means that a factor π is replaced by a factor $\eta\pi$, where η is a unit.

We shall often work with cube roots of Eisenstein integers. For convenience of references, we formulate the following simple fact:

Lemma 3.1. *Every non-zero Eisenstein integer α can be represented in the form $\alpha = \mu\nu^2{\alpha'}^3$, where $\mu\nu$ is a unit or a product of different Eisenstein primes and α' is an Eisenstein integer.*

Proof. If α is a unit, we can take $\mu = \alpha, \nu = 1, \alpha' = 1$. If α is a nonunit, then we represent it as a product of Eisenstein primes. We group these primes in such a way that μ is the product of different Eisenstein primes which in α have exponents giving residue 1 modulo 3, and ν of those whose exponents give residue 2 modulo 3. The remaining factors of α give a third power of an integer α', so we have $\alpha = \mu\nu^2{\alpha'}^3$. □

In the representation $\alpha = \mu\nu^2\alpha'^3$, the product $\mu\nu^2$ is called the **cube-free part** of α (it is unique up to a sign).

Now we use the Eisenstein integers in order to describe the cubic extensions of E. In the next section, we will "go down" and use the Eisenstein integers in order to describe the cubic cyclic extensions of the rational numbers.

Proposition 3.1. (*a*) *For every cubic Galois extension L of E there is $\alpha \in E$ such that $L = E(\sqrt[3]{\alpha})$.*

(*b*) *Two cubic extensions $E(\sqrt[3]{\alpha})$ and $E(\sqrt[3]{\beta})$ of E are isomorphic if and only if (the images of) α and β generate the same subgroup of E^*/E^{*3}, that is, $\alpha\beta$ or $\alpha^2\beta$ is a cube in E.*

(*c*) *Every cubic extension L of E is of the form $L = E(\sqrt[3]{\mu\nu^2})$, where μ, ν are Eisenstein integers and $\mu\nu^2 \neq 1$ is a unit or $\mu\nu$ is a product of different Eisenstein primes.*

Proof. (a) This is a special case of a much more general result concerning arbitrary cyclic Galois extensions of any degree n over fields containing n different nth roots of 1 (see see e.g. [L], Theorem 6.2).

In order to prove this denote by σ a nontrivial automorphism of L over E and take any $x \in L \setminus E$ such that the second coefficient (by X^2) of the minimal polynomial $\varphi(X)$ of x over E is 0. The zeros of this polynomial are $x, \sigma(x), \sigma^2(x)$ and, of course, $L = E(x)$. Moreover, we have $\mathrm{Tr}(x) = x + \sigma(x) + \sigma^2(x) = 0$. Take $y = x + \varepsilon\sigma(x) + \varepsilon^2\sigma^2(x)$. It is easy to check that $\sigma(y) = \varepsilon^2 y$, so $y \notin E$ if only $y \neq 0$. Then we have $\sigma(y^3) = y^3$, that is, $y^3 = \alpha \in E$. Thus, we have $L = E(\sqrt[3]{\alpha})$. If $y = 0$, then the equations $y = 0$ and $\mathrm{Tr}(x) = 0$ easily imply (subtract the equation and divide by $1 - \varepsilon$), that $\sigma(x) = \varepsilon x$, that is, $\sigma(x^3) = x^3$ and already $x^3 = \alpha \in E$.

(b) The abelian Kummer theory (see [L], Chap. VI, §8) says that cubic extensions of E are in a one-to-one correspondence with the cyclic subgroups of E^*/E^{*3}, when to the extension $E(\sqrt[3]{\alpha})$ corresponds the subgroup generated by the image of α in E^*/E^{*3}. Now α and β define the same subgroup if and only if $\beta E^{*3} = \alpha E^{*3}$ or $\beta E^{*3} = \alpha^2 E^{*3}$, which is equivalent to $\alpha^2\beta \in E^{*3}$ or $\alpha\beta \in E^{*3}$.

For convenience of the Reader, we give a direct proof. If $\alpha\beta$ or $\alpha^2\beta$ is a cube in E, then one checks immediately that $E(\sqrt[3]{\alpha}) = E(\sqrt[3]{\beta})$. Let $E(\sqrt[3]{\alpha})$ and $E(\sqrt[3]{\beta})$ be isomorphic. Then the field $E(\sqrt[3]{\alpha})$ contains elements x, y such that $x^3 = \alpha$ and $y^3 = \beta$. If σ is a nontrivial automorphism of L over E, then $\sigma(x) = \varepsilon^i x$ and $\sigma(y) = \varepsilon^j y$ for $i, j = 1, 2$. Assume that $\sigma(x) = \varepsilon^i x$ and $\sigma(y) = \varepsilon^i y$. Then $\sigma(x/y) = x/y$, which means that $x/y = \rho \in E$. Hence $\alpha = \rho^3\beta$ or, equivalently, $\alpha\beta^2$ is a cube in E. Assume now that $\sigma(x) = \varepsilon^i x$ and $\sigma(y) = \varepsilon^j y$, where $i \neq j$ (that is, one of the exponents equals 1, the other equals 2). Then $\sigma(x/y^2) = x/y^2$, which means that $x/y^2 = \rho \in E$. Hence $\alpha = \rho^3\beta^2$ or, equivalently, $\alpha\beta$ is a cube in E.

(c) If $L = E(\sqrt[3]{\alpha})$, then we can always assume that $\alpha \neq 0$ is an Eisenstein integer, since E is the quotient field of $\mathbb{Z}[\varepsilon]$. With the notations of Lemma 3.1, we have $L = E(\sqrt[3]{\alpha}) = E(\sqrt[3]{\mu\nu^2})$. □

4 Going up and down

In this section, we establish a correspondence between the cubic Galois extensions of the rational numbers and the cubic Galois extensions of the Eisenstein numbers. It appears that it is not difficult to read off the properties of the cubic Galois extensions of the rational numbers by "moving" them up to the Eisenstein numbers and then down to the rational numbers.

Proposition 4.1. *There is a one-to-one correspondence between cyclic cubic extensions $K \supset \mathbb{Q}$ and the cyclic cubic extensions $L = EK$ of E such that $L \supset \mathbb{Q}$ is Galois with cyclic Galois group $\mathbb{Z}_6$. Moreover, two extensions K_1 and K_2 are isomorphic if and only if the extensions $L_1 = EK_1$ and $L_2 = EK_2$ are isomorphic over E.*

Proof. It is clear that if $K \supset \mathbb{Q}$ is a cyclic cubic extension, then EK is a cyclic Galois extensions of E and Galois extensions of $\mathbb{Q}$ with Galois Group $\mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_6$. Moreover, if K_1 and K_2 are isomorphic, then EK_1 and EK_2 are isomorphic over E.

Conversely, if L is a Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}_6$ containing E, then the fixed field of the only subgroup of $\mathbb{Z}_6$ of order 2 (the identity and the complex conjugation) is a cyclic cubic extension K of $\mathbb{Q}$. It is uniquely defined by L. Thus, if L_1 and L_2 are two isomorphic Galois extensions of $\mathbb{Q}$ with Galois group $\mathbb{Z}_6$ both containing E, then the corresponding cyclic cubic subfields K_1 and K_2 are isomorphic. □

Since the extension $L = KE$ of the Eisenstein numbers obtained from a cubic Galois extension K of the rational numbers is a cyclic Galois extension of $\mathbb{Q}$, it is important to find conditions characterizing the typical cubic Galois extensions $L = E(\sqrt[3]{\alpha})$ of E which are Galois over $\mathbb{Q}$. Moreover, we want to characterize those, which have a cyclic Galois group.

Proposition 4.2. *If $L = E(\sqrt[3]{\alpha})$, where $\alpha \in E$, is a cubic extension of E, then L is a Galois extension of $\mathbb{Q}$ if and only if $E(\sqrt[3]{\alpha}) = E(\sqrt[3]{\bar{\alpha}})$, which happens if and only if $\mathrm{Nr}(\alpha) \in \mathbb{Q}^{*3}$ or $\alpha \,\mathrm{Nr}(\alpha) \in \mathbb{Q}^{*3}$. In the first case the Galois group $G(L/\mathbb{Q})$ is cyclic, and in the second, it is symmetric.*

Proof. The minimal polynomial of $\sqrt[3]{\alpha}$ over $\mathbb{Q}$ is $\varphi(X) = (X^3 - \alpha)(X^3 - \bar{\alpha}) = X^6 - \mathrm{Tr}(\alpha)X^3 + \mathrm{Nr}(\alpha)$, since it has rational coefficients and the degree 6 equal to the degree $[L : \mathbb{Q}]$. Thus if L over $\mathbb{Q}$ is Galois, we have $\sqrt[3]{\bar{\alpha}} \in L$, since it is a zero of the same irreducible polynomial which has $\sqrt[3]{\alpha}$ as its zero. Hence, we have $L = E(\sqrt[3]{\alpha}) = E(\sqrt[3]{\bar{\alpha}})$. Conversely, if these equalities hold, then the field L is a splitting field of the polynomial $\varphi(X)$, so it is a Galois extension of $\mathbb{Q}$.

According to Proposition 3.1 (b), the equality $E(\sqrt[3]{\alpha}) = E(\sqrt[3]{\bar{\alpha}})$ is equivalent to $\alpha\bar{\alpha} = \mathrm{Nr}(\alpha) \in E^{*3}$ or $\alpha^2\bar{\alpha} = \alpha\,\mathrm{Nr}(\alpha) \in E^{*3}$. By Proposition 3.1, we have $\alpha = \mu\nu^2$, where $\mu\nu$ is a unit or a product of different Eisenstein primes. It is easy to see that $\alpha\bar{\alpha} = \mu\nu^2\bar{\mu}\bar{\nu}^2$ is a cube if and only if $\nu = \eta\bar{\mu}$, and $\alpha^2\bar{\alpha} = \mu^2\nu^4\bar{\mu}\bar{\nu}^2$ is a cube if and only if $\bar{\mu} = \eta\mu$ and $\bar{\nu} = \pm\eta\nu$ (η a unit). We see that in the first case $\mathrm{Nr}(\alpha) \in \mathbb{Q}^{*3}$, and in the second, $\alpha\,\mathrm{Nr}(\alpha) \in \mathbb{Q}^{*3}$.

Assume that the first case occurs. As a splitting field of $\varphi(X)$, the field L has 6 automorphisms mapping its zero $\sqrt[3]{\alpha}$ (a fixed value) on one of the 6 others: $\varepsilon^i\sqrt[3]{\alpha}$, $\varepsilon^i\sqrt[3]{\bar{\alpha}}$ for $i=0,1,2$. It is easy to check that the automorphism mapping $\sqrt[3]{\alpha}$ onto $\varepsilon\sqrt[3]{\bar{\alpha}}$ has order 6 (it follows from the assumption that $\sqrt[3]{\alpha}\sqrt[3]{\bar{\alpha}} = \sqrt[3]{\mathrm{Nr}(\alpha)}$ is a rational number). Hence, the Galois group $G(L/\mathbb{Q})$ is cyclic.

Conversely, assume that $G(L/\mathbb{Q})$ is cyclic. We want to prove that $\mathrm{Nr}(\alpha)$ is a rational cube. In fact, we have $\sqrt[3]{\alpha}\sqrt[3]{\bar{\alpha}} = \sqrt[3]{\mathrm{Nr}(\alpha)} \in L$. Hence L contains a splitting field of the polynomial $X^3-\mathrm{Nr}(\alpha)$ with rational coefficients if this polynomial is irreducible. But the splitting field of such an irreducible polynomial is of degree 6 over $\mathbb{Q}$ and its Galois group is the symmetric group S_3. This contradicts our assumption about $G(L/\mathbb{Q})$. Hence the polynomial $X^3-\mathrm{Nr}(\alpha)$ must be reducible, which shows that $\mathrm{Nr}(\alpha)$ is a rational cube.

Thus we have proved that the Galois group $G(E(\sqrt[3]{\alpha})/\mathbb{Q})$ is cyclic if and only if $\mathrm{Nr}(\alpha)$ is a rational cube. Consequently, it must be symmetric if and only if $E(\sqrt[3]{\alpha})$ is Galois over $\mathbb{Q}$ and $\alpha\,\mathrm{Nr}(\alpha)$ is a cube in $\mathbb{Q}$, since there are only two non-isomorphic groups with 6 elements. □

Now we are ready to prove that every cubic Galois extension of the rational numbers can be uniquely defined by an Eisenstein integer, which we define below. Notice that if z is a complex number such that $\Re z\cdot\Im z\neq 0$, then exactly one of the four numbers $\pm z, \pm\bar{z}$ is in the first quadrant of the complex plane.

Theorem 4.1. *For every cubic Galois field over $\mathbb{Q}$ there exists a unique Eisenstein integer in the first quadrant of the complex plane called the* **invariant** *of the field such that two cubic Galois fields are isomorphic if and only if the corresponding invariants are equal. More exactly:*

(a) If K is a cubic Galois field and $L=KE$, then there exists a unique f in the first quadrant of the complex plane such that $L=E(\sqrt[3]{f\bar{f}^2})$ and $f=-\bar{\varepsilon}$ or f is a product of different split Eisenstein primes. Two cubic Galois fields over the rational numbers are isomorphic if and only if the corresponding numbers f are equal.

(b) The field $L=\mathbb{Q}(\sqrt[3]{f\bar{f}^2})$ is the splitting field of the sextic polynomial

$$X^6-\mathrm{Nr}(f)\,\mathrm{Tr}(f)X^3+\mathrm{Nr}(f)^3. \tag{1}$$

The cubic subfield K of L is generated by $x=\sqrt[3]{f\bar{f}^2}+\sqrt[3]{\bar{f}f^2}$, when the second cubic root is chosen so that the product of both equals $\mathrm{Nr}(f)$. The minimal polynomial of x over $\mathbb{Q}$ is

$$X^3-3\,\mathrm{Nr}(f)X-\mathrm{Tr}(f)\,\mathrm{Nr}(f), \tag{2}$$

and K is its splitting field.

Proof. (a) By Proposition 3.1 (c), we have $L=E(\sqrt[3]{\mu\nu^2})$, where $\mu\nu$ is a unit or a product of different Eisenstein primes. In the first case, we note that $L=E(\sqrt[3]{\eta})$,

for any unit $\eta \neq \pm 1$. The only unit in the first quadrant of the complex plane is $\eta = -\bar{\varepsilon}$, so taking $f = -\bar{\varepsilon}$, we get $L = E(\sqrt[3]{f\bar{f}^2})$.

In the second case, by Proposition 4.2, we have $\mathrm{Nr}(\mu\nu^2) = \mu\nu^2\bar{\mu}\bar{\nu}^2$ is a cube and $\mu\nu$ is divisible by at least one Eisenstein prime π. It is easy to see that the product contains a cube of π if and only if $\bar{\mu} = \eta\nu$, where η is a unit. Hence, we have $\bar{\nu} = \eta\mu$ and it follows that $L = E(\sqrt[3]{\mu\bar{\mu}^2})$. Now notice that if an inert prime π or the prime $\pi = \sqrt{-3}$ divides μ, then its cube divides $\mu\bar{\mu}^2$, so it can be removed as a factor of μ. Hence, we can assume that μ is a product of only split Eisenstein primes. Assume that both the real and the imaginary parts of μ are non-zero. If the real part of μ is not positive, we can replace it by $-\mu$ without changing the field $L = E(\sqrt[3]{\mu\bar{\mu}^2})$. If now μ is not in the upper half plane, we can replace it by $\bar{\mu}$. Thus if finally μ is in the first quadrant, we define $f = \mu$ and we have $L = E(\sqrt[3]{f\bar{f}^2})$ as required. We prove that $\Re f \cdot \Im f \neq 0$ in (b).

Assume now that $E(\sqrt[3]{f\bar{f}^2})$ and $E(\sqrt[3]{f'\bar{f}'^2})$ are isomorphic. According to Proposition 3.1 (b), we get that either $f\bar{f}^2 f'\bar{f}'^2$ or $f\bar{f}^2 f'^2\bar{f}'^4$ is a cube. Similar argument as above shows that in the first case, we have $\bar{f}' = \eta f$ and in the second, $f' = \eta f$ for a unit η. Taking this into account, we use again that the products are cubes and get $\eta = \pm 1$. However, the choice of f, f' in the first quadrant makes the equalities $\bar{f}' = \eta f$ and $f' = \eta f$ impossible unless $f' = f$.

(b) As we noted in the proof of Proposition 4.2, the field L is a splitting field of the polynomial $(X^3 - f\bar{f}^2)(X^3 - \bar{f}f^2)$, which is just (1). The number x is fixed by the automorphism of order 2 mapping $\sqrt[3]{f\bar{f}^2}$ on $\sqrt[3]{\bar{f}f^2}$ and it is easy to find the cubic polynomial whose zero is x. Since x is not rational number, it generates the fixed field K of the automorphism of order 2. The field K is a cubic Galois extension of $\mathbb{Q}$, which must be the splitting field of the minimal polynomial of x.

Finally notice that if $\Im f = 0$, then $L = \mathbb{Q}(\sqrt[3]{f\bar{f}^2})$ is a real field, which is not the case. If $\Re f = 0$, then $\mathrm{Tr}(f) = 0$ and the polynomial (1) is reducible, which is impossible. Thus, we have $\Re f \cdot \Im f \neq 0$. □

The non-unit invariants of the cubic Galois fields are products of split Eisenstein primes. If g is any complex number which is a product of such Eisenstein primes, then exactly one of $\pm g, \pm\bar{g}$ is in the first quadrant. In this sense, we shall say that each product of split Eisenstein primes defines uniquely a cubic Galois extension of the rational numbers. According to Theorem 4.1 (b), it is easy to find a cubic Galois field over $\mathbb{Q}$ when its invariant f is given – it is simply the splitting field of the polynomial (2). We shall say that this polynomial is **canonical** for its splitting field.

Now we can construct a list of cubic Galois extensions of $\mathbb{Q}$ using their invariants $f \in \mathbb{Z}[\varepsilon]$. We can order such polynomials with respect to the value of the norm $\mathrm{Nr}(f)$ of such numbers f. First we note an observation concerning the number of such polynomials:

Proposition 4.3. *The number of non-isomorphic cubic Galois extensions of rational numbers with the invariant f such that $\mathrm{Nr}(f)$ is fixed equals $3 \cdot 2^{k-1}$, where k is the number of different primes dividing $\mathrm{Nr}(f)$, when $\mathrm{Nr}(f) \neq 1$, and it is equal*

1, *when* $\mathrm{Nr}(f) = 1$. *These cubic Galois fields are splitting fields of the polynomials* (2) *with fixed* $p = 3\,\mathrm{Nr}(f)$.

Proof. According to Proposition 4.1 and Theorem 4.1, it suffices to count the number of invariants f corresponding to fields with given $\mathrm{Nr}(f)$. For $\mathrm{Nr}(f) = 1$, we get only one cubic Galois field over $\mathbb{Q}$ (see the first argument in the proof of Theorem 4.1 (a)).

If $\mathrm{Nr}(f) = p_1 \cdots p_k$ is a product of prime numbers congruent to 1 modulo 3, and we fix a prime π_i such that $\mathrm{Nr}(\pi_i) = p_i$ for $i = 1, \ldots, k$, then each solution of the equation $\mathrm{Nr}(f) = p_1 \cdots p_k$ has the form $f = \eta\alpha_1 \cdots \alpha_k$, where η is one of $\pm 1, \pm\varepsilon, \pm\varepsilon^2$ and $\alpha_i = \pi_i$ or $\bar{\pi}_i$ for $i = 1, \ldots, k$. Hence, we have $6 \cdot 2^k$ different solutions. Now we need to count the number of different solutions f in the first quadrant of the complex plane. Since the mappings $f \mapsto -f$ and $f \mapsto \bar{f}$ do not change the field $E(\sqrt[3]{f\bar{f}^2})$ and exactly one of the numbers $\pm f, \pm\bar{f}$ is in the first quadrant, the number of such invariants f equals $3 \cdot 2^{k-1}$. □

Example 2. It is easy to construct the cubic Galois field corresponding to a given invariant f. In the next section, we list cubic Galois fields together with their *minimal* canonical polynomials, which we define there. Already now, we could list cubic Galois fields ordered by the increasing norm $\mathrm{Nr}(f)$ and defined by their canonical polynomials. The first few values of $\mathrm{Nr}(f)$ are $1, 7, 13, 19, 31, \ldots$. The first composite number in the sequence is $91 = 7 \cdot 13$. For $\mathrm{Nr}(f) = 1$, we have only one polynomial corresponding to the extension $L = E(\sqrt[3]{\varepsilon})$ whose invariant is the only 6th root of 1 in the first quadrant, that is, $f = -\bar{\varepsilon} = \frac{1+\sqrt{3}}{2}$. In fact, it is easy to check that L is the splitting field of $X^6 - X^3 + 1$ with Galois group $\mathbb{Z}_6$ and the corresponding cyclic Galois field over $\mathbb{Q}$ is the splitting field of $X^3 - 3X + 1$. For $\mathrm{Nr}(f) = 7$, as for any prime number congruent to 1 modulo 3 in the sequence, we have 3 polynomials. An easy computation shows that these are the splitting fields of the trinomials $X^3 - 21X - 7$, $X^3 - 21X - 28$, $X^3 - 21X - 35$ with corresponding invariants $f = 2 + 3\varepsilon$, $f = 3 + 2\varepsilon$, $f = 3 + \varepsilon$.

We end this section showing how to find the invariant f when a cubic Galois field K over the rational numbers is given as a splitting field of some cubic polynomial.

Proposition 4.4. *Let* K *be the splitting field of the cyclic cubic* $\varphi(X) = X^3 - pX + q$, *where* $\Delta(\varphi) = 4\,p^3 - 27\,q^2 = d^2$ $(d = \delta(\varphi))$. *Then* K *is the splitting field of the polynomial* (2) *with the invariant* f *defined in the following way:* $4(d + 3q\sqrt{-3}) = f\bar{f}^2h^3$, *where* $h \in \mathbb{Z}[\varepsilon]$, *the factor* f *is in the first quadrant of the complex plane and is a unit or a product of different split Eisenstein primes.*

Proof. The equality $\Delta(\varphi) = 4\,p^3 - 27\,q^2 = d^2$ implies that $p = \frac{27}{4}\,s^2 + \frac{1}{4}\,r^2$, where $d = rp$ and $q = sp$ for some parameters r, s. Let x_1 be one of the zeros of $\varphi(X)$ in K. It is not difficult to find the remaining two zeros x_2, x_3 expressed by r, s. Then, as in the proof of Proposition 3.1 (b), we have $x = x_1 + \varepsilon x_2 + \varepsilon^2 x_3$, which satisfies $x^3 = \alpha \in \mathbb{Q}(\varepsilon)$ (we have $x \neq 0$ as $p \neq 0$). A short computation shows that α equals $4(d + 3q\sqrt{-3})$ up to a third power in $\mathbb{Q}(\varepsilon)$. Hence, by Theorem 4.1 (a), we get a representation of $4(d + 3q\sqrt{-3})$ in the desired form. □

Example 3. Let K be the splitting field of the polynomial $X^3 + 3\,X^2 - 88\,X - 25$ over $\mathbb{Q}$. First we transform the polynomial to a trinomial using the standard transformation $X \mapsto X - 1$. We get $\varphi(X) = X^3 - 91\,X + 65$. We check that $\Delta(\varphi) = 1073^2 = d^2$, so K is a cubic Galois field over $\mathbb{Q}$. What is its invariant and the canonical polynomial? Using Proposition 4.4 and the equality $\sqrt{-3} = 2\varepsilon+1$, we find $4(d+3q\sqrt{-3}) = 4(1703+195\sqrt{-3}) = 8\cdot 13(73+15\varepsilon) = -8\cdot(4+3\varepsilon)(1-3\varepsilon)^2(1-2\varepsilon)^3$. Since $\mathrm{Nr}(4+3\varepsilon) = 13$, we get $f = 4 + 3\varepsilon$. Thus the canonical polynomial (2) is $X^3 - 39X - 65$.

Corollary 4.1. *If a cubic Galois field K with invariant f is a splitting field of $X^3 - pX + q$, then $\mathrm{Nr}(f) \mid p$.*

Proof. By Proposition 4.4, we have $4(d + 3q\sqrt{-3}) = f\bar{f}^2h^3$, where h is an integer in K. Hence $64p^3 = 4 \cdot 16(d^2 + 27q^2) = \mathrm{Nr}(f)^3\,\mathrm{Nr}(h)^3$. Since f is a unit or f is a product of different split Eisenstein primes in $\mathbb{Z}[\varepsilon]$, the norm $\mathrm{Nr}(f)$ is either 1 or a product of different prime numbers congruent to 1 modulo 3. Thus $\mathrm{Nr}(f) \mid p$. □

5 Minimal canonical polynomials

As we already know, the cubic Galois fields cannot be described by binomials, so the next "simple" choice were trinomials $X^3 - pX + q$. Using the canonical trinomials given by Theorem 4.1, we get a solution of our problem, but one can ask whether there are polynomials with smaller integer coefficients, which have the same splitting field. In the present section, we adress this problem and characterize the minimal canonical polynomials having the smallest possible value of the coefficient of X. It appears (see Theorem 5.1) that the polynomial (2) corresponding to f is already minimal in this sense unless its reduced discriminant is divisible by 27. We shall prove that every cyclic cubic extension K of $\mathbb{Q}$ is a splitting field of exactly one cubic polynomial $X^3 - pX - q$ for which $p, q > 0$ and p is minimal. This cubic polynomial will be called **minimal canonical** for K and it is given in the following way:

Theorem 5.1. *Let K be a cubic Galois extension of $\mathbb{Q}$ with the invariant $f = a + b\varepsilon$. Then K has the minimal canonical polynomial $\varphi(X)$ given by (2) if and only if $27 \nmid \delta(\varphi)$, and by $X^3 - \mathrm{Nr}(f)X - \frac{1}{27}\delta(\varphi)$ when $27 \mid \delta(\varphi)$. Moreover, these two cases are equivalent to $3 \nmid b$ and $3 \mid b$, respectively, and the minimal canonical polynomial in the second case is equal $X^3 - \mathrm{Nr}(f)X - \frac{1}{3}\,\mathrm{Nr}(f)b$.*

In order to prove this, we need some auxiliary notions and results. Let K be a cubic Galois extension of $\mathbb{Q}$ with Galois group G and denote by $\mathcal{I}(K)$ the ring of integers in K. We shall denote by $\mathcal{I}(K)_0$ the integers whose trace equals to 0. It is clear that $\mathcal{I}(K)_0$ is an abelian group (a $\mathbb{Z}$-module) of rank 2 as a lattice on the kernel of the linear map $\mathrm{Tr} : K \to \mathbb{Q}$, which has dimension 2 over the rational numbers. If σ is an automorphism of K and $x \in K$ is an integer with trace equal to 0, then also $\sigma(x)$ is an integer in K and has trace equal to 0. Thus, the abelian group $\mathcal{I}(K)_0$ is a G-module of rank 2 over $\mathbb{Z}$. The ideals I in the ring $\mathbb{Z}[\varepsilon]$ can be also considered

as G-modules if $\sigma \cdot \alpha = \varepsilon\alpha$ for $\alpha \in I$. It is well-known that $\mathcal{I}(K)_0$ as a G-module is isomorphic to an ideal in $\mathbb{Z}[\varepsilon]$ as a G-module (see [CR], (74.3), p.508).

An element $a + b\sigma$ of $\mathbb{Z}[G]$ acts on $\alpha \in I$ by $(a + b\sigma) \cdot \alpha = (a + b\varepsilon)\alpha$. Since, as a consequence of the unique factorization of the Eisenstein integers, every element of I is a multiple $(a + b\varepsilon)\alpha_0$, where α_0 is a generator of I as an ideal in $\mathbb{Z}[\varepsilon]$, an isomorphism of I with $\mathcal{I}(K)_0$ maps such a product onto $(a+b\sigma)\cdot x_0 = ax_0+b\sigma(x_0)$, where x_0 is an image of α_0. Hence $\mathcal{I}(K)_0$ is generated by x_0 as a module over $\mathbb{Z}[\varepsilon]$ when its structure as such a module is defined by $(a + b\varepsilon) \cdot x = ax + b\sigma(x)$ for $x \in \mathcal{I}(K)_0$ (observe that x_0 is also a generator of $\mathcal{I}(K)_0$ as a G-module, since $\sigma^2(x_0) = -x_0 - \sigma(x_0)$). Notice that $\mathcal{I}(K)_0$, as every non-zero ideal in $\mathbb{Z}[\varepsilon]$, has 6 different generators.

Lemma 5.1. *Let x_1, x_2, x_3 be the zeros of $X^3 - pX - q$ and let $4\,p^3 - 27\,q^2 = d^2$. Then, with a suitable choice of the sign of d and arbitrary a, b, the numbers $ax_1 + bx_2, ax_2 + bx_3, ax_3 + bx_1$ satisfy the equation $X^3 - P(a, b)X - Q(a, b) = 0$, where*

$$P(a, b) = p(a^2 - ab + b^2),$$

$$Q(a, b) = qa^3 + \frac{d - 3q}{2}a^2b - \frac{d + 3q}{2}ab^2 + qb^3$$

Proof. We have

$$\pm d = (x_1-x_2)(x_2-x_3)(x_3-x_1) = (x_1-x_2)(x_1+2x_2)(2x_1+x_2) = 2x_1^3+3x_1^2x_2-3x_1x_2^2-2x_2^3,$$

and

$$q = x_1x_2x_3 = -x_1x_2(x_1 + x_2) = -x_1^2x_2 - x_1x_2^2.$$

The numbers ax_1+bx_2, ax_2+bx_3 and ax_3+bx_1 satisfy an equation $X^3-P(a,b)X-Q(a,b) = 0$, where the coefficient $P(a, b)$ is the sum of 3 products of two of these numbers. Taking into account that $x_3 = -x_1 - x_2$, we easily get the equality $P(a, b) = p(a^2 - ab + b^2)$.

The coefficient $Q(a, b)$ is the product of these 3 numbers. The coefficients of a^3 and b^3 are the products $x_1x_2x_3 = q$. The coefficient of a^2b is $x_1^2x_2 + x_2^2x_3 + x_3^2x_1 = x_1^3 + 3x_1^2x_2 - x_2^3$, and ab^2 is $x_1^2x_3 + x_3^2x_2 + x_2^2x_1 = x_1^3 + 3x_1x_2^2 - x_2^3$. Choosing $d = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$, we get that the first is $(d - 3q)/2$ and the second $-(d + 3q)/2$. □

Remark 5.1. Let $X^3 - pX - q$ be given, where $4p^3 - 27q^2 = d^2$ and choose $a = 1, b = -\varepsilon$ in Lemma 5.1. Then $P(a, b) = 0$ and $Q(a, b) = \frac{d+3q}{2}+3q\varepsilon =: \alpha \in \mathbb{Z}[\varepsilon]$. If we now set $\zeta = x_1 - \varepsilon x_2$, then $\zeta^3 = \alpha$ (cf. Proposition 4.4). Furthermore, given $\zeta = \sqrt[3]{\alpha}$ (a fixed value), we can recapture x_i $(i = 1, 2, 3)$ and thus get the Cardano formulas for the solutions of a cubic equation. In fact, since x_1, x_2 are real, we have $\bar{\zeta} = x_1 + (1 + \varepsilon)x_2$, so $\bar{\zeta} - \zeta = (1 + 2\varepsilon)x_2$, which gives $x_2 = \frac{\bar{\zeta}-\zeta}{\sqrt{-3}}$ and x_1, x_3 can be easily computed.

Remark 5.2. Let K be the cubic Galois field defined by a zero x of a polynomial $X^3 - pX - q$ and consider $\mathcal{I}(K)_0$ as a module over the Eisenstein integers. Then for $\lambda = a + b\varepsilon \in \mathbb{Z}[\varepsilon]$, the number $\lambda \cdot x = ax + b\sigma(x)$ is a zero of the polynomial $X^3 - P(a,b)X - Q(a,b)$, where $P(a,b) = \mathrm{Nr}(\lambda)p$ and $Q(a,b) = 2\Re(\lambda^3\alpha_0)$ and $\alpha_0 = \frac{9q-d-2d\varepsilon}{18}$. This follows from $\alpha_0 = -\frac{1+2\varepsilon}{9}\alpha$, where α is defined in Remark 5.1 (cf. also Remark 5.3).

Proposition 5.1. *Let K be a cubic Galois field over $\mathbb{Q}$. Then K has the minimal canonical polynomial, which can be defined as the minimal polynomial of a suitable generator of $\mathcal{I}(K)_0$ as a $\mathbb{Z}[\varepsilon]$-module. If $X^3 - pX - q$ is the minimal canonical polynomial of K, then its zeros are 3 generators $\mathcal{I}(K)_0$, while the remaining 3 generators satisfy the equation $X^3 - pX + q = 0$. Moreover, for any polynomial $X^3 - p'X + q'$ with $p', q' \in \mathbb{Z}$ having K as its splitting field, we have $p \mid p'$.*

Proof. Let x_0 be a generator of $\mathcal{I}(K)_0$ as $\mathbb{Z}[\varepsilon]$-module and let $X^3 - pX - q$ be its minimal polynomial. We have $p > 0$, since $4\,p^3 - 27\,q^2 = d^2$ and we can assume that $q > 0$, since $-x_0$ is also a generator and satisfies the equation $X^3 - pX + q = 0$. Now let x_0' be another generator of the $\mathbb{Z}[\varepsilon]$-module $\mathcal{I}(K)_0$. Then $x_0' = ax_0 + b\sigma(x_0)$, where $a, b \in \mathbb{Z}$. Let x_0' be a zero of the polynomial $X^3 - p'X - q'$. As before, we may assume that $q' > 0$. According to Lemma 5.1, we have $p' = (a^2 - ab + b^2)p$, that is, $p \mid p'$. By symmetry, we have also $p' \mid p$, so $p' = p$. Moreover, we have $a^2 - ab + b^2 = 1$, where a, b are integers. Thus, we get six possibilities corresponding to the six units in the ring $\mathbb{Z}[\varepsilon]$: $(a,b) = (\pm 1, 0), (0, \pm 1), (1,1), (-1,-1)$. Using again Lemma 5.1, this time for the free coefficients of the cubic polynomials, we get $q' = q$. Thus the generators of $\mathcal{I}(K)_0$ satisfy one of the equations $X^3 - pX \pm q = 0$. Moreover, the arguments above show that if $X^3 - pX - q'$ is any integer polynomial whose splitting field is equal K and $q' > 0$, then $q' = q$.

Let now $X^3 - p'X + q'$, where $p', q' \in \mathbb{Z}$, be any polynomial whose splitting field is equal K and x' some of its zeros. Then $x' = ax_0 + b\sigma(x_0)$ for some integers a, b. By Lemma 5.1, we have $p \mid p'$, so p is really the least value of the coefficients of x in polynomials having K as its splitting field and it divides the corresponding coefficient of X in any trinomial of this type which splits in K. □

Proof of Theorem 5.1. Let $X^3 - pX + q$ be the minimal canonical polynomial of a cubic Galois extension K of $\mathbb{Q}$ with the invariant f. According to Corollary 4.1, Proposition 5.1 and Theorem 4.1, we have $\mathrm{Nr}(f) \mid p$ and $p \mid 3\,\mathrm{Nr}(f)$. Hence $p = 3\,\mathrm{Nr}(f)$ or $p = \mathrm{Nr}(f)$, since $\mathrm{Nr}(f)$ is a product of different prime numbers or $\mathrm{Nr}(f) = 1$. If $p = 3\,\mathrm{Nr}(f)$, then the polynomial (2) is up to the sign of the free term, the minimal canonical polynomial of K.

Assume that $p = \mathrm{Nr}(f)$ and let x denote a zero of the polynomial (2). According to Lemma 5.1, equation (2) implies $3\,\mathrm{Nr}(f) = (a^2 - ab + b^2)\,\mathrm{Nr}(f)$ for some integers a, b such that $x = ax_0 + b\sigma(x_0)$, where x_0 is a zero of the minimal canonical polynomial of K. Hence, we have $a^2 - ab + b^2 = 3$. The last equation has 6 solutions: $(a,b) = \pm(1,-1), \pm(1,2), \pm(2,1)$. Taking into account $x = ax_0 + b\sigma(x_0)$, we have

$$\sigma(x) = a\sigma(x_0) + b\sigma^2(x_0) = a\sigma(x_0) - b(x_0 + \sigma(x_0)) = (a-b)\sigma(x_0) - bx_0,$$

and solving the system of these two equations, we get

$$x_0 = \frac{(a-b)x - b\sigma(x)}{a^2 - ab + b^2} = \frac{1}{3}\left((a-b)x - b\sigma(x)\right).$$

An uncomplicated computation (most conveniently using, for example, Maple), shows that such an x_0 is a zero of one of the equations $X^3 - \mathrm{Nr}(f)X \pm \frac{d}{27}$ (the choice of sign depends on the choice of a, b). This can happen if and only if $27 \mid d$.

Since

$$d^2 = 4\,p^3 - 27\,q^2 = 4\cdot 27\,\mathrm{Nr}(f)^3 - 27\,\mathrm{Tr}(f)^2\,\mathrm{Nr}(f)^2 = 27\,\mathrm{Nr}(f)^2\left(4\,\mathrm{Nr}(f) - \mathrm{Tr}(f)^2\right),$$

we have $27 \mid d$ if and only if 27 divides the last factor. An easy computation gives $4\,\mathrm{Nr}(f) - \mathrm{Tr}(f)^2 = 3b^2$, which is divisible by 27 if and only if $3 \mid b$. □

Remark 5.3. Let (p, q, d) denote the coefficients and the square root of the discriminant of the polynomial $X^3 - pX - q$. Choose $a = 2, b = 1$ in Lemma 5.1. Then $P(a, b) = 3p, Q(a, b) = d$ and $(3p, d, 27q)$ is the triple corresponding to the polynomial $X^3 - 3pX - 27q$. Notice that if we have $4p^3 = 27q^2 + d^2$ and multiply by 27, we get $4(3p)^3 = (27q)^2 + 27d^2$, so d and q "change places". This explains the relation between these two polynomials (in fact, $(2+\varepsilon)^2 = -3$ up to a unit, so if we do the transformation twice, we get $(9p, 27q, 27d)$). Notice also that if the first polynomial is minimal canonical, then the second is the one given by (2).

As we know, there are $3 \cdot 2^{k-1}$ non-isomorphic cubic Galois fields over $\mathbb{Q}$ for which the norm of the invariant is a product of k primes. For one third of the corresponding canonical polynomials (2), the minimal canonical polynomial is different:

Proposition 5.2. *There exist 2^{k-1} non-isomorphic cubic Galois fields for which the norm of the invariant is a product of k fixed primes and the minimal canonical polynomial is not equal to the canonical polynomial.*

Proof. Let K be a cubic Galois field over $\mathbb{Q}$ and let the norm of its invariant f be a product of k Eisenstein primes. The numbers εf and $\varepsilon^2 f$ have the same norm and it is easy to check using Proposition 3.1 and Theorem 4.1 that they define non-isomorphic cubic Galois fields, which both are non-isomorphic to the field defined by f. Now we prove that for exactly one of the invariants $f, \varepsilon f, \varepsilon^2 f$, the reduced discriminant is divisible by 27, that is, the minimal canonical and the canonical polynomial are not equal. Of course, this will prove the Proposition.

Let $f = a + b\varepsilon$. Then $\varepsilon f = -b + (a-b)\varepsilon$ and $\varepsilon^2 f = (b-a) - a\varepsilon$. Now $\mathrm{Nr}(f) = a^2 - ab + b^2 = 1 \pmod 3$ says that either exactly one of a, b is divisible by 3 or a, b give the same residue modulo 3. In any of these cases, exactly one of the coefficients $a, b, a-b$ is divisible by 3. By last part of Theorem 5.1 this proves our claim concerning the numbers $f, \varepsilon f, \varepsilon^2 f$. □

Example 4. We continue the previous Example 3. We obtained there the canonical polynomial $X^3 - 39X - 65$ corresponding to the polynomial $X^3 - 91X + 65$. Since $f = 4+3\varepsilon$, we get according to Theorem 5.1 that the minimal canonical polynomial is $X^3 - 13X - 13$.

It is not difficult to construct a list of cubic Galois fields over the rational numbers in terms of their invariants and the minimal canonical polynomials using Theorems 4.1 and 5.1. On the inside of the back cover you can find a table of all cases with $\mathrm{Nr}(f) \leq 100$.

6 Sieving cyclic Galois fields

In this section, we show how to list non-isomorphic cubic Galois fields using a sieving process similar to the sieve of Eratosthenes applied to the sequence of all cubic traceless trinomials defining such fields. In order to introduce this method, let us start with a similar task for (real) quadratic fields. Every such field is a splitting field of a quadratic polynomial $X^2 - q$ with $q > 0$. Of course, the splitting field of such a polynomial is quadratic if and only if q is not a square. Two quadratic number fields (subfields of the complex numbers) are isomorphic if and only if they are equal, so we want to know when $X^2 - q$ and $X^2 - q'$ define the same field. We start listing the sequence of all non-square integers (binomials $X^2 - q$) up to any given limit, starting with the least one, that is, the number 2. This number defines our first quadratic field $\mathbb{Q}(\sqrt{2})$. Now we mark all integers in the sequence which define the same field, that is, the numbers $2a^2$ for integers $a > 1$ (or polynomials $X^2 - 2a^2$). The next unmarked number is 3. Thus the next field is $\mathbb{Q}(\sqrt{3})$ and we mark all the numbers $3a^2$ with $a > 1$. The next number is 5 and so on. We get the sequence $2, 3, 5, 6, 7, 10, 11, 13, 14, \ldots$. The polynomials (or the integers), which remain on our list unmarked give non-isomorphic quadratic fields and have the least possible value of q among the binomials having the same splitting field as $X^2 - q$. Of course, our sequence is the sequence of all square-free integers – those which are marked are exactly multiples of the square-free integers by a square $\neq 1$. We describe this process in detail in order to show that a similar sieving procedure can be used in order to get all cubic Galois fields.

First we note that two cubic Galois fields over $\mathbb{Q}$ (contained in the complex numbers) are also isomorphic if and only if they are equal – this is a general property of Galois fields. Hence we want to list all different cubic Galois fields. Every such field is a splitting field of an irreducible cubic polynomial $X^3 - pX + q$, where p, q are positive integers and the discriminant is a square, that is, $4p^3 - 27q^2 = d^2$ for an integer d. We can write down the sequence of all such polynomials starting with the least possible p (in fact, $p = 3$) and then for each fixed p, we can list all irreducible polynomials with q in increasing order – since $27q^2 < 4p^2$, the number of such polynomials is finite. Identifying the polynomials with the pairs of their coefficients (p, q), the beginning of the sequence is $(3, 1), (7, 7), (9, 9), (12, 8), (13, 13), (19, 19), (21, 7), \ldots$. We start with the first polynomial, which defines the "least" cubic Galois field – the splitting field of $X^3 - 3X + 1$ given by the pair $(3, 1)$. According to Lemma 5.1, we

have to mark on our list all polynomials corresponding to $(P(a,b),Q(a,b))$, where $P(a,b)=3(a^2-ab+b^2)$, $Q(a,b)=a^3+3a^2b-6ab^2+b^3$, $a,b\in\mathbb{Z}$, since they define the same field as $(3,1)$. The next pair is $(7,7)$ and in practise, we check whether it is marked by solving $P(a,b)=7, Q(a,b)=7$. It is unmarked, so it defines a new field – the splitting field of X^3-7X+7. Now we mark all the pairs, which give polynomials defining the same field as this polynomial according to Lemma 5.1, but in practise, we check whether a pair is marked when we know the status of all earlier pairs. For example, the next pair is $(9,9)$ and we check that this pair is marked because of the pair $(3,1)$ as the corresponding system $P(a,b)=9$, $Q(a,b)=9$ has a solution $a=-1, b=1$. Hence, we mark this polynomial. The same can be said about $(12,8)$, but the next pair $(13,13)$ is not represented as $P(a,b),Q(a,b)$ neither for $(3,1)$ or $(7,7)$, so it gives a new field. We continue the algorithm in this way. The polynomials, which are unmarked on our list give different cubic Galois fields and have the least possible coefficients among the trinomials having the same splitting field. Thus, they are the minimal canonical polynomials defining these fields.

The reason this works is, because as remarked before Lemma 5.1, the traceless integral elements of a cubic Galois field form a rank one module over $\mathbb{Z}[\varepsilon]$, which is generated (up to a unit) by an element x_0. The polynomial corresponding to x_0 is the original unmarked polynomial (the minimal canonical), and furthermore all "multiples" of the minimal canonical polynomials form a partition of all cubic (traceless) polynomials, i.e. they never meet unless they coincide. Finally the process works even if we are not able to mark all the infinite number of "multiplies". Say that we are only interested in (p,q) such that $p\leq P_0$ with P_0 given in advance. We then look at the finite number of pairs (a,b) such that the corresponding $p(a,b)\leq P_0$ and restrict our marking to those. What is left unmarked remains unmarked no matter how many more (a,b) we will consider. This process can be easily implemented on a computer and on the inside of the back cover you can find a table presenting the beginning of a run.

Referenser

[C] H. Cohen, A Course in Computational Algebraic Number Theory, GTM 138, Springer-Verlag, New York, Heidelberg, Berlin, 1993.

[CR] C. W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, AMS, Chelsea Publishing, Providence, Rhode Island, 1962.

[IR] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, GTM 84, Springer-Verlag, New York, Heidelberg, Berlin, 1990.

[L] S. Lang, Algebra, GTM 211, Springer-Verlag, New York, Heidelberg, Berlin, 2002.