What you should know about cubic and quartic equations

Juliusz Brzeziński

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

1 *Introduction*

Polynomial algebraic equations of low degrees in the context of their Galois groups are discussed in many places. A very long time ago, the supervisor of my Master Thesis, the great logician, professor Andrzej Mostowski urged me to write a text concerning this topic in order to answer several questions from the students attending his class on Galois theory in which I was a teaching assistant. The idea was to give a straightforward, simple and direct description suitable for undergraduates. I eagerly accepted my first serious pedagogical mission. The text, far from perfect, appeared in Polish in [B]. During the years which followed, I taught Galois theory several times and very often was asked similar questions as during my first teaching task. I often xeroxed a table summarizing all cases from my paper (correcting some printing errors in it), but I couldn't give a simple and easily accessible reference explaining the results. Now there are many sources which could be recommended, notably [C], and several others. But in spite of the fact that there exist different presentations of this topic, it seems that there are many people who are in one way or another dissatisfied with the existing texts. So here is one more with the hope that simplicity of the formulations and arguments will give a useful pedagogical reference.

We intend to work over an arbitrary field K of characteristic 0, but one can think of K as any number field[1], e.g. the field of rational numbers $\mathbb{Q}$. We shall study particular polynomial equations $f(x) = 0$ with coefficients in K. The set of all such polynomials $f(x)$ will be denoted, as usual, by $K[x]$.

Let $f(x) \in K[x]$ be a polynomial of degree n and let $\alpha_1, \alpha_2, \dots, \alpha_n$ denote the solutions of the equation $f(x) = 0$ in a field containing the field K. If the polynomial has number coefficients, we can take the complex numbers as such a field containing K. However, if K is an arbitrary field, we can fix a field $\overline{K}$ containing K in which

[1] The results are exactly the same when K is an arbitrary field whose characteristic is neither 2 or 3, but one has to be a little more cautious with formulations assuming only this.

every polynomial over K can be factorized into a product of linear factors, that is, for every polynomial $f(x)$ of degree n with coefficients in K, there exist $\alpha_1, \ldots, \alpha_n \in \overline{K}$ such that $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$, where $a \in K$. For a proof of existence of such a field, see [L], p. 231.

The **splitting field** of a polynomial $f(x)$ over K is the field $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, which is the least set obtained from the elements of K and the solutions $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $f(x) = 0$ in $\overline{K}$ by means of the four arithmetical operations (addition, subtraction, multiplication and division). Sometimes, this field will be denoted by K_f.

Solving the polynomial equations or describing their Galois groups over a field K, we shall often assume that the polynomials (of degree at least 2), which we discuss, are **irreducible**, that is, can not be represented as a product of two nonconstant polynomials of lower degrees with coefficients in K. In practice, it is a natural assumption if we know how to handle the polynomials of degrees lower than the degree of $f(x)$, since a nonconstant reducible polynomial is a product of two polynomials of lower degrees. The simplest possibility is that $f(x)$ has a zero $\alpha \in K$. Then, of course, $f(x) = (x-\alpha)f_1(x)$, where $f_1(x) \in K[x]$ has the degree one lower than the degree of $f(x)$. A polynomial is called **separable** if its zeros are different. We shall always assume that irreducible polynomials have this property. This is the case over the fields of characteristic 0 (like the number fields) and over the finite fields.

If $f(x) \in K[x]$ is a polynomial with coefficients in K, then its Galois group (one may say, the Galois group of the equation $f(x) = 0$) is the automorphism group of the splitting field K_f over K. This group will be denoted by $G(K_f/K)$. If $\sigma \in G(K_f/K)$, then

$$\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta), \quad \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) \quad \text{and} \quad \sigma(a) = a$$

for any $\alpha, \beta \in K_f$ and $a \in K$. Hence $\sigma(g(\alpha)) = g(\sigma(\alpha))$ for every polynomial $g \in K[x]$ and every $\alpha \in K_f$. In particular, we have $\sigma(f(\alpha_i)) = f(\sigma(\alpha_i)) = 0$ for $i = 1, 2, \ldots, n$, so $\sigma(\alpha_i)$ is also a solution of the equation $f(x) = 0$ (notice that $\sigma(0) = 0$). Therefore, an automorphism σ gives a permutation of the zeros α_i of $f(x) = 0$. Such a permutation defines uniquely the effect of σ on all the elements of K_f. When we have fixed a numbering of the zeros of $f(x)$, then every automorphism σ gives a permutation: to $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ corresponds the permutation mapping i onto $\sigma(i)$ for $i = 1, 2, \ldots, n$. Usually, we shall identify the permutation of the α_i with the permutation of their indices i and we shall consider the corresponding permutation group as the Galois group of the polynomial $f(x)$. One of the main results of Galois theory is a one-to-one correspondence between the subgroups of the Galois group $G(K_f/K)$ and the subfields of K_f containing K: If H is a subgroup of $G(K_f/K)$ then the corresponding subfield consists of all $\alpha \in K_f$ for which $\sigma(\alpha) = \alpha$ for each $\sigma \in H$. Conversely, to a subfield L of K_f containing K corresponds the subgroup consisting of all $\sigma \in G(K_f/K)$ for which $\sigma(\alpha) = \alpha$ for each $\alpha \in L$ (the Galois group $G(K_f/L)$).

As a permutation group, the Galois group $G(K_f/K)$ of a polynomial $f(x)$ of degree n is a subgroup of the symmetric group S_n consisting of all permutations of the numbers $1, 2, \ldots, n$. As we know, the group S_n has $n!$ elements. For every particular polynomial $f(x)$ of degree n, we get a particular subgroup of S_n. A description of these subgroups for arbitrary polynomials is not easy (and in full generality, probably, impossible), but for polynomials of law degrees, in particular, for cubic and quartic polynomials, the task is not too difficult and its solution is the main purpose of this text. Of course, it is necessary to identify different subgroups of S_3 and S_4 in order to identify different cases. Such a discussion of S_3 and S_4 is given in the Appendix.

Let $f(x)$ be a polynomial of degree n over K with splitting field K_f. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be all zeros of $f(x)$ in K_f. The **discriminant** of $f(x)$ is defined as the product

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \tag{1}$$

Rudimentary Galois theory says that an element of the splitting field K_f belongs to K if and only if it is fixed by all automorphism belonging to the Galois group $G(K_f/K)$. Therefore $\Delta(f)$ must be in K, since, evidently, it is fixed by all possible permutations of α_i, $i = 1, 2, \ldots, n$. In fact, it is always possible to express the discriminant as a polynomial of the coefficients of $f(x)$ (see below such formulae for polynomials of degrees ≤ 4 and the comments on checking their validity in the next section – see 2.1).

After these introductory remarks, we look at the cases, which we want to discuss – the cubic and quartic polynomials.

A general cubic polynomial can be written in the form $a_3x^3 + a_2x^2 + a_1x + a_0$, where $a_i \in K$ and $a_3 \neq 0$. Dividing by a_3, we get a polynomial with the same zeros, so we can always assume that $a_3 = 1$. It is also very easy to achieve $a_2 = 0$. In fact, if already $a_3 = 1$, we can always choose y, such that $x = y - \frac{a_2}{3}$. Substituting this x gives an equation in which the coefficient of y^2 is 0. Thus, we shall only consider cubic equations:

$$f(x) = x^3 + px + q = 0, \tag{2}$$

with $p, q \in K$. How to solve arbitrary cubic equations in general case is presented in Section 2 (see 2.11). If the given cubic polynomial $f(x)$ is reducible, that is, it can be factorized as a product of a linear and a quadratic factor over K, then it is easy to solve the equation $f(x) = 0$ and to find the Galois group $G(K_f/K)$. We discuss in Section 2 (see 2.4) how to decide whether $f(x)$ is reducible or not. Now we describe the Galois groups of irreducible cubic polynomials. They are subgroups of the permutation group S_3 of all permutations of its 3 zeros and are given in the following simple way (for a proof see 2.11 and 2.1 for the discriminant formula):

Theorem 1.1. *Let $f(x) = x^3 + px + q \in K[x]$ be an irreducible polynomial of degree 3 and let $\Delta = \Delta(f) = -4p^3 - 27q^2$. Then*

$$G(K_f/K) = \begin{cases} S_3 & when \quad \sqrt{\Delta} \notin K, \\ A_3 & when \quad \sqrt{\Delta} \in K. \end{cases}$$

A general quartic equation has a shape $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$, where $a_i \in K$ and $a_0 \neq 0$. As for the cubics, we may divide by a_4 and assuming $a_4 = 1$, we achieve $a_3 = 0$ substituting this time $x = y - \frac{a_3}{4}$. This gives an equation in which the coefficient of y^3 is 0. Thus, we shall only consider equations:

$$f(x) = x^4 + px^2 + qx + r = 0, \tag{3}$$

with $p, q, r \in K$.

How to solve a general quartic equation, we discuss in 2.12. Studying the Galois group in this case, like in the case of cubics, first of all we would like to know whether the equation has a solution in K. If so, then we essentially have to handle a cubic equation when we want to solve (3) or to determine its Galois group, since $f(x)$ is then a product of a linear and a cubic factor over K. For a discussion how to decide whether $f(x) = 0$ has a solution in K see 2.4.

Thus, in principle, the problem is reduced to the case when a quartic polynomial does not have zeros in K, so it can not be factored as a product of a first degree polynomial and a cubic polynomial. But it may be possible to factor $f(x)$ as a product of two quadratic polynomials. In fact, studying possibility to factorize a quartic polynomial as a product of two quadratic polynomials is not only a key to a solution of the equation $f(x) = 0$, but also to the description of its Galois group. So let us consider a factorization

$$x^4 + px^2 + qx + r = (x^2 + ax + b)(x^2 + a'x + b'), \tag{4}$$

where a, b, a', b' may belong to a field containing K. Compering the coefficient for x^3 to the right and to the left, we see immediately that $a + a' = 0$, so $a' = -a$. Then compering the remaining coefficients, we get the system

$$\begin{aligned} b + b' &= a^2 + p, \\ a(b' - b) &= q, \\ bb' &= r. \end{aligned} \tag{5}$$

Multiply the first equation by a, then square the first two equations and finally subtract the second from the first! We get

$$4a^2bb' = a^2(a^2 + p)^2 - q^2.$$

Replacing bb' from the last equation gives our final result:

$$a^6 + 2pa^4 + (p^2 - 4r)a^2 - q^2 = 0.$$

The polynomial

$$r(f)(t) = t^3 + 2pt^2 + (p^2 - 4r)t - q^2 \tag{6}$$

is called **the resolvent of** $f(x)$. One of its zeros is $t = a^2$. In general, the resolvent is responsible for the possibility to split $f(x)$ into a product of two quadratic polynomials. We can formulate this as follows in a special case when we urge that the factorization is already over K:

Proposition 1.1. *Let $f(x) = x^4+px^2+qx+r$ be a polynomial with coefficients in a field K without zeros in K. Then f is reducible in K (a product of two quadratic polynomials with coefficients in K) if and only if*

(a) $q \neq 0$ and the resolvent $r(f)$ has a zero, which is a square in K,

or

(b) $q = 0$ and the resolvent $r(f)$ has two zeros, which are squares in K or $\delta = p^2-4r$ is a square in K.

For a proof see 2.5.

Remark 1.1. Notice that the case (b) is concerned with the biquadratic polynomials. Notice also that $q = 0$ if and only if the resolvent $r(f)(t) = t^3 + 2pt^2 + (p^2 - 4r)t - q^2$ of $f(x) = x^4 + px^2 + qx + r = 0$ has a zero $t = 0$.

Once we know that the polynomial $f(x)$ is reducible (but without zeros in K), we can easily describe its Galois group (see 2.9):

Theorem 1.2. *Let $f(x) = x^4 + px^2 + qx + r$ be reducible in K but without zeros in K. Then*

$$G(K_F/K) = \begin{cases} V_4 & \textit{when} \quad r(f) \textit{ has only one zero in } K, \\ C_2 & \textit{when} \quad r(f) \textit{ has all its zeros in } K. \end{cases}$$

The Galois group of an irreducible quartic is given in the following way (for a proof see 2.8 and 2.1 for the discriminant formula):

Theorem 1.3. *Let K be a field and $f(x) = x^4+px^2+qx+r \in K[x]$ an irreducible polynomial. Let*

$$r(f)(t) = t^3 + 2pt^2 + (p^2 - 4r)t - q^2$$

be the resolvent of f and

$$\Delta = \Delta(f) = \Delta(r(f)) = -4p^3q^2 - 27q^4 + 16p^4r - 128p^2r^2 + 144pq^2r + 256r^3$$

its discriminant. Let $\delta = p^2 - 4r$. Then:

$$G(K_F/K) = \begin{cases} S_4 & \textit{when} \quad r(f) \textit{ does not have zeros in } K \textit{ and } \sqrt{\Delta} \notin K, \\ A_4 & \textit{when} \quad r(f) \textit{ does not have zeros in } K \textit{ and } \sqrt{\Delta} \in K, \\ D_4 & \textit{when} \quad r(f) \textit{ has only one zero } \beta \in K \textit{ and } \sqrt{\beta\Delta} \notin K \\ & \qquad\quad \textit{if } \beta \neq 0 \textit{ or } \sqrt{\delta\Delta} \notin K \textit{ if } \beta = 0, \\ C_4 & \textit{when} \quad r(f) \textit{ has only one zero } \beta \in K \textit{ and } \sqrt{\beta\Delta} \in K \\ & \qquad\quad \textit{if } \beta \neq 0 \textit{ or } \sqrt{\delta\Delta} \in K \textit{ if } \beta = 0, \\ V_4 & \textit{when} \quad r(f) \textit{ has all its zeros in } K. \end{cases}$$

Example. Let us find the Galois group of the polynomial $f(x) = x^4 + 4x - 1$ over the rational numbers. Is the polynomial $f(x)$ reducible or irreducible over $\mathbb{Q}$? First we test possibility that $f(x)$ has a rational zero. According to 2.4, we look at the divisors of 1 (that is, ± 1) and check that $f(\pm 1) \neq 0$. Thus $f(x)$ can not be factored as a product of rational polynomials of degrees 1 and 3. Then we want to test possibility that $f(x)$ is a product of two quadratic polynomials. According to 2.5, we look at the resolvent $r(f)(x) = x^3 + 4x - 16$. Testing the divisors of 16, we find that $\beta = 2$ is the only rational zero of the resolvent and $-1 \pm i\sqrt{7}$ are the remaining two. Thus, we know that the polynomial $f(x)$ is irreducible according to 2.5, since $\sqrt{\beta} \notin \mathbb{Q}$. Now, we can use Theorem 1.3, which says that the Galois group depends on the product $\beta\Delta$, where $\Delta = -7168$. Of course, $\sqrt{\beta\Delta} \notin \mathbb{Q}$, so the Galois group of $f(x)$ is D_4. □

2 Proofs

2.1 How to compute the discriminant?

The discriminant of a polynomial $f(x)$ with coefficients in K whose all zeros are $\alpha_1, \ldots, \alpha_n$ (in some field $\overline{K}$ containing K) was defined as

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \qquad (7)$$

If $f(x) = x^2 + px + q$, then

$$\Delta(f) = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = p^2 - 4q,$$

since $\alpha_1 + \alpha_2 == -p$ and $\alpha_1\alpha_2 = q$.

If $f(x) = x^3 + px + q$, then similar, but much more complicated, computations show that

$$\Delta(f) = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 = -4p^3 - 27q^2$$

taking into account the Vietâ formulae $\alpha_1 + \alpha_2 + \alpha_3 = 0$, $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = p$, $\alpha_1\alpha_2\alpha_3 = -q$.

Still more complicated is a computation showing that for $f(x) = x^4 + px^2 + qx + r$,

$$\Delta(f) = \prod_{1\leq i<j\leq 4} (\alpha_i - \alpha_j)^2 = -4p^3q^2 - 27q^4 + 16p^4r - 128p^2r^2 + 144pq^2r + 256r^3.$$

A detailed computation in the case of cubic equations can be found in [N], p. 188. More general considerations and formulae, which explain very well the notion of discriminant and a method, which gives a possibility to express it by means of the coefficients of the equation, can be found in [T], pp. 167–170. Today, it is easy to use different symbolic computer packages like Maple, Pari or Mathematica in order to get these formulae and compute discriminants of many other interesting polynomials. However, those given above is all what we need in order to find Galois groups in particular cases and we only need the definition of the discriminant together with its fundamental property in Proposition 2.1 in order to prove all results on Galois groups in this text.

2.2 What is the role of the discriminant?

First of all, the discriminant of a polynomial tells us whether its zeros are different. This follows from the very definition (7), which easily implies that $\Delta(f) \neq 0$ if and only if all the zeros of $f(x)$ are different. The following property of the discriminant is very important in applications related the the study of the Galois groups of polynomials:

Proposition 2.1. *Let $\Delta = \Delta(f)$ be the discriminant of the polynomial $f(x)$. Then $\sqrt{\Delta} \in K$ if and only if all permutations in $G(K_f/K)$ are even.*

Proof. By the definition (7), we have $\sqrt{\Delta} \in K_f$. If there is an odd permutation in the Galois group $G(K_f/K)$, then it acts on $\sqrt{\Delta} \in K_f$ by the change of its sign, so $\sqrt{\Delta}$ can not be in K. If all permutations in the Galois group $G(K_f/K)$ are even, then $\sqrt{\Delta} \in K_f$ is mapped on itself by all off them. Hence, we have $\sqrt{\Delta} \in K$. □

2.3 The resolvent of a quartic – some properties

Lemma 2.1. *If $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are all the zeros of a quartic polynomial $f(x)$ (in a field $\overline{K} \supseteq K$), then $\beta_1 = (\alpha_1 + \alpha_4)^2, \beta_2 = (\alpha_2 + \alpha_4)^2, \beta_3 = (\alpha_3 + \alpha_4)^2$ are all the zeros of its resolvent.*

Proof. As we noted before, depending on the choice of the factorization (4), the zeros of the first factor can be taken as α_1, α_4 or α_2, α_4 or α_3, α_4. Hence $a = -(\alpha_i + \alpha_4)$ for $i = 1, 2, 3$ and the corresponding zero a^2 of $r(f)$ is one of the β_i. □

Notice that the relation $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ shows that the particular role of α_4 in the notations is not essential – the numbers β_i do not change if we replace α_4 by any other solution of $f(x) = 0$.

Lemma 2.2. *The discriminants of the polynomials f and $r(f)$ are equal. In particular, if a quartic polynomial $f(x)$ is separable, then its resolvent $r(f)(x)$ is also separable.*

Proof. With the notations as in Lemma 2.1, we have

$$\Delta(r(f)) = (\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_3 - \beta_1)^2 =$$

$$(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_4)^2(\alpha_2 - \alpha_3)^2(\alpha_2 - \alpha_4)^2(\alpha_3 - \alpha_1)^2(\alpha_3 - \alpha_4)^2 = \Delta(f).$$

Thus $\Delta(r(f)) \neq 0$ if and only if $\Delta(f) \neq 0$, that is, all α_i are different if and only if all β_i have this property. □

2.4 How to decide that a cubic or a quartic has a linear factor?

A cubic polynomial $f(x) = x^3 + px + q$ is reducible over a field K if and only if it has a linear factor over K. Thus reducibility means that the polynomial has a zero in K. Observe that this is not the case for polynomials of higher degree than 3. For example, $f(x) = x^4 + 4$ does not have real zeros, but $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$, that is, the polynomial is reducible over $\mathbb{R}$ as well over $\mathbb{Q}$.

If we have a polynomial with coefficients in an arbitrary field K, we do not have a general method by which we could decide whether or not the equation $f(x) = 0$ has a solution in K. The situation is somewhat easier when we have a polynomial with rational coefficients (which already gives a possibility to exemplify many results concerning Galois groups in a non-trivial way). Usually one uses an elementary result saying that if $f(x)$ is a polynomial with integer coefficients and a rational number $\alpha = a/b$, where a, b are relatively prime integers, is a solution of the equation $f(x) = 0$, then a divides $f(0)$ and b divides the highest coefficient of $f(x)$. We omit an easy proof. Thus rational solutions must be integer if the highest coefficient is 1 and all divide $f(0)$ (the “variable-free" term of $f(x)$). It is still a serious numerical problem to find all the divisors of the integer $f(0)$ (if it is big), but there is a lot of good “pedagogical" examples of Galois groups when finding the divisors of $f(0)$ does not create any problem.

2.5 How to decide that a quartic is reducible?

Proposition 2.1 answers this question as regards factorization into a product of two quadratic polynomials (the possibility of factorization as a product of a linear and a cubic polynomial is discussed above in 2.4). For convenience, we recall:

Proposition 2.1. *Let $f(x) = x^4 + px^2 + qx + r$ be a polynomial with coefficients in a field K without zeros in K. Then f is reducible in K (a product of two quadratic polynomials with coefficients in K) if and only if*

(a) $q \neq 0$ and the resolvent $r(f)$ has a zero, which is a square in K,

or

(b) $q = 0$ and the resolvent $r(f)$ has two zeros, which are squares in K or $\delta = p^2 - 4r$ is a square in K.

Proof. If f has no zeros in K and is reducible, then it must be a product of two quadratic polynomials as in (4). The computations leading from (4) to (6) clearly show that $t = a^2$ is a zero of the resolvent $r(f)$, that is, the resolvent has a zero which is a square in K.

If $q \neq 0$ and the resolvent has a zero $t = a^2$, $a \in K$, then $a \neq 0$. Using the system (5), we find $b, b' \in K$ and, consequently, a factorization of $f(x)$ as a product of two quadratic polynomials. This completes our proof of the first case (a).

In the case (b), if there is a factorization with $a = 0$ (of course, a square in K – the first zero of the resolvent, which is a square in K), then the quadratic polynomial $t^2 + pt + r$ has zeros in K, namely, $-b, -b'$, so $\delta = p^2 - 4r$ must be a square in K. Conversely, if δ is a square in K, then this quadratic polynomial has some zeros $-b, -b'$ and we get a factorization of $f(x)$ with $a = 0$.

If in the case (b), we have a factorization with $a \neq 0$, then $t = a^2$ is a second zero of the resolvent, which is a square in K. Conversely, assume that the resolvent $r(f)$ has two zeros which are squares in K (these two may be equal to 0). We find easily that the zeros of $r(f)(t) = t^3 + 2pt^2 + (p^2 - 4r)t$ are: $\beta_1 = 0, \beta_2 = -p + 2\sqrt{r}, \beta_3 = -p - 2\sqrt{r}$ (observe that $\sqrt{r} \in K$). Of course, 0 is one of the squares. If the second is β_2, we easily check that we get a factorization of $f(x)$ in $K[x]$ noting that:

$$f(x) = x^4 + px^2 + r = (x^2 + \sqrt{r})^2 - \beta_2 x^2$$

and similarly for β_3, when β_3 is a square in K. □

We note as a corollary an observation made in the last part of the proof:

Corollary 2.1. *If $f(x) = x^4 + px^2 + r$, then 0 is always one of the zeros of the resolvent $r(f)$ and all three zeros of $r(f)$ are in K if and only if $\sqrt{r} \in K$. Moreover, the discriminant of $f(x)$ (and $r(f)(t)$) is*

$$\Delta(f) = 16r(p^2 - 4r)^2,$$

so $K(\sqrt{\Delta}) = K(\sqrt{r})$.

Proof. Use the general formulae on $\Delta(f)$ from Theorem 1.3 in the case, when $q = 0$. □

2.6 How to describe the splitting field of a quartic?

The following description of a relation between the splitting field of a quartic polynomial and the splitting field of its resolvent is the core of the presentation in this text. Denote, as before, the solutions of the equation $f(x) = x^4+px^2+qx+r = 0$ by $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, and the solutions of the resolvent $r(f)(t) = t^3+2pt^2+(p^2-4r)t-q^2 = 0$ given by Lemma 2.1, by $\beta_1, \beta_2, \beta_3$ (in some field $\overline{K}$ containing K). Then the splitting fields of these two polynomials are related in the following way:

Theorem 2.1. *The splitting field K_f over K of a quartic separable polynomial $f(x) \in K[x]$ can be obtained from the splitting field $K_{r(f)}$ of its resolvent $r(f)$ over K by adjunction of one arbitrary solution of the equation $f(x) = 0$, that is,*

$$K_f = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = K_{r(f)}(\alpha_i),$$

where $i = 1, 2, 3, 4$.

Proof. It is clear that

$$K_{r(f)}(\alpha_i) = K(\beta_1, \beta_2, \beta_3, \alpha_i) \subseteq K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = K_f.$$

In order to prove the converse inclusion, choose $i = 4$ and consider the equations:

$$f_i(x) = (x + \alpha_4)^2 - \beta_i$$

for $i = 1, 2, 3$. This quadratic polynomial has its coefficients in the field $K_{r(f)}(\alpha_4)$. Assume that $f_i(x)$ is irreducible in this field. By Lemma 2.1, it has a zero $x = \alpha_i$, which is a zero of the polynomial $f(x)$. Hence $f_i(x)$ divides $f(x)$ (as an irreducible polynomial having a common zero). Thus one more of the numbers $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ different from α_i is a zero of $f_i(x)$, say, α_j, where $j \neq i$. Then

$$f_i(\alpha_i) = f_i(\alpha_j) = 0,$$

that is,

$$(\alpha_i + \alpha_4)^2 = (\alpha_j + \alpha_4)^2$$

for $j \neq i$, which says that $\beta_i = \beta_j$ – a contradiction according to Lemma 2.2. Thus the polynomial is reducible in the field $K_{r(f)}(\alpha_4)$ and its zero α_i belongs it. This holds for $i = 1, 2, 3$ (and, of course, also for $i = 4$) and shows that also $K_f \subseteq K_{r(f)}(\alpha_4)$. Together with the converse inclusion, we get $K_f = K_{r(f)}(\alpha_4)$. □

2.7 Proof of Theorem 1.1: Galois groups of irreducible cubics

Proof. Since $f(x)$ is irreducible, the Galois group is a transitive subgroup of the symmetric group S_3, that is, it is either A_3 or S_3 (see Appendix). Hence, the splitting field K_f has degree either 3 or 6 over K. The square root of the discriminant $\sqrt{\Delta}$ is a non-zero element of K_f, since the polynomial $f(x)$ has different zeros.

If $\sqrt{\Delta} \in K$, then the Galois group must consist of even permutations, since odd permutations change the sign of $\sqrt{\Delta}$. Hence, $G(K_f/K) = A_3$ and $K_f = K(\alpha_i)$ for any zero α_i, $i = 1, 2, 3$, of $f(x)$.

If $\sqrt{\Delta} \notin K$, then the Galois group must consist of both even and odd permutations (see Proposition 2.1). Hence the Galois group must be S_3 and the degree of K_f over K is 6. □

Notice that in the second case above, the extension $K(\sqrt{\Delta})$ has degree 2 over K and $K_f = K(\sqrt{\Delta}, \alpha_i)$ for any zero α_i, $i = 1, 2, 3$, of $f(x)$. In fact, the polynomial $f(x)$ is still irreducible over $K(\sqrt{\Delta})$ (as the degree of this field over K is 2 and the degree of the irreducible over K polynomial $f(x)$ is 3 – see 2.10), so the degree of $K_f = K(\sqrt{\Delta}, \alpha_i)$ over $K(\sqrt{\Delta})$ is 3. Hence, we have the following analogue of Theorem 2.1:

Corollary 2.2. *If $f(x) \in K[x]$ is an irreducible polynomial of degree 3, then $K_f = K(\sqrt{\Delta}, \alpha_i)$, where α_i, $i = 1, 2, 3$ is any zero of $f(x)$.*

2.8 Proof of Theorem 1.3: Galois groups of irreducible quartics

Proof. We consider 3 cases:

Case 1: The resolvent $r(f)$ has not zeros in K.

This means that $r(f)$ is an irreducible cubic over K. According to Theorem 1.1, the splitting field $K_{r(f)}$ has degree 3 or 6 over K depending on the discriminant $\Delta = \Delta(r(f)) = \Delta(f)$: the first case when $\sqrt{\Delta} \in K$, and the second, when $\sqrt{\Delta} \notin K$.

If $\sqrt{\Delta} \in K$ (so the degree of $K_{r(f)}$ over K is 3), then the polynomial $f(x)$ of degree 4 is still irreducible over $K_{r(f)}$ (see 2.10). Hence the splitting field $K_f = K(\sqrt{\Delta}, \alpha_1)$, where α_1 is any zero of $f(x)$ (see 2.6), has degree 4 over $K_{r(f)}$. Thus the degree of K_f over K equals 12, which means that the Galois group $G(K_f/K)$ is a subgroup of order 12 of S_4. There is only one such subgroup (see the Appendix) and it is the alternating group A_4 of all even permutations of $1, 2, 3, 4$.

If $\sqrt{\Delta} \notin K$, then the Galois group $G(K_f/K)$ must contain both even and odd permutations according to Proposition 2.1 and its order is divisible by 6, since the splitting field K_f over K contains a subfield $K_{r(f)}$ of degree 6 over K. Moreover, the Galois group is transitive, since $f(x)$ is irreducible over K. There is only one such subgroup of S_4 and it is S_4 itself (see the Appendix concerning the claim that S_4 is the only transitive subgroup of S_4 of order divisible by 6).

Case 2: The resolvent $r(f)$ has exactly one zero $\beta = \beta_1 = (\alpha_1 + \alpha_4)^2$ in K.

First of all, let us notice that in this case, we have $\sqrt{\Delta} \notin K$. In fact, the splitting field of the resolvent $K_{r(f)} = K(\sqrt{\Delta}, \beta) = K(\sqrt{\Delta})$ must be bigger than K, since otherwise all the zeros of the resolvent are in K. Thus $\sqrt{\Delta}$ can not belong K, so the Galois group $G(K_f/K)$ must contain both even and odd permutations according to Proposition 2.1.

Which permutations of the zeros $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of $f(x) = 0$ may belong to $G(K_f/K)$? Since $\beta = \beta_1 = (\alpha_1 + \alpha_4)^2$ is in K, the permutations in $G(K_f/K)$ must fix this element. We see immediately that such permutations are all in the group:

$$D_4 = V_4 \cup \{(1,2,4,3),(1,3,4,2),(1,4),(2,3)\},$$

where

$$V_4 = \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$$

(remember that $\alpha_1 + \alpha_4 = -(\alpha_2 + \alpha_3)$ and see the Appendix concerning the notations).

All other permutations in S_4 map $\beta = \beta_1$ on different elements since $(1,2)$ maps $\beta_1 = (\alpha_1 + \alpha_4)^2$ onto β_2 and $(1,3)$ onto β_3. Thus the 16 products in the cosets $(1,2)D_4$ and $(1,3)D_4$ are different and map β_1 onto either β_2 or β_3.

Assume now that $\beta_1 \neq 0$, so $K(\sqrt{\beta}) = K(\alpha_1 + \alpha_4)$ is a quadratic extensions of K. Since the polynomial $f(x)$ is irreducible, the Galois group $G(K_f/K)$ must contain at least 4 elements. As a subgroup of D_4 it must consist of 4 or 8 permutations in D_4. The group D_4 is the square group and contains 3 subgroups of order 4 (see the Appendix on the group S_4 and its subgroups). Assume that $G(K_f/K)$ has 4 elements. It can not be the subgroup V_4, since it only has even permutations all fixing $\sqrt{\Delta}$, which however is not in K. It can not be

$$V_4' = \{(1),(1,4),(2,3),(1,4)(2,3)\},$$

(see the Appendix for the notations), since this group has $\alpha_1 + \alpha_4$ as fixed element and this is also an element not in K. Thus $G(K_f/K)$ must be the third group:

$$C_4 = \{(1),(1,2,4,3),(1,3,4,2),(1,4)(2,3)\},$$

which is cyclic. But this group only has one subgroup of order 2, so the quadratic fields $K(\sqrt{\Delta})$ and $K(\sqrt{\beta})$ (over K) must be equal, that is, $\sqrt{\beta\Delta} \in K$. If these two fields are different, that is, $\sqrt{\beta\Delta} \notin K$, it remains the only possibility that the Galois group has order 8 and consists of all permutations in D_4.

It may happen that $\beta = 0$, that is, $\alpha_1 + \alpha_4 = 0$ (and, consequently, $\alpha_2 + \alpha_3 = 0$). As we noted before (see Remark 1), it happens if and only if the polynomial $f(x)$ is biquadratic (that is, $q = 0$). Then we have to find another field extension instead of

$K(\sqrt{\beta})$, since now $K(\sqrt{\beta}) = K$. We take instead $K(\sqrt{\delta})$, since $f(x)$ is irreducible, so $\sqrt{\delta} \notin K$. Notice that

$$\delta = p^2 - 4r = (\alpha_1^2 - \alpha_2^2)^2$$

(take into account that $\alpha_4 = -\alpha_1$ and $\alpha_3 = -\alpha_2$, so $p = -(\alpha_1^2 + \alpha_2^2)$ and $r = \alpha_1^2\alpha_2^2$).

The arguments are similar as in the previous case. As before, the first two groups with 4 elements are impossible, since the first fixes $\sqrt{\Delta}$ and the other one, $\sqrt{\delta} = \alpha_1^2 - \alpha_2^2$ (this should be checked case by case taking into account the equalities $\alpha_4 = -\alpha_1$ and $\alpha_3 = -\alpha_2$). Thus, if the Galois group $G(K_f/K)$ has order 4, it must be cyclic. But in this case, the fields $K(\sqrt{\Delta})$ and $K(\sqrt{\delta})$ must be equal, so $\sqrt{\delta\Delta} \in K$. Otherwise, if they are not equal, that is, $\sqrt{\delta\Delta} \notin K$, then the Galois group has order 8 and contains all permutations in the square group (in this case, D_4 above).

Case 3: The resolvent has all three zeros in K. Since now $K_{r(f)} = K$, the splitting field $K_f = K(\alpha)$, where α is any zero of $f(x)$ according to Theorem 2.1. Since $f(x)$ is irreducible, this field has degree 4 over K. Since all $\beta_i = (\alpha_i + \alpha_4)^2$ are in K, they are fixed by the four permutations in V_4, which is the Galois group $G(K_f/K)$ in this case. □

2.9 How to find Galois groups of reducible quartics?

Once we know that the polynomial $f(x)$ is reducible (but without zeros in K), we can easily describe its Galois group:

Proposition 2.2. *Let $f(x) = x^4 + px^2 + qx + r$ be reducible in K but without zeros in K. Then*

$$G(K_F/K) = \begin{cases} V_4 & \textit{when} \quad r(f) \textit{ has only one zero in } K \\ C_2 & \textit{when} \quad r(f) \textit{ has all its zeros in } K \end{cases}$$

Proof. Assume that

$$f(x) = x^4 + px^2 + qx + r = (x^2 - ax + b)(x^2 + ax + b'),$$

where $a, b, b' \in K$, $\delta = a^2 - 4b$ and $\delta' = a^2 - 4b'$ are not squares in K (since otherwise, the polynomial $f(x)$ has zeros in K). The zeros of $f(x)$ are $a/2 \pm \sqrt{\delta}$ and $-a/2 \pm \sqrt{\delta'}$. The splitting field of $f(x)$ over K is $K_f = K(\sqrt{\delta}, \sqrt{\delta'})$.

The zeros of the resolvent $r(f)$ are according to Lemma 2.1: $a^2, (\sqrt{\delta} \pm \sqrt{\delta'})^2 = \delta + \delta' \pm 2\sqrt{\delta\delta'}$.

The resolvent $r(f)$ has only one zero in K if and only if $\sqrt{\delta\delta'} \notin K$, which is equivalent to $K(\sqrt{\delta}) \neq K(\sqrt{\delta'})$, that is, $K_f = K(\sqrt{\delta}, \sqrt{\delta'})$ has degree 4 over K. The Galois group $G(K_f/K)$, in this case, is of course isomorphic to V_4 – the Kleins four-group, since all the automorphisms are given by $\sqrt{\delta} \mapsto \pm\sqrt{\delta}$ and $\sqrt{\delta'} \mapsto \pm\sqrt{\delta'}$.

(Notice however that as permutation group, it is not V_4, which in our notations, denotes a transitive copy of Klein's four group in S_4).

The resolvent $r(f)$ has 3 zeros in K if and only if $\sqrt{\delta\delta'} \in K$, which is equivalent to $K(\sqrt{\delta}) = K(\sqrt{\delta'})$, that is, $K_f = K(\sqrt{\delta})$. Thus in this case the splitting field K_f is quadratic over K and its Galois group is C_2 – cyclic of order 2. □

In fact, when we test irreducibility using Proposition 2.1, we can factor $f(x)$ into a product of two quadratic polynomials (see 2.5 for details). If we already have such a factorization, then it is useful to note the following direct corollary from the last proof:

Proposition 2.3. *Let*

$$f(x) = x^4 + px^2 + qx + r = (x^2 + ax + b)(x^2 - ax + b')$$

be a factorization of f over K, $\delta = a^2 - 4b$ and $\delta' = a^2 - 4b'$. Then

$$G(K_f/K) = \begin{cases} V_4 & \textit{when} \quad \sqrt{\delta\delta'} \notin K \\ C_2 & \textit{when} \quad \sqrt{\delta\delta'} \in K \end{cases}$$

2.10 A useful Lemma

Several times in this text, we use the following easy result:

Lemma 2.3. *Let L be a finite field extension of a field K and let $f(x) \in K[x]$ be an irreducible polynomial. If the degrees of $f(x)$ and L over K are relatively prime, then the polynomial $f(x)$ is still irreducible over L.*

Proof. Let $n = \deg(f)$ and $r = [L : K]$ (the degree of the field extension). Let α be a zero of $f(x)$ in a field containing L. Then $[K(\alpha) : K] = n$ (since $f(x)$ is irreducible over K) and let $[L(\alpha) : L] = m$. Of course, we have $m \leq n$, since $f(x)$ has degree n and may be reducible over L. The field $L(\alpha)$ contains the field $K(\alpha)$ as well as the field L.

$$\begin{tikzcd}
 & L(\alpha) \arrow[dl, dash] \arrow[dr, dash, "m"] & \\
K(\alpha) \arrow[dr, dash, "n"'] & & L \arrow[dl, dash, "r"] \\
 & K &
\end{tikzcd}$$

Since n and r are relatively prime and both divide $[L(\alpha) : K]$, the product nr also divides $[L(\alpha) : K] = [L(\alpha) : L][L : K] = mr$. Thus n divides m, and since $m \leq n$, we have $m = n$. This tells us that $f(x)$ is also irreducible over L, since $[L(\alpha) : L] = n$. □

2.11 How to solve cubic equations?

We want to solve the equation

$$x^3 + px + q = 0. \tag{8}$$

Compare the last equality with the well-known identity:

$$(a+b)^3 - 3ab(a+b) - (a^3+b^3) = 0 \tag{9}$$

and choose a, b in such a way that:

$$\begin{array}{rcl} p & = & -3ab, \\ q & = & -(a^3+b^3). \end{array} \tag{10}$$

If a, b are so chosen, then $x = a + b$ is a solution of the equation (8). The system

$$\begin{array}{rcl} a^3+b^3 & = & -q, \\ a^3b^3 & = & -\dfrac{p^3}{27}, \end{array}$$

shows that a^3, b^3 are solutions of the quadratic equation:

$$t^2 + qt - \frac{p^3}{27} = 0.$$

Solving this equation gives two solutions: $t_1 = a^3$ and $t_2 = b^3$. Then we choose a, b, which satisfy (10) and find $x = a + b$. An (impressing) formula, which hardly needs to be memorized (it is much easier to memorize the presented method based on the well-known binomial identity (9)) is thus the following:

$$x_1 = a + b = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Notice that a, b are simply third roots of t_1, t_2, but we have to be a little cautious since both a and b my be chosen in 3 different ways.

We leave a discussion of different choices of a, b as an easy exercise, but notice that in order to solve a cubic equation, it is sufficient to find only one root x_1 and solve a quadratic equation after dividing the cubic by $x - x_1$. The above expression (in different notations) was first published by Gerolamo Cardano in his book “Ars Magna” in 1545 and is known today as **Cardano’s formula**.

2.12 How to solve quartic equations?

Essentially, we already know the answer – any quartic polynomial with coefficients in a field K can be split into a product of two quadratic polynomials according to (4) (with $a' = -a$):

$$f(x) = x^4 + px^2 + qx + r = (x^2 + ax + b)(x^2 - ax + b'). \tag{11}$$

where a, b, b' are in a field containing K. We know that if we take a as square root of any nonzero solution of the resolvent equation

$$r(f)(t) = t^3 + 2pt^2 + (p^2 - 4r)t - q^2 = 0,$$

the system (5), gives us b and b'. Thus we factorize the quartic and solve two quadratic equations in order to find all zeros of $f(x)$. This is a very simple method and very easy to remember if we only know how to deal with a cubic equation (see 2.11). Observe that the resolvent equation always has a nonzero solution, since 0 is the only (triple) solution if and only if $p = q = r = 0$, that is, $f(x) = x^4$.

This is in principle the original method given by L. Ferrari[2] in the middle of 16th century and published in Cardano's book mentioned above. But the formal language of algebra was of course different during Cardano's and Ferrari's time, so the solution method was presented rather as recipe how to transform the equation in order to get a solution. Today, it is usually presented in the following way. One can start with the general equation

$$x^4 + mx^3 + px^2 + qx + r = 0, \tag{12}$$

– it is even not important to assume that $m = 0$ (but it could be achieved substituting $x = y - \frac{m}{4}$). It is easy to check that the above equation can be rewritten in the following way:

$$\left(x^2 + \frac{m}{2}x + \frac{\lambda}{2}\right)^2 - \left[\left(\frac{m^2}{4} + \lambda - p\right)x^2 + \left(\frac{m\lambda}{2} - q\right)x + \left(\frac{\lambda^2}{4} - r\right)\right] = 0 \tag{13}$$

We simply want to find a number λ such that the quadratic polynomial in square brackets is a square of a first degree polynomial. This is achieved when the discriminant of the quadratic polynomial in the square bracket equals 0, that is,

$$\left(\frac{m\lambda}{2} - q\right)^2 - 4\left(\frac{m^2}{4} + \lambda - p\right)\left(\frac{\lambda^2}{4} - r\right) = 0 \tag{14}$$

[2] Lodovico Ferrari (1522-1565) was an Italian mathematician who was a servant, later a student and finally a successor at the Universisty of Pavia of G. Cardano.

This is a cubic equation with respect to λ. Solving it (e.g. according to 2.11), we get a root λ, which gives a possibility to split the quartic polynomial (12) into a product of two quadratic polynomials and then solve two quadratic equations.

3 APPENDIX: The group S_4 and their subgroups

As a permutation group, the Galois group $G(K_f/K)$ of an irreducible polynomial $f(x) \in K[x]$ has an important property of transitivity. A permutation group $G \subseteq S_n$ is called **transitive** if for any pair $i, j \in \{1, 2, \ldots, n\}$ there is a permutation $\sigma \in G$ such that $\sigma(i) = j$. Of course, this property is valid for Galois groups of irreducible polynomials, since according to well-known properties of automorphisms of splitting fields, there is always an automorphism which maps any given zero of $f(x)$ onto any other zero of this polynomial.

The symmetric group S_3 of all permutations of $1, 2, 3$ consists of $3! = 6$ elements. We can represent each permutation as an isometry of the plane mapping the equatorial triangle with vertices in the points 1, 2, 3 on itself. If $\{a, b, c\} = \{1, 2, 3\}$, then there are 3 rotations: the identity (1), the rotations $\pm 120^0$: $(1, 2, 3)$, $(1, 3, 2)$ and 3 symmetries in the three heights of the triangle: $(1, 2), (2, 3), (1, 3)$. There are only two transitive subgroups of S_3: the group S_3 itself and the subgroup of the rotations (all even permutations) $A_3 = \{(1), (1, 2, 3), (1, 3, 2)\}$. All these facts are very easy to check (e.g. by listing all the subgroups of S_3).

The symmetric group S_4 of all permutations of $1, 2, 3, 4$ consists of $4! = 24$ elements. We can represent each permutation as an isometry of the space mapping the tetrahedron with vertices in the points 1, 2, 3, 4 on itself. If $\{a, b, c, d\} = \{1, 2, 3, 4\}$, then each non-identity permutation can be written as a cycle or a composition of them:

6 symmetries (a, b) of order 2: in the planes through the vertices c, d and the middle of the side between a and b;

8 rotations (a, b, c) of order 3: around the axis through the vertex d perpendicularly to the plane through the points a, b, c;

3 rotations $(a, b)(c, d)$ of order 2: 180 degrees around the axis through the middles of the sides a, b and c, d. Notice that these rotations together with the identity (1) form a transitive group of order 4. It is a transitive presentation of Klein's four group, which is usually denoted by V_4, that is,

$$V_4 = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

6 cycles (a, b, c, d) of order 4: compositions of the rotation (a, b, c) with the symmetry (c, d).

Together with the identity (1), we have 24 all possible isometric mappings of the tetrahedron on itself. Notice that the even permutations are exactly the 12 rotations, and the odd permutations are the 6 symmetries and the 6 compositions of a rotation of order 3 and a symmetry.

In order to describe all transitive subgroups of S_4, notice that in any subgroup G, which contains at least one odd permutation σ, the half of the elements are odd permutations, and the other half are even. In fact, if G_0 denotes all even permutations in G, then G_0 is a (normal) subgroup of G and $G = G_0 \cup \sigma G_0$, since every permutation τ in G is either even or, if it is odd, then $\sigma^{-1}\tau$ is even (that is, in G_0).

Using this observation, we first note that the group S_4 has exactly one (normal) subgroup of order 12. This is the subgroup A_4 consisting of even permutations (rotations of the tetrahedron)[3]. In fact, if G is a subgroup of S_4 of order 12 and contains at least one odd permutation, then the intersection $A_4 \cap G$ is a subgroup of A_4 of order 6. Such a subgroup of order 6 is not cyclic (there are no elements of order 6 in S_4), so it must be isomorphic with S_3. Hence, it contains 3 elements of order 2. The only even permutations of order 2 in S_4 are the 3 rotations 180^0, which together with the identity form the group V_4 of order 4. This is of course a contradiction, since a group of order 4 can not be a subgroup of a group of order 6. Thus S_4 has only one subgroup of order 12 – the one consisting of all even permutations.

Next, the group S_4 may have subgroups of order 8. There are in fact 3 subgroups of order 8. All are isomorphic with the square group D_4 and are transitive. In order to prove this, assume that G is a subgroup of order 8. Then it must consist of both even and odd permutations – all can not be even, since a group of order 8 can not be a subgroup of a group of order 12. The subgroup G_0 of G consisting of the even permutations (that is, rotations of the tetrahedron) must be $G_0 = V_4$, since the remaining rotations all have order 3 (can not belong to a group of order 4). The odd permutations in G can not all be of order 2. Those are exactly the symmetries of the tetrahedron. Between 4 such symmetries, there are at least 2 which shift the same vertex (of four possible), that is, they have form (a, b) and (a, c). Then the group G contains $(a, b)(a, c) = (a, c, b)$, which as an element of order 3. This order is not allowed by G. Thus G must contain an odd permutation σ of order 4. An easy direct computation shows that there are exactly 3 possibilities for σV_4, which give 3 possibilities for G:

$$D_4 = V_4 \cup \{(1, 2, 4, 3), (1, 3, 4, 2), (1, 4), (2, 3)\},$$

$$D_4' = V_4 \cup \{(1, 2, 3, 4), (1, 4, 3, 2), (1, 3), (2, 4)\},$$

$$D_4'' = V_4 \cup \{(1, 3, 2, 4), (1, 4, 2, 3), (1, 2), (3, 4)\}.$$

It is clear that these groups are transitive. Each group gives a description of all isometries of a square corresponding to a numbering of its vertices a, b, c, d according to the rotations of square given by the elements of order 4 belonging to it.

[3] In general, the subgroup consisting of all even permutations in S_n is denoted by A_n and called the alternated group of degree n. Its order is $n!/2$.

There are no transitive subgroups G of S_4 of order 6. In fact, such a subgroup can not be cyclic, since there are no elements of order 6 in S_4. Thus it must be isomorphic to S_3. As we know such a group has 3 elements of order 2 and 2 elements of order 3. Between the elements of order 2 must be at least 2 symmetries (otherwise G_0 is a subgroup of G, which is impossible). They must shift a common vertex a. Otherwise, they are of the form $(a, b), (c, d)$ with different a, b, c, d. Then $(1), (a, b), (c, d), (a, b)(c, d)$ is a subgroup of G, which is impossible. If (a, b) and (a, c) are in G, then it is easy to check that G is the group of all permutations of a, b, c. It is not transitive on the set $\{1, 2, 3, 4\}$.

Finally, there is only one transitive subgroup of order 4 – the group V_4. In fact, it is easy to check that the subgroups generated by the elements of order 4 are not transitive. A non-cyclic subgroup of order 4 must contain 3 elements of order 2. A similar argument to that given above in connection with the subgroups of order 6 shows that it is impossible to get a transitive group with two symmetries. Thus we can only have the rotations giving V_4.

Of course, the subgroups of order 2 are never transitive.

Summarizing, we have the following list of transitive subgroups of S_4:

$$S_4, A_4, D_4, D_4', D_4'', V_4.$$

The group V_4 is a subgroup of all these groups. Notice that the groups D_4, D_4', D_4'' are all isomorphic. They consist of all isometries of a square corresponding to a numbering of its vertices a, b, c, d (according to the rotations given by the elements of order 4 belonging to it). Recall that such a group contains 3 subgroups of order 4: V_4 (the rectangle group), the cyclic group of the rotations of the square:

$$C_4 = \{(1), (a, b, c, d), (a, d, c, b), (a, c)(b, d)\}$$

and a non-transitive representation of Klein's four group (the romb group):

$$V_4' = \{(1), (a, b), (c, d), (a, b)(c, d)\}.$$

REFERENCES

[B] J. Brzeziński, *Galois groups of quartic polynomials* (in Polish), Wiadomości Matematyczne X(1968), 133–143.

[C] D. Cox, *Galois Theory*, Wiley-Interscience, 2012.

[L] S. Lang, *Algebra*, Addison–Wesley, 1993.

[N] T. Nagell, *Lärobok i algebra*, Hugo Gebers Förlag, Uppsala 1949.

[T] N.G. Tschebotaröw, H. Schwerdtfeger, *Grundzüge Der Galois'schen Theorie*, P. Nordhoff N.V., Groningen-Djakarta, 1950.