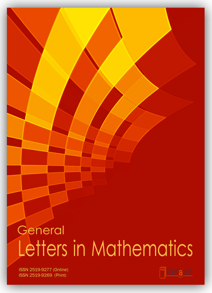


General Letters in Mathematics Vol. 3, No. 3, Dec 2017, pp.132-153
e-ISSN 2519-9277, p-ISSN 2519-9269
Available online at http:// www.refaad.com

Field Extension by Galois Theory

Md Taufiq Nasseef

University of Kent, UK
taufiq278@gmail.com

Abstract. Galois Theory, a wonderful part of mathematics with historical roots date back to the solution of cubic and quantic equations in the sixteenth century. However, beside understanding the roots of polynomials, Galois Theory also gave birth to many of the central concepts of modern algebra, including groups and fields. In particular, this theory is further great due to primarily for two factors: first, its surprising link between the group theory and the roots of polynomials and second,the elegance of its presentation. This theory is often descried as one of the most beautiful parts of mathematics. Here I have specially worked on field extensions. To understand the basic concept behind fundamental theory, some necessary Theorems, Lammas and Corollaries are added with suitable examples containing Lattice Diagrams and Tables. In principle, I have presented and solved a number of complex algebraic problems with the help of Galois theory which are designed in the context of various rational and complex numbers.

Keywords: *Field Extension, Splitting fields, Separability, Galois theory.*

MSC2010 12E30.

1 Introduction and Preliminaries

Evariste Galois (French pronunciation: [evarist galwa]) (October 25, 1811-?May 31, 1832) was a French mathematician born in Bourg-la-Reine. While still in his teens, he was able to determine a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a long-standing problem. His work laid the foundations for Galois theory and group theory, two major branches of abstract algebra, and the subfield of Galois connections. He was the first to use the word ”group” (French: groupe) as a technical term in mathematics to represent a group of permutations [1].

Galois' most significant contribution to mathematics by far is his development of Galois theory. He realized that the algebraic solution to a polynomial equation is related to the structure of a group of permutations associated with the roots of the polynomial, the Galois group of the polynomial. He found that an equation could be solved in radicals if one can find a series of subgroups of its Galois group, each one normal in its successor with abelian quotient, or its Galois group is solvable [2]. This proved to be a fertile approach, which later mathematicians adapted to many other fields of mathematics besides the theory of equations to which Galois originally applied it. Field extension is the focal ambition to work. So it would be a very good idea to start with the definition of field extensions.

1.1 Field extensions

A field L is an extension of another field K if K is a subfield of L.

Definition 1.1. A field extension is a monomorphism $i : \mathbf{K} \to \mathbf{L}$ where $\mathbf{K}$ and $\mathbf{L}$ are fields. $\mathbf{K}$ is the small field, $\mathbf{L}$ the large field.

1.2 Simple extensions

A simple extension is an extension **L**:**K** having the property that $\mathbf{L} = \mathbf{K}(\alpha)$ *for some* $\alpha \in \mathbf{L}$.
Polynomials are known to all.It is important to know about the specific group of polynomials and properties which are needed in my field extension.
A polynomial

$$f(t) = a_0 + a_1 + ... + a_n t^n$$

over a field **K** is monic if $a_n = 1$.
Definition 1.2 Let $\mathbf{K}(\alpha) : \mathbf{K}$ be a simple extention.If there exists a non-zero polynomial p over K such that $p(\alpha) = 0$ then α is an algebraic element over **K** and the extension is simple algebraic extension.
Definition 1.3 Let $\mathbf{L} : \mathbf{K}$ be the field extension, and suppose that $\alpha \in \mathbf{L}$ is algebraic over **K**.Then the minimum polynomial of over **K** is the unique monic polynomial m over **K** of the smallest degree such that $m(\alpha) = 0$.
An example could be the best thing to clear the definitions. For example, $i \in C$ is algebraic over **R**. If we let m $(t) = t^2 + 1$ then $m(i) = 0$.Clearly m is monic. The only monic polynomials over **R** of smaller degree are those of the form $t + r(r \in \mathbf{R})$ or 1.But i cannot be zero of any of these. Hence the minimum polynomial of i over **R** is $t^2 + 1$.
Two theorems are going to present with no proofs that are closely related to this project.
Theorem.1.1 If **K** is any field and m is any irreducible monic polynomial over **K**, then there exists an extension $\mathbf{K}(\alpha) : \mathbf{K}$ such that α has minimum polynomial m over **K**.
Theorem.1.2 Suppose **K** and **L** are fields and $i : \mathbf{K} \to \mathbf{L}$ is an isomorphism.Let $\mathbf{K}(\alpha)$, $\mathbf{L}(\beta)$ be simple algebraic extensions of **K** and **L** respectively, such that α has minimum polynomial $m_\alpha(t)$ over **K** and β has minimum polynomial $m_\beta(t)$ over **L**.Suppose further that$m_\beta = i(m_\alpha(t))$.Then there exists an isomorphism $j : \mathbf{K}(\alpha) \to \mathbf{L}(\beta)$ such that $j|_\mathbf{K} = iandj(\alpha) = \beta$.
Definition 1.4. The degree $[\mathbf{L} : \mathbf{K}]$ of a field extension $\mathbf{L} : \mathbf{K}$ is the dimension of **L** considered as a vector space over **K**. **Example 1.1**. The complex numbers **C** are 2-dimensional over the real numbers $\mathbf{R}, 1, i$ being a basis.Hence $[\mathbf{C} : \mathbf{R}] = 2$.
Definition 1.5. If **K**,**L**,**M** are fields and $\mathbf{K} \subseteq \mathbf{L} \subseteq \mathbf{M}$, then **L** is the Intermediate Field.
Theorem.1.3 If **K**,**L**,**M** are fields and $\mathbf{K} \subseteq \mathbf{L} \subseteq \mathbf{M}$, then

$$[\mathbf{M} : \mathbf{K}] = [\mathbf{M} : \mathbf{L}][\mathbf{L} : \mathbf{K}]$$

Example 1.2 Suppose we wish to find $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}]$. It is easy to see that $\{1, \sqrt{2}\}$ is a basis for $\mathbf{Q}(\sqrt{2})$ over **Q**. It is a little harder to see that $\{1, \sqrt{3}\}$ is a basis for $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ *over* $\mathbf{Q}(\sqrt{2})$.Hence $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}\sqrt{2} : \mathbf{Q}] = 2.2 = 4$. [2]

1.3 Splitting fields

Definition 1.6. If **K** is a field and f is a polynomial over **K** then f splits over **K** if it can be expressed as a product of linear factors

$$f(t) = k(t - \alpha_1)....(t - \alpha_n)$$

where k, $\alpha_1 ... \alpha_n \in \mathbf{K}$.
Example 1.3 Let $f(t) = (t^2 - 3)(t^3 + 1)$ over **Q**. We can construct a splitting field for f as follows: inside **C** f splits into linear factors

$$f(t) = (t + \sqrt{3})(t - \sqrt{3})(t + 1)(t - \frac{-1 + i\sqrt{3}}{2})(t - \frac{-1 - i\sqrt{3}}{2})$$

so there exists a splitting field inside **C**, namely

$$\mathbf{Q}(\sqrt{3}, \frac{-1 + i\sqrt{3}}{2})$$

This is clearly the same as $\mathbf{Q}(\sqrt{3}, i)$.

1.4 Discriminant

The discriminant of $X^2+aX+b=(X-r)(X-r')$ is $(r-r')^2=r^2-2rr'+r'^2=(r+r')^2-4rr'=a^2-4b$; which is the usual discriminant of a monic quadratic polynomial.In low-degree cases, explicit formulas for discriminants of some trinomials are

$$disc(X^2+aX+b)=a^2-4b;$$

$$disc(X^3+aX+b)=-4a^3-27b^2;$$

$$disc(X^4+aX+b)=-27a^4+256b^3;$$

$$disc(X^5+aX+b)=256a^5+3125b^4$$

Example 1.4 The discriminant of X^3-X-1 is -23, the discriminant of X^3-3X-1 is 81, and the discriminant of X^3-4X-1 is 229. [2]

1.5 Normality

Definition 1.7. An extension **L**:**K** is normal if every irreducible polynomial f over **K** which has at least one zero in **L** splits in **L**.

1.6 Separability

Definition 1.8. An irreducible polynomial f over a field **K** is separable over **K** if it has no multiple zero in a splitting field. This means that in any splitting field f takes the form

$$k(t-\sigma_1)...(t-\sigma_n)$$

where the σ_i are all different.

Lemma 1.1. Let **L**:**K** be a separable algebraic extension and let **M** be an intermediate field. Then **M**:**K** and **L**:**K** are separable.
Minimum polynomial is new term to us. To know about it we need to follow the Eisentein's Irreducibility Criterion.
Eisentein's Irreducibility Criterion

Let

$$f(t)=a_0+a_1t+.......+a_nt^n$$

be a polynomial over **Z**. Suppose that there is a prime q such that

(1)$q \nmid a_n$

(2)$q \mid a_i(i=0,1,........n-1)$

(3)$q^2 \nmid a_0$.

Then f is irreducible over **Q**

Example 1.5 Consider $f(t)=\frac{2}{9}t^5+\frac{5}{3}t^4+t^3+\frac{1}{3}$ over **Q**. This is irreducible if and only if $9f(t)=2t^5+15t^4+9t^3+3$ is irreducible over **Q**.Eisentein's Criterion applies with q=3, showing that f is irreducible. [2]

2 Galois Theory

Definition 2.1. Let **K** be a subfield of the field **L**.An automorphism α of **K**-automorphism of **L** if $\alpha(k)=k$ for all $k\in$ **K**.
A simple but effective theorem would be the next one.
Theorem.2.1 If **L**:**K** is a field extension then set of all **K**-automorphisms of **L** forms a group under composition of maps.
The next example will give us a rough idea about our problem.
Definition 2.2. The Galois group $\Gamma(L:K)$ of the extension $L:K$ is the group of all K-automorphisms of L under composition of maps.
Example 2.1 The extension **C** : **R** .Suppose that α is an **R**-automorphism of **C**. Let $j=\alpha(i)$ where $i=\sqrt{-1}$. Then

$$j^2=(\alpha(i))^2=\alpha(i^2)=\alpha(-1)=-1$$

since $\alpha(r) = r$ for all $r \in \mathbf{R}$.Hence either $j = i$ or $j = -i$. Now for any $x, y \in \mathbf{R}$ we have

$$\alpha(x + iy) = \alpha(x) + \alpha(i)\alpha(y)$$
$$= x + jy$$

Thus we have two candidates for **R**-automorphisms:

$$\alpha_1 : x + iy \to x + iy$$
$$\alpha_2 : x + iy \to x - iy$$

Now α_1 is the identity, and thus is an **R**-automorphism of **C**.The map α_2 is known as complex conjugation and can be shown to be an **R**-automorphism as follows:

$$\alpha_2((x + iy) + (u + iv)) = (x + iy) - (u + v)i$$
$$= \alpha_2(x + iy) + \alpha_2(u + iv)$$
$$\alpha_2((x + iy)(u + iv)) = \alpha_2(xu - yv + i(xv + yu))$$
$$= xu - yv - i(xv + yu)$$
$$= (x - iy)(u - iv)$$
$$= \alpha_2(x + iy)\alpha_2(u + iv)$$

Thus α_2 is an automorphism. And

$$\alpha_2(x + 0i) = x - 0i = x$$

so that α_2 is an **R**-automorphism. Obviously $\alpha_2^2 = \alpha_1$,so that the Galois group $\Gamma(\mathbf{C} : \mathbf{R})$ is a cyclic group of order 2.

If **L**:**K** is a field extension then a field **M** such that $\mathbf{K} \subseteq \mathbf{M} \subseteq \mathbf{L}$ is called an *intermediate field.*Each intermediate field **M** associates the group $\mathbf{M}^* = \Gamma(\mathbf{L} : \mathbf{M})$. Thus $\mathbf{K}^*$is the whole Galois group.

Lemma 2.1. If **H** is a subgroup of $\Gamma(\mathbf{L} : \mathbf{K})$ then $\mathbf{H}^\dagger$ is a subfield of **L** containing **K**. With the above notation,$H^\dagger$ is a fixed field of H.

Theorem.2.2 Let G be a finite subgroup of the group of automorphisms of a field **K** and let $\mathbf{K}_0$ be the fixed field of G. then

$$[\mathbf{K} : \mathbf{K}_0] = |G|$$

Example 2.2 Let $K = \mathbf{Q}(\alpha)$ where $\alpha = e^{\frac{2\pi i}{5}} \in \mathbf{C}$. Now $\alpha^5 = 1$ and $\mathbf{Q}(\alpha)$ consists of all elements

$$a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 \qquad (1)$$

Where $a, b, c, d, e \in \mathbf{Q}$. The Galois group of $\mathbf{Q}(\alpha) : \mathbf{Q}$ is easy to find, for if σ is a **Q**-automorphism of $\mathbf{Q}(\alpha)$ then $(\sigma(\alpha))^5 = \sigma(\alpha^5) = \sigma(1) = 1$, so that $\sigma(\alpha) = \alpha, \alpha^2, \alpha^3,\ or\ \alpha^4$. This gives 4 candidates for **Q**-automorphisms:

$\sigma_1 : a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 \to a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4$
$\sigma_2 : \to a + c\alpha + d\alpha^2 + e\alpha^3 + b\alpha^4$
$\sigma_3 : \to a + d\alpha + e\alpha^2 + b\alpha^3 + c\alpha^4$
$\sigma_4 : \to a + e\alpha + b\alpha^2 + c\alpha^3 + d\alpha^4$

It is easy ti check that these are all **Q**-automorphisms.Hence the Galois group $\mathbf{Q}(\alpha) : \mathbf{Q}$ has order 4.The fixed field of this Galois group is easy to complete: it turns out to be **Q**.There we have $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4$. At first sight this might seem wrong for (1) expresses each element in terms of 5 basis elements;the degree should be 5.In support of this contention, α is a zero of $t^5 - 1$. $t^5 - 1$ is not the minimum polynomial of α over **Q**,since it is reducible.The minimum polynomial is in fact

$$t^4 + t^3 + t^2 + t + 1$$

which has degree 4. Equation (1) holds, but the elements of the supposed 'basis' are linearly dependent :

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$$

Hence every element of $\mathbf{Q}(\alpha)$ can be expressed uniquely in the form

$$a + b\alpha + c\alpha^2 + d\alpha^3$$

where $a, b, c, d \in \mathbf{Q}$.

Sufficient background knowledge has been acquired to get in the fundamental theorem. The property given below will be very useful for the theorem.

Let **L**:**K** be a field extension with Galois group **G**, which consists of all **K**-automorphisms of **L**. Let F be the set of intermediate fields M, and g the set of all subgroups H of G.We have defined two maps

$$^* : F \to g$$

$$^\dagger : g \to F$$

as follows : if $M \in F$ then M^* is the group of all **M**-automorphisms of **L**. If $H \in \mathbf{g}$ then $H^\dagger$ is the fixed field of H.We have observed that the maps * and † reverse inclusions that $M \subseteq M^{*\dagger}$, and $H \subseteq H^{\dagger *}$. [2]

2.1 Fundamental Theorem of Galois Theory

If **L**:**K** is a finite separate normal field extension of degree n, with Galois group **G**;and if f,g, *,† are defined as above, then:

(1) The Galois group **G** has order n.

(2) The maps * and † are mutual inverses and set up an order-reversing 1-1 correspondence between f and g.

(3) If **M** is an intermediate field then

$$[L : M] = |M^*|$$

$$[M : K] = |G|/|M^*|.$$

(4) An intermediate field **M** is a normal extension of **K** if and only if M^* is a normal subgroup of **G**(in the usual sense of group theory).

(5) If an intermediate field **M** ia normal extension of **K** then the Galois group of **M**:**K** is isomorphic to the quotient group G/M^*

Theorem 2.3 (Dedekind). Let $f(X) \in Z[X]$ be monic irreducible over **Q** of degree n. For any prime p not dividing disc f, let the monic irreducible factorization of f(X) mod p be

$$f(X) \equiv \pi_1(X)...\pi_k(X) \ mod \ p$$

and set $d_i = deg\pi_i(X)$, so $d_1 + ... + d_k = n$. The Galois group of f(X) over **Q**, viewed as a subgroup of S_n, contains a permutation of type $(d_1, ..., d_k)$. [2]

3 Problems

3.1 Problem A

1.Let $f(t) = t^4 - 5$ over **Q**, and let **K** be a splitting field for f such that $K \subseteq \mathbf{C}$.In **C** we can factorize f as follows:

$$f(t) = (t - \xi)(t + \xi)(t - i\xi)(t + i\xi)$$

where $\xi = \sqrt[4]{5}$ is real and positive.Clearly therefore $\mathbf{K} = \mathbf{Q}(\xi, i)$.There characteristic is 0 and **K** is a splitting field, so that **K**:**Q** is finite,separable, and normal.

2.We shall find the degree of **K**:**Q**.We have

$$[\mathbf{K} : \mathbf{Q}] = [\mathbf{Q}(\xi, i) : \mathbf{Q}(\xi)][\mathbf{Q}(\xi) : \mathbf{Q}]$$

The minimum polynomial of i over $\mathbf{Q}(\xi)$ is t^2+1 since $i^2+1=0$ but $i \notin \mathbf{R} \supseteq \mathbf{Q}(\xi)$.So $[\mathbf{Q}(\xi,i):\mathbf{Q}(\xi)]=2$. Now ξ is a zero of f over $\mathbf{Q}$, and f is irreducible by Eisenstein's criterion.Hence f is the minimum polynomial of ξ over $\mathbf{Q}$ and $[\mathbf{Q}(\xi):\mathbf{Q}]=4$. Therefore

$$[\mathbf{K}:\mathbf{Q}]=2.4=8$$

3.We shall find the elements of the Galois group of **K**:**Q**.Now i varies from i to -i.So there must be two automorphisms.By a direct check,we see that there is **Q**-automorphism σ of **K** such that

$$\sigma(i)=i, \quad \sigma(\xi)=i\xi$$

and another, τ, such that

$$\tau(i)=-i, \quad \tau(\xi)=\xi.$$

Product of these yield 8 distinct **Q**-automorphism of **K**, as follows:

automorphism	effect on ξ	effect on i
1	ξ	i
σ	$i\xi$	i
σ^2	$-\xi$	i
σ^3	$-i\xi$	i
τ	ξ	-i
$\sigma\tau$	$i\xi$	-i
$\sigma^2\tau$	$-\xi$	-i
$\sigma^3\tau$	$-i\xi$	-i

other products do not give new automorphisms, since $\sigma^4=1, \tau^2=1, \sigma\tau=\sigma^3\tau, \tau\sigma^2=\sigma^2\tau, \tau\sigma^3=\sigma\tau$. (The last two relations follow from the first three.)

Now any **Q**-automorphism of **K** sends i to some zero of t^2+1,so $i \rightarrow^{+}_{-} i$; similarly ξ is mapped to $\xi, i\xi$, or $-i\xi$.All possible combinations of these(8 in number) appears in the above list, so these are precisely the **Q**-automorphisms of **K**.

4.The abstract structure of the Galois group **G** can be found.From the generator-relation presentation

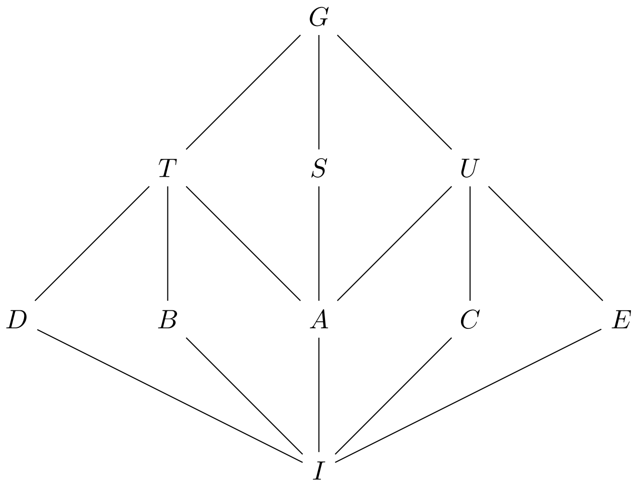
$$\mathbf{G} =< \sigma,\tau : \sigma^4=\tau^2, \tau\sigma=\sigma^3\tau >$$

it follows that **G** is the dihedral group of order 8, which we shall write as $\mathbf{D}_8$

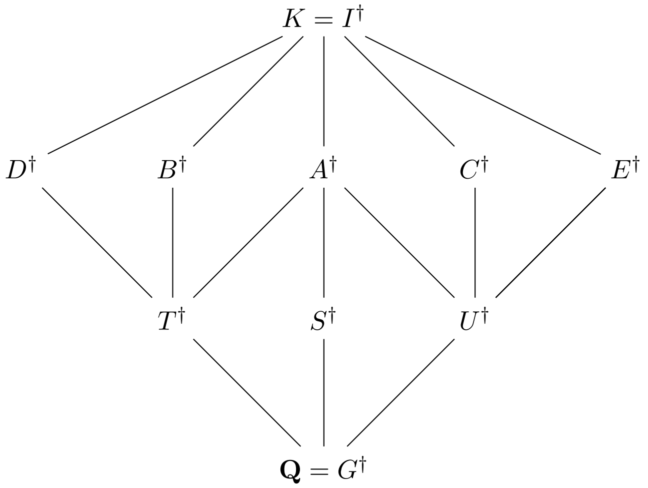
5. It is an easy exercise to find the subgroups of G.If we let C_n denote the cyclic group of order n, and × the direct product, then the subgroups are as follows:

Order 8:G	$G \cong \mathbf{D}_8$
Order 4:$\{1,\sigma,\sigma^2,\sigma^3\}$	$S \cong \mathbf{C}_4$
$\{1,\sigma^2,\tau,\sigma^2\tau\}$	$T \cong \mathbf{C}_2 \times \mathbf{C}_2$
$\{1,\sigma^2,\sigma\tau,\sigma^3\tau\}$	$U \cong \mathbf{C}_2 \times \mathbf{C}_2$
Order 2:$\{1,\sigma^2\}$	$A \cong \mathbf{C}_2$
$\{1,\tau\}$	$B \cong \mathbf{C}_2$
$\{1,\sigma\tau\}$	$C \cong \mathbf{C}_2$
$\{1,\sigma^2\tau\}$	$D \cong \mathbf{C}_2$
$\{1,\sigma^3\tau\}$	$E \cong \mathbf{C}_2$
Order 1:$\{1\}$	$I \cong \mathbf{C}_1$

6 The inclusion relations between the subgroups of G can be summed up by the following *lattice diagram*:



7 Under the Galois correspondence we obtain the intermediate fields. Since the correspondence reverses inclusions this gives a lattice diagram of fields as follows:



8 We now describe the elements of these intermediate fields.

There are three obvious subfields of $\mathbf{K}$ degree 2 over Q,namely $Q(i), Q(\sqrt{5}), Q(i\sqrt{5})$.These are clearly the fixed fields $S^\dagger$,$T^\dagger and\ U^\dagger$ (respectively).The other fixed fields are less obvious.To illustrate a possible approach we shall find $C^\dagger$. Now any element of $\mathbf{K}$ can be expressed in the form

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3 \ where\ a_0, ..., a_7 \in \mathbf{Q}.$$

Then

$$\sigma\tau(x) = a_0 + a_1 i\xi - a_2\xi^2 - a_3 i\xi^3 - a_4 i + a_5(-i)i\xi - a_6 i(i\xi)^2 - a_7 i(i\xi)^3$$

$$= a_0 + a_5\xi - a_2\xi^2 - a_7\xi^3 - a_4 i + a_1 i\xi + a_6 i\xi^2 - a_3 i(i\xi^3$$

Therefore x is fixed by $\sigma\tau$ (and hence by C) if and only if $a_0 = a_0, a_1 = a_5, a_2 = -a_2, a_3 = -a_7, a_4 = -a_4, a_5 = a_1, a_6 = a_6, a_7 = -a_3$. Therefore a_0 and a_6 are arbitrary, $a_2 = 0 = a_4, a_1 = a_5, and a_3 = -a_7$.It follows that

$$x = a_0 + a_1(1+i)\xi + a_6 i\xi^2 + a_3(1-i)\xi^3$$

$$= a_0 + a_1\{(1+i)\xi\} + \frac{a_6}{2}\{(1+i)\xi\}^2 - \frac{a_3}{2}\{(1+i)\xi\}^3$$

$$= a_0 + a_1\{(1+i)\xi\} + \frac{a_6}{2}(1+i)^2\xi^2 - \frac{a_3}{2}(1+i)^3\xi^3$$

$$= a_0 + a_1\{(1+i)\xi\} + \frac{a_6}{2}(1+i)(1+i)\xi^2 - \frac{a_3}{2}2i(1+i)\xi^3$$

which means that

$$C^{\dagger} = \mathbf{Q}((1+i)\xi).$$

Now again

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3 \ where\ a_0, ..., a_7 \in \mathbf{Q}.$$

Then

$$\sigma^2(x) = a_0 - a_1\xi + a_2\xi^2 - a_3\xi^3 + a_4 i - a_5 i\xi + a_6 i\xi^2 - a_7 i\xi^3 \ where\ a_0, ..., a_7 \in \mathbf{Q}.$$

Therefore x is fixed by σ^2 (and hence by C) if and only if $a_0 = a_0, a_1 = -a_1, a_2 = a_2, a_3 = -a_3, a_4 = a_4, a_5 = -a_5, a_6 = a_6, a_7 = -a_7$. Therefore a_0, a_2, a_4 and a_6 are arbitrary.It follows that

$$x = a_0 + a_2\xi^2 + a_4 i + a_6 i\xi^2$$

$$x = (a_0 + a_2\xi^2) + i(a_4 + a_6\xi^2)$$

which means that

$$A^{\dagger} = \mathbf{Q}(i, \sqrt{5}).$$

Similarly we have

$$B^{\dagger} = \mathbf{Q}(\xi).$$
$$D^{\dagger} = \mathbf{Q}(i\xi).$$
$$E^{\dagger} = \mathbf{Q}((1-i)\xi).$$

It is now easy to verify the inclusion relations determined by the lattice diagram of section 7.

9 If we check by hand that these are indeed the only intermediate fields.

10 The normal subgroups of G are G,S,T,U,A,I. By the theory,$G^{\dagger}, S^{\dagger}, T^{\dagger}, U^{\dagger}, A^{\dagger}, I^{\dagger}$ should be the only normal extensions of $\mathbf{Q}$ which are contained in $\mathbf{K}$.Since these are all splitting fields over $\mathbf{Q}$,for the polynomial $t, t^2+1, t^2-5, t^2+5, t^4-4t^2-5, t^4-5$ (respectively)they are normal extensions of $\mathbf{Q}$. On the other hand $B^{\dagger} : \mathbf{Q}$ is not normal, since $t^4 - 5$ has a zero, namely ξ in $B^{\dagger}$ but does not split in $B^{\dagger}$. Similarly $C^{\dagger}, D^{\dagger}, E^{\dagger}$ are not normal extensions of $\mathbf{Q}$.

11 The intermediate field $A^{\dagger}$ is a normal extension of $\mathbf{Q}$ then the Galois group of $A^{\dagger} : \mathbf{Q}$ is isomorphic to the quotient group G/A. Now G/A is isomorphic to $\mathbf{C}_2 \times \mathbf{C}_2$.We calculate directly the Galois group of $A^{\dagger}$. Since $A^{\dagger} = \mathbf{Q}(i, \sqrt{5})$ there are 4 $\mathbf{Q}$-automorphisms

automorphism	effect on i	effect on $\sqrt{5}$
1	i	$\sqrt{5}$
α	i	$-\sqrt{5}$
β	$-i$	$\sqrt{5}$
$\alpha\beta$	$-i$	$-\sqrt{5}$

and since $\alpha^2 = \beta^2 = 1$ and $\alpha\beta = \beta\alpha$, this group is $\mathbf{C}_2 \times \mathbf{C}_2$ as expected.

The next example is completely different from the above.

3.2 Problem B

Let $\mathbf{Q}(\sqrt[4]{2}, \xi_8)$, where $\xi_8 = e^{\frac{2\pi i}{8}}$ is a root of unity of order 8,whose minimum polynomial over $\mathbf{Q}$ is $X^4 + 1$. Both $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(\xi_8)$ have degree 4 over $\mathbf{Q}$. Since $\xi_8^2 = i$,$\mathbf{Q}(\sqrt[4]{2}, \xi_8)$ is a splitting field over $\mathbf{Q}$ of $(X^4-2)(X^4+1)$ and therefore is Galois over $\mathbf{Q}$.We would like to find out its Galois group.We have the following field diagram.

$$\begin{tikzcd}
& Q(\sqrt[4]{2},\xi_8) \arrow[dl, dash, "\leq 4"'] \arrow[dr, dash, "\leq 4"] & \\
Q(\sqrt[4]{2}) \arrow[dr, dash, "4"'] & & Q(\xi_8) \arrow[dl, dash, "4"] \\
& Q &
\end{tikzcd}$$

Thus $[\mathbf{Q}(\sqrt[4]{2},\xi_8) : \mathbf{Q}]$ is at most 16.We will see that degree is not 16: there are some hidden algebraic relation between $\sqrt[4]{2}$ and ξ_8.

Any $\sigma \in G^{\dagger}((\mathbf{Q}(\sqrt[4]{2},\xi_8)/\mathbf{Q})$ is determined by its values

(1.1) $\sigma(\xi_8) = \xi_8^a (a \in (\mathbf{Z}/8\mathbf{Z})^{\times}))$ and $\sigma(\sqrt[4]{2}) = i^b\sqrt[4]{2}(b \in \mathbf{Z}/4\mathbf{Z})$.

There are 4 choices each for a and b. Taking independent choices of a and b, there are at most 16 automorphisms in the Galois group.But the choices of a and b can not be made independently because ξ_8 and $\sqrt[4]{2}$ are linked to each other:

(1.2) $\xi_8 + \xi_8^{-1} = e^{\frac{2\pi i}{8}} + e^{\frac{-2\pi i}{8}} = 2cos(\frac{\pi}{4}) = \sqrt{2} = (\sqrt[4]{2})^2$

This says $\sqrt{2}$ belongs to both $\mathbf{Q}(\xi_8)$ and $\mathbf{Q}(\sqrt[4]{2})$. Here is a field diagram which emphasizes the common subfield $\mathbf{Q}(\sqrt{2})$ in $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(\xi_8)$, This subfield is the source of (1.2)

$$\begin{tikzcd}
& Q(\sqrt[4]{2},\xi_8) \arrow[dl, dash, "\leq 4"'] \arrow[dr, dash, "\leq 4"] & & \\
Q(\sqrt[4]{2}) \arrow[dr, dash, "2"'] & & Q(\xi_8) \arrow[dl, dash, "2"] \arrow[dr, dash, "2"] & \\
& Q(\sqrt{2}) \arrow[dr, dash, "2"'] & & Q(i) \arrow[dl, dash, "2"] \\
& & Q &
\end{tikzcd}$$

Rewriting $\xi_8 + \xi_8^{-1} = \sqrt{2}$ as $\xi_8^2 - \sqrt{2}\xi_8 + 1 = 0, \xi_8$ has degree at most 2 over $\mathbf{Q}(\sqrt[4]{2})$. Since ξ_8 is not real, isn't inside $\mathbf{Q}(\sqrt[4]{2})$, so it has degree 2 over $\mathbf{Q}(\sqrt[4]{2})$. Therefore $[\mathbf{Q}(\sqrt[4]{2},\xi_8) : \mathbf{Q}] = 2.4 = 8$ and the degrees marks as " $\leqslant 4$" in the diagram both equal 2.

Returning to the Galois group.(1.2) tells us the effect of $\sigma \in G^{\dagger}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q})$ on $\sqrt[4]{2}$ partially determines it on ξ_8, and conversely: $(\sigma(\sqrt[4]{2}))^2 = \sigma(\xi_8) + \sigma(\xi_8)^{-1}$, which in the notation of (1.1) is the same as

(1.3) $(-1)^b = \frac{\xi_8^a + \xi_8^{-a}}{\sqrt{2}}$

This tells us that if $a \equiv 1, 7$ mod 8 then $(-1)^b = 1$, so $b \equiv 0$, 2 mod 4, while if $a \equiv 3, 5$ mod 8 then $(-1)^b = -1$, so $b \equiv 1, 3$ mod 4.For example σ can't both fix $\sqrt[4]{2}(b = 0)$ and send ξ_8 to $\xi_8^3(a = 3)$ because (1.3) would not hold.

This simplest way to understand $\mathbf{Q}(\sqrt[4]{2})$ is to use a different set of generators.Since $\xi_8 = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}} = (1+i)/\sqrt{2})$,

$$\mathbf{Q}(\sqrt[4]{2},\xi_8) = \mathbf{Q}(\sqrt[4]{2}, i)$$

and from the second representation we know its Galois group over $\mathbf{Q}$ is isomorphic to D_4 with independent choices of where to send $\sqrt[4]{2}$ (to any fourth root of 2) and i (to any square root of -1) rather than $\sqrt[4]{2}$ and ξ_8.A different choice of field generators can make it easier to what Galois group looks like. We see immediately from the second representation that $[\mathbf{Q}(\sqrt[4]{2},\xi_8) : \mathbf{Q}] = 8$

Now we are moving to a very simple exercise problem.

3.3 Problem C

1.Let $f(t) = (t^2 - 2)(t^2 - 5)$ over $\mathbf{Q}$, and let $\mathbf{K}$ be a splitting field for f such that $K \subseteq \mathbf{R}$. In $\mathbf{R}$ we can factorize f as follows:

$$f(t) = (t - \sqrt{2})(t + \sqrt{2})(t - \sqrt{5})(t + \sqrt{5})$$

where $\sqrt{2}$ and $\sqrt{5}$ are real and positive.Clearly therefore $\mathbf{K} = \mathbf{Q}(\sqrt{2}, \sqrt{5})$.The characteristic is 0 and $\mathbf{K}$ is a splitting field, so that $\mathbf{K}$:$\mathbf{Q}$ is finite, separable, and normal.

2.We shall find the degree of $\mathbf{K}$:$\mathbf{Q}$.We have

$$[\mathbf{K} : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{5}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$$

The minimum polynomial of $\sqrt{2}$ over $\mathbf{Q}$ is $t^2 - 2$ since $(\sqrt{2})^2 - 2 = 0$ but $\sqrt{2} \in \mathbf{R} \supseteq \mathbf{Q}(\sqrt{2})$. So $[\mathbf{Q}(\sqrt{2}, \sqrt{5}) : \mathbf{Q}(\sqrt{2})] = 2$. Now $\sqrt{2}$ is a zero of f over $\mathbf{Q}$, and f is irreducible over $\mathbf{Q}(\sqrt{2})$ .Hence f is the minimum polynomial of $\sqrt{2}$ over $\mathbf{Q}$ and $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$. Therefore

$$[\mathbf{K} : \mathbf{Q}] = 2.2 = 4$$

3.We shall find the elements of the Galois group of $\mathbf{K}$:$\mathbf{Q}$.By a direct check,we see that there is $\mathbf{Q}$-automorphism σ of $\mathbf{K}$ such that

$$\sigma_1(\sqrt{2}) \;\; \textit{and} \;\; \sigma_2(\sqrt{5})$$

Product of these yield 4 distinct $\mathbf{Q}$-automorphism of $\mathbf{K}$, as follows:

$\sigma_1(\sqrt{2})$	$\sigma_2(\sqrt{5})$
$\sqrt{2}$	$\sqrt{5}$
$\sqrt{2}$	$-\sqrt{5}$
$-\sqrt{2}$	$\sqrt{5}$
$-\sqrt{2}$	$-\sqrt{5}$

other products do not give new automorphisms,

Now any $\mathbf{Q}$-automorphism of $\mathbf{K}$ sends $\sqrt{2}$ to some zero of $t^2 - 2$, so $\sqrt{2} \to^{+}_{-} \sqrt{2}$; similarly $\sqrt{5}$ is mapped to $\sqrt{5}, -\sqrt{5}$. All possible combinations of these(4 in number) appears in the above list, so these are precisely the $\mathbf{Q}$-automorphisms of $\mathbf{K}$.

4.The abstract structure of the Galois group $\mathbf{G}$ can be found. From the generator-relation presentation

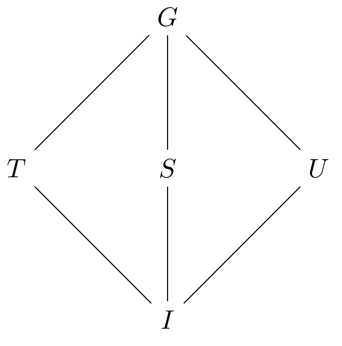
$$G =< \sigma_1(\sqrt{2}), \sigma_2(\sqrt{5}) : (\sigma_1(\sqrt{2}))^2 = 2, (\sigma_2(\sqrt{5}))^2 = 5 >$$

it follows that $\mathbf{G}$ is the cyclic group of order 2, which we shall write as $\mathbf{G} \simeq C_2 \times C_2$

5. It is an easy exercise to find the subgroups of G.If we let C_n denote the cyclic group of order n, and × the direct product, then the subgroups are as follows:

Order 4:G	$G \cong \mathbf{C}_2 \times \mathbf{C}_2$
Order 2:{1,$\sigma_1(\sqrt{2})$ }	$S \cong \mathbf{C}_2$
{1,$\sigma_2(\sqrt{5})$ }	$T \cong \mathbf{C}_2$
{1,$\sigma_1(\sqrt{2})\sigma_2(\sqrt{5})$ }	$U \cong \mathbf{C}_2$
Order 1:{1 }	$I \cong \mathbf{C}_1$

6 The inclusion relations between the subgroups of G can be summed up by the following *lattice diagram*:



7 Under the Galois correspondence we obtain the intermediate fields. Since the correspondence reverses inclusions this gives a lattice diagram of fields as follows:

$$\begin{tikzcd}
 & K = I^{\dagger} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
T^{\dagger} \arrow[dr, dash] & S^{\dagger} \arrow[d, dash] & U^{\dagger} \arrow[dl, dash] \\
 & G^{\dagger} &
\end{tikzcd}$$

8 We now describe the elements of these intermediate fields.

There are three obvious subfields of **K** degree 2 over Q, namely $Q(\sqrt{2}), Q(\sqrt{5}), Q(\sqrt{2}.\sqrt{5})$.These are clearly the fixed fields $S^{\dagger}, T^{\dagger} and\ U^{\dagger}$ (respectively).The other fixed fields are less obvious. Now any element of **K** can be expressed in the form

$$x = a_0 + a_1\sqrt{2} + a_2\sqrt{5} + a_3\sqrt{2}\sqrt{5} \quad where\ a_0, ..., a_3 \in \mathbf{Q}.$$

It is now easy to verify the inclusion relations determined by the lattice diagram of section 7.

9 If we check by hand that these are indeed the only intermediate fields.

10 The normal subgroups of G are G,S,T,U,I.By the theory, $G^{\dagger}, S^{\dagger}, T^{\dagger}, U^{\dagger}, I^{\dagger}$ should be the only normal extensions of **Q** which are contained in **K**.Since these are all splitting fields over **Q**.for the polynomial $t, t^2-5, t^2-2, t^2-(\sqrt{2}+\sqrt{5})t+\sqrt{2}\sqrt{5}, (t^2-2)(t^2-5)$ (respectively). They are normal extensions of **Q**.

Now If we multiply another polynomial of degree two with the previous problem then the next problem will be the solution.

3.4 Problem D

1.Let $f(t) = (t^2-2)(t^2-3)(t^2-5)$ over **Q**, and let **K** be a splitting field for f such that $K \subseteq \mathbf{R}$. In **R** we can factorize f as follows:

$$f(t) = (t-\sqrt{2})(t+\sqrt{2})(t-\sqrt{3})(t+\sqrt{3})(t-\sqrt{5})(t+\sqrt{5})$$

where $\sqrt{2}, \sqrt{3}$ and $\sqrt{5}$ are real and positive. Clearly therefore $\mathbf{K} = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.There characteristic is 0 and **K** is a splitting field, so that **K**:**Q** is finite, separable, and normal.

2.We shall find the degree of **K**:**Q**.We have

$$[\mathbf{K} : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbf{Q}(\sqrt{2}, \sqrt{3})][\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$$

The minimum polynomial of $\sqrt{2}$ over **Q** is t^2-2 since $(\sqrt{2})^2 - 2 = 0$ but $\sqrt{2} \in \mathbf{R} \supseteq \mathbf{Q}(\sqrt{2})$. So $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})] = 2$. Now $\sqrt{2}$ is a zero of f over **Q** , and f is irreducible over $\mathbf{Q}(\sqrt{2})$.Hence f is the minimum polynomial of $\sqrt{2}$ over **Q** and $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$. Similarly we have $[\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbf{Q}(\sqrt{2}, \sqrt{3})] = 2$. Therefore

$$[\mathbf{K} : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbf{Q}] = 2.2.2 = 8$$

3.We shall find the elements of the Galois group of **K**:**Q**.By a direct check,we see that there is **Q**-automorphism σ of **K** such that

$$\sigma_1(\sqrt{2})\ , \sigma_2(\sqrt{3})\ and\ \ \sigma_3(\sqrt{5})$$

Product of these yield 8 distinct **Q**-automorphism of **K**, as follows:

$\sigma_1(\sqrt{2})$	$\sigma_2(\sqrt{3}$	$\sigma_3(\sqrt{5})$
$\sqrt{2}$	$\sqrt{3}$	$\sqrt{5}$
$\sqrt{2}$	$\sqrt{3}$	$-\sqrt{5}$
$\sqrt{2}$	$-\sqrt{3}$	$\sqrt{5}$
$\sqrt{2}$	$-\sqrt{3}$	$-\sqrt{5}$
$-\sqrt{2}$	$\sqrt{3}$	$\sqrt{5}$
$-\sqrt{2}$	$\sqrt{5}$	$-\sqrt{5}$
$-\sqrt{2}$	$-\sqrt{5}$	$\sqrt{5}$
$-\sqrt{2}$	$-\sqrt{5}$	$-\sqrt{5}$

other products do not give new automorphisms,

Now any **Q**-automorphism of **K** sends $\sqrt{2}$ to some zero of $t^2 - 2$, so $\sqrt{2} \to^{+}_{-} \sqrt{2}$; similarly $\sqrt{3}$ is mapped to $\sqrt{3}, -\sqrt{3}$ and $\sqrt{5}$ is mapped to $\sqrt{5}, -\sqrt{5}$. All possible combinations of these(8 in number) appears in the above list, so these are precisely the **Q**-automorphisms of **K**.

4.The abstract structure of the Galois group G can be found.From the generator-relation presentation

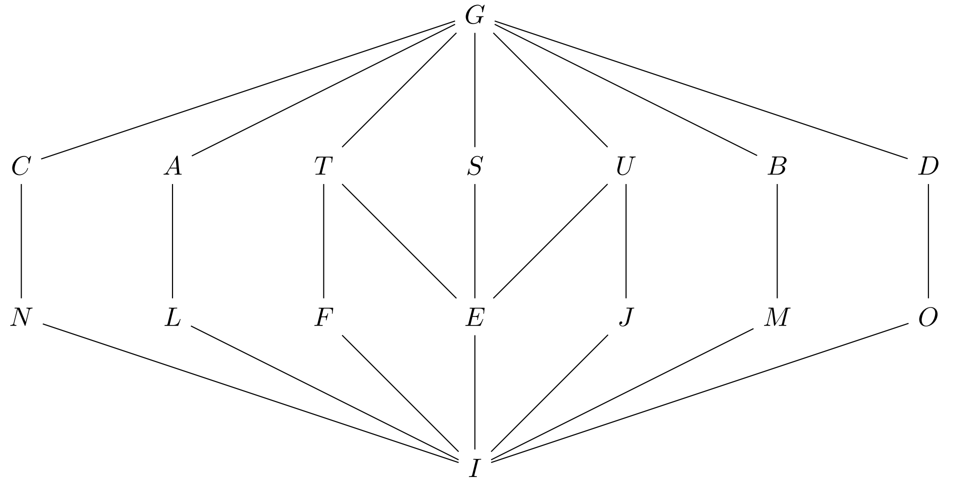
$$G =< \sigma_1(\sqrt{2}), \sigma_2(\sqrt{3}), \sigma_3(\sqrt{5}) : (\sigma_1(\sqrt{2}))^2 = 2, (\sigma_2(\sqrt{3}))^2 = 3, (\sigma_3(\sqrt{5}))^2 = 5 >$$

it follows that G is the cyclic group of order 2, which we shall write as $G \simeq \mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2$

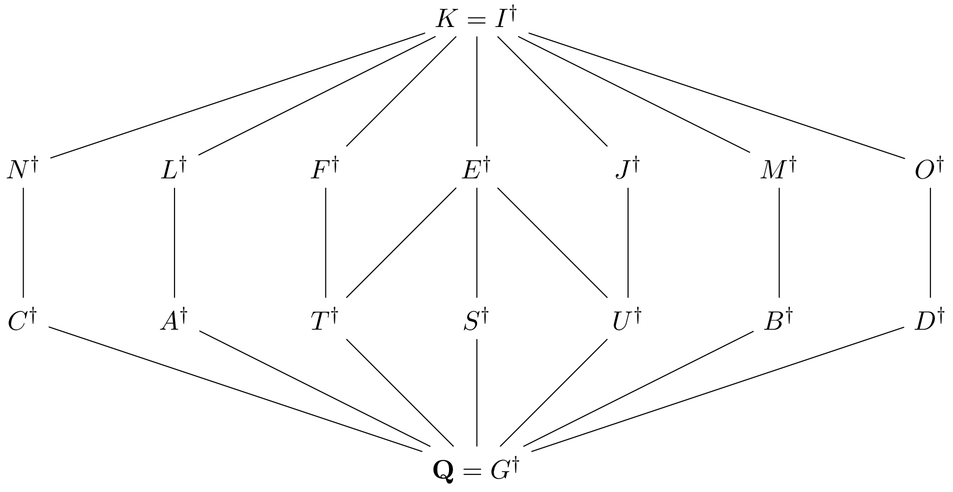
5. It is an easy exercise to find the subgroups of G. If we let C_n denote the cyclic group of order n, and × the direct product, then the subgroups are as follows:

Order 8:	G	$G \cong \mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2$
Order 4:	$\{1,\sigma_1(\sqrt{2}), \sigma_2(\sqrt{3}), \sigma_1(\sqrt{2})\sigma_2(\sqrt{3}))\ \}$	$S \cong \mathbf{C}_2 \times \mathbf{C}_2$
	$\{1,\sigma_2(\sqrt{3}), \sigma_3(\sqrt{5}), \sigma_2(\sqrt{3})\sigma_3(\sqrt{5}))\ \}$	$T \cong \mathbf{C}_2 \times \mathbf{C}_2$
	$\{1,\sigma_1(\sqrt{2}), \sigma_3(\sqrt{5}), \sigma_1(\sqrt{2})\sigma_3(\sqrt{5}))\ \}$	$U \cong \mathbf{C}_2 \times \mathbf{C}_2$
	$\{1,\sigma_1(\sqrt{2}), \sigma_2(\sqrt{3})\sigma_3(\sqrt{5}), \sigma_1(\sqrt{2})\sigma_2(\sqrt{3})\sigma_3(\sqrt{5}))\ \}$	$A \cong \mathbf{C}_2 \times \mathbf{C}_2$
	$\{1,\sigma_2(\sqrt{3}), \sigma_1(\sqrt{2})\sigma_3(\sqrt{5}), \sigma_1(\sqrt{2})\sigma_2(\sqrt{3})\sigma_3(\sqrt{5}))\ \}$	$B \cong \mathbf{C}_2 \times \mathbf{C}_2$
	$\{1,\sigma_3(\sqrt{5}), \sigma_1(\sqrt{2})\sigma_2(\sqrt{3}), \sigma_1(\sqrt{2})\sigma_2(\sqrt{3})\sigma_3(\sqrt{5}))\ \}$	$C \cong \mathbf{C}_2 \times \mathbf{C}_2$
	$\{1,\sigma_1(\sqrt{2})\sigma_2(\sqrt{3}), \sigma_1(\sqrt{2})\sigma_3(\sqrt{5}), \sigma_2(\sqrt{3})\sigma_3(\sqrt{5}))\ \}$	$D \cong \mathbf{C}_2 \times \mathbf{C}_2$
Order 2:	$\{1,\sigma_1(\sqrt{2})\ \}$	$E \cong \mathbf{C}_2$
	$\{1,\sigma_2(\sqrt{3})\ \}$	$F \cong \mathbf{C}_2$
	$\{1,\sigma_3(\sqrt{5})\ \}$	$J \cong \mathbf{C}_2$
	$\{1,\sigma_1(\sqrt{2})\sigma_2(\sqrt{3})\ \}$	$L \cong \mathbf{C}_2$
	$\{1,\sigma_2(\sqrt{3})\sigma_3(\sqrt{5})\ \}$	$M \cong \mathbf{C}_2$
	$\{1,\sigma_1(\sqrt{2})\sigma_3(\sqrt{5})\ \}$	$N \cong \mathbf{C}_2$
	$\{1,\sigma_1(\sqrt{2})\sigma_2(\sqrt{3})\sigma_3(\sqrt{5})\ \}$	$O \cong \mathbf{C}_2$
Order 1:	$\{1\ \}$	$I \cong \mathbf{C}_1$

6 The inclusion relations between the subgroups of G can be summed up by the following *lattice diagram*:



7 Under the Galois correspondence we obtain the intermediate fields. Since the correspondence reverses inclusions this gives a lattice diagram of fields as follows:



8 We now describe the elements of these intermediate fields.

There are seven obvious subfields of $\mathbf{K}$ degree 2 over Q,namely $Q(\sqrt{5}), Q(\sqrt{2}), Q(\sqrt{3}), Q(\sqrt{3}\sqrt{5}), Q(\sqrt{2}\sqrt{5}), Q(\sqrt{2}\sqrt{3}), Q(\sqrt{2}\sqrt{3})Q(\sqrt{5})$.These are clearly the fixed fields $S^\dagger, T^\dagger, U^\dagger, A^\dagger, B^\dagger, C^\dagger$ *and* $D^\dagger$ (respectively).The other fixed fields are less obvious.To illustrate a possible approach we shall find $C^\dagger$. Now any element of K can be expressed in the form

$$x = a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{5} + a_4\sqrt{2}\sqrt{3} + a_5\sqrt{3}\sqrt{5} + a_6\sqrt{2}\sqrt{5} + a_7\sqrt{2}\sqrt{3}\sqrt{5} \text{ } where \ a_0, ..., a_7 \in \mathbf{Q}.$$

So we have

$$S^\dagger = \mathbf{Q}(\sqrt{5}).$$

$$\begin{aligned}
&T^\dagger = \mathbf{Q}(\sqrt{2}).\\
&U^\dagger = \mathbf{Q}(\sqrt{3}).\\
&A^\dagger = \mathbf{Q}(\sqrt{3}\sqrt{5}).\\
&B^\dagger = \mathbf{Q}(\sqrt{2}\sqrt{5}).\\
&C^\dagger = \mathbf{Q}(\sqrt{2}\sqrt{3}).\\
&D^\dagger = \mathbf{Q}(\sqrt{2}\sqrt{3}\sqrt{5}).\\
&E^\dagger = \mathbf{Q}(\sqrt{3}, \sqrt{5}).\\
&F^\dagger = \mathbf{Q}(\sqrt{2}, \sqrt{5}).\\
&J^\dagger = \mathbf{Q}(\sqrt{2}, \sqrt{3}).\\
&L^\dagger = \mathbf{Q}(\sqrt{5}, \sqrt{2}\sqrt{3}).\\
&M^\dagger = \mathbf{Q}(\sqrt{2}, \sqrt{3}\sqrt{5}).\\
&N^\dagger = \mathbf{Q}(\sqrt{3}, \sqrt{2}\sqrt{5}).\\
&O^\dagger = \mathbf{Q}(\sqrt{2}\sqrt{3}, \sqrt{2}\sqrt{5}).
\end{aligned}$$

It is now easy to verify the inclusion relations determined by the lattice diagram of section 7.

9 If we check by hand that these are indeed the only intermediate fields.

10 The normal subgroups of G are G,S,T,U,E,F,J,I.By the theory, $G^\dagger, S^\dagger, T^\dagger, U^\dagger, E^\dagger, F^\dagger, J^\dagger, I^\dagger$ should be the only normal extensions of $\mathbf{Q}$ which are contained in $\mathbf{K}$. Since these are all splitting fields over $\mathbf{Q}$, for the polynomial $t, t^2-5, t^2-2, t^2-3, t^4-8t^2+15, t^4-7t^2+10, t^4-5t^2+6, (t^2-2)(t^2-3)(t^2-5)$ (respectively). They are normal extensions of $\mathbf{Q}$.On the other hand $A^\dagger$ is not normal since $t^2 - 15$ has a zero in $\sqrt{3}\sqrt{5}$. Similarly $B^\dagger, C^\dagger, D^\dagger, L^\dagger, M^\dagger, N^\dagger, O^\dagger$ are not normal extension of $\mathbf{Q}$.

3.5 Problem E

1.Let $f(t) = (t^4 + 1)$ over $\mathbf{Q}$, and let $\mathbf{K}$ be a splitting field for f such that $\mathbf{K} \subseteq \mathbf{C}$. In $\mathbf{C}$ we can factorize f as follows:

$$f(t) = (t^2 + t - 1)(t^2 - t - 1)$$

Now for $(t^2 + t - 1)$ we get

$$t = \frac{-1 \pm \sqrt{1+4}}{2} = \frac{-1 \pm \sqrt{5}}{2} = -\frac{1}{2} \pm \frac{\sqrt{5}}{2}$$

and for

$(t^2 - t - 1)$ we get

$$t = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2} = \frac{1}{2} \pm \frac{\sqrt{5}}{2}$$

So we get

$$f(t) = (t - (-\frac{1}{2} + \frac{\sqrt{5}}{2}))(t - (-\frac{1}{2} - \frac{\sqrt{5}}{2}))(t - (\frac{1}{2} + \frac{\sqrt{5}}{2}))(t - (\frac{1}{2} - \frac{\sqrt{5}}{2}))$$

where $\frac{1}{2}$ and $\frac{\sqrt{5}}{2}$ are real and positive.Clearly therefore $\mathbf{K} = \mathbf{Q}(\frac{1}{2} \pm \frac{\sqrt{5}}{2}) = \mathbf{Q}(\sqrt{5})$.There characteristic is 0 and $\mathbf{K}$ is a splitting field, so that $\mathbf{K}$:$\mathbf{Q}$ is finite,separable, and normal.

2.We shall find the degree of $\mathbf{K}$:$\mathbf{Q}$.We have

$$[\mathbf{K} : \mathbf{Q}] = [Q(\sqrt{5}) : \mathbf{Q}]$$

The minimum polynomial of $\sqrt{5}$ over $\mathbf{Q}$ is $t^2 - 5$ since $(\sqrt{5})^2 - 5 = 0$ but $\sqrt{5} \in \mathbf{R} \supseteq \mathbf{Q}(\sqrt{5})$. So $[Q(\sqrt{5}) : \mathbf{Q}] = 2$. Now $\sqrt{5}$ is a zero of $t^2 - 5$ over $\mathbf{Q}$. Hence $t^2 - 5$ is the minimum polynomial of $\sqrt{5}$ over $\mathbf{Q}$ Therefore

$$[\mathbf{K} : \mathbf{Q}] = 2$$

3.We shall find the elements of the Galois group of $\mathbf{K}$:$\mathbf{Q}$.By a direct check,we see that there is only one $\mathbf{Q}$-automorphism σ of $\mathbf{K}$ such that

$$\sigma(\sqrt{5}) = \sqrt{5}, \qquad \sigma(\frac{1}{2} + \frac{\sqrt{5}}{2}) = \frac{1}{2} + \frac{\sqrt{5}}{2}$$

Now any $\mathbf{Q}$-automorphism of K sends $\sqrt{5}$ to some zero of $t^2 - 5$, so $\sqrt{5} \to^{-}_{+} \sqrt{5}$; similarly $\frac{1}{2} + \frac{\sqrt{5}}{2}$ is mapped to $\frac{1}{2} + \frac{\sqrt{5}}{2}, \frac{1}{2} - \frac{\sqrt{5}}{2}$. All possible combinations of these(2 in number) appears in the above list,so these are precisely the $\mathbf{Q}$-automorphisms of $\mathbf{K}$.

4.The abstract structure of the Galois group G can be found.

it follows that G is the cyclic group of order 2, which we shall write as $G \simeq \mathbf{C}/_2$

5. It is an easy exercise to find the subgroups of G.If we let C_n denote the cyclic group of order n, and × the direct product, then the subgroups are as follows:

Order 2:G	$G \cong \mathbf{C}_2$
Order 1:{1 }	$I \cong \mathbf{C}_1$

6 The inclusion relations between the subgroups of G can be summed up by the following *lattice diagram*:

$$\begin{tikzcd} G \arrow[d, dash] \\ I \end{tikzcd}$$

7 Under the Galois correspondence we obtain the intermediate fields. Since the correspondence reverses inclusions this gives a lattice diagram of fields as follows:

$$\begin{tikzcd} K = I^{\dagger} \arrow[d, dash] \\ \mathbf{Q} = G^{\dagger} \end{tikzcd}$$

8 We now can see that no elements of these intermediate field.

There are no subfields of $\mathbf{K}$ over Q,

3.6 Problem F

1.Let $f(t) = (t^4 - 3t^2 + 4)$ over $\mathbf{Q}$,and let $\mathbf{K}$ be a splitting field for f such that $K \subseteq \mathbf{C}$.In $\mathbf{C}$ we can factorize f as follows:

$$f(t) = (t^2 - \sqrt{7}t + 2)t^2 + \sqrt{7}t + 2))$$

Now for $t^2 - \sqrt{7}t + 2$ we get

$$t = \frac{\sqrt{7} \pm \sqrt{7 + 4.2}}{2} = \frac{\sqrt{7} \pm \sqrt{-1}}{2} = -\frac{\sqrt{7}}{2} \pm \frac{i}{2}$$

and for

$t^2 + \sqrt{7}t + 2$ we get

$$t = \frac{-\sqrt{7} \pm \sqrt{7 + 4.2}}{2} = \frac{-\sqrt{7} \pm \sqrt{-1}}{2} = \frac{-\sqrt{7}}{2} \pm \frac{i}{2}$$

So we get

$$f(t) = (t - (\frac{\sqrt{7}}{2} + \frac{i}{2}))(t - (\frac{\sqrt{7}}{2} - \frac{i}{2}))(t - (\frac{-\sqrt{7}}{2} + \frac{i}{2}))(t - (\frac{-\sqrt{7}}{2} - \frac{i}{2}))$$

where $\frac{\sqrt{7}}{2}$ *and* $\frac{1}{2}$ are real and positive.Clearly therefore $\mathbf{K} = \mathbf{Q}(\frac{\sqrt{7}}{2} + \frac{1}{2}, i) = \mathbf{Q}(\sqrt{7}, i)$.There characteristic is 0 and $\mathbf{K}$ is a splitting field, so that $\mathbf{K}$:$\mathbf{Q}$ is finite,separable, and normal.

2.We shall find the degree of $\mathbf{K}$:$\mathbf{Q}$.We have

$$[\mathbf{K} : \mathbf{Q}] = [\mathbf{Q}(\sqrt{7}, i) : \mathbf{Q}(\sqrt{7})][\mathbf{Q}(\sqrt{7}) : \mathbf{Q}]$$

The minimum polynomial of i over $\mathbf{Q}$ is $t^2 + 1$ since $(i)^2 + 1 = 0$ but $i \notin \mathbf{R} \supseteq \mathbf{Q}(\sqrt{7})$. So $[\mathbf{Q}(\sqrt{7}, i) : \mathbf{Q}(\sqrt{7})] = 2$. Now $\sqrt{7}$ is a zero of $t^2 - 7$ over $\mathbf{Q}$, and $t^2 - 7$ is irreducible by Eisenstein's criterion.Hence $t^2 - 7$ is the minimum polynomial of

$\sqrt{7}$ over $\mathbf{Q}$ and $[\mathbf{Q}(\sqrt{7}) : \mathbf{Q}] = 2$. Therefore

$$[\mathbf{K} : \mathbf{Q}] = 2.2 = 4$$

3.We shall find the elements of the Galois group of $\mathbf{K}$:$\mathbf{Q}$.By a direct check,we see that there is $\mathbf{Q}$-automorphism σ of $\mathbf{K}$ such that

$$\sigma(i) = i, \qquad \sigma(\frac{\sqrt{7}}{2} + \frac{1}{2}) = \frac{\sqrt{7}}{2} + i\frac{1}{2}$$

and another ,τ,such that

$$\tau(i) = -i, \qquad \tau(\frac{\sqrt{7}}{2} + \frac{1}{2}) = \frac{\sqrt{7}}{2} - i\frac{1}{2}$$

Product of these yield 4 distinct $\mathbf{Q}$-automorphism of $\mathbf{K}$, as follows:

automorphism	effect on $\frac{\sqrt{7}}{2} + \frac{1}{2}$	effect on i
1	$\frac{\sqrt{7}}{2} + \frac{1}{2}$	i
σ	$\frac{\sqrt{7}}{2} + i\frac{1}{2}$	i
τ	$\frac{\sqrt{7}}{2} - i\frac{1}{2}$	-i
$\sigma\tau$	$\frac{\sqrt{7}}{2} + \frac{1}{2}$	-i

other products do not give new automorphisms,since $\sigma^2 = 1, \tau^2 = 1$

Now any $\mathbf{Q}$-automorphism of K sends i to some zero of $t^2 + 1$,so $i \rightarrow^{+}_{-} i$;similarly $\frac{\sqrt{7}}{2} + \frac{1}{2}$ is mapped to $\frac{\sqrt{7}}{2} + \frac{1}{2}$, $\frac{\sqrt{7}}{2} + i\frac{1}{2}$, $\frac{\sqrt{7}}{2} - i\frac{1}{2}$ .All possible combinations of these(4 in number) appears in the above list,so these are precisely the $\mathbf{Q}$-automorphisms of $\mathbf{K}$.

4.The abstract structure of the Galois group G can be found.From the generator-relation presentation

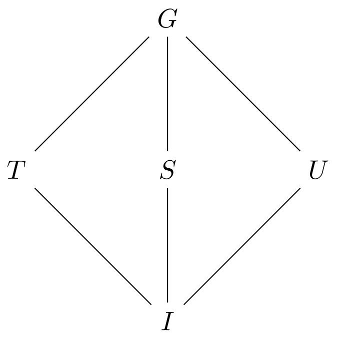
$$G =< \sigma, \tau : \sigma^2 = \tau^2 >$$

it follows that G is the Cyclic group of order 4, which we shall write as $\mathbf{C}_4$

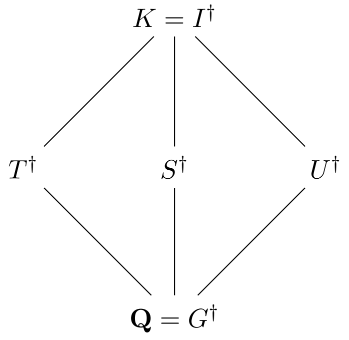
5. It is an easy exercise to find the subgroups of G.If we let C_n denote the cyclic group of order n, and × the direct product, then the subgroups are as follows:

Order 4:G	$G \cong \mathbf{C}_2 \times \mathbf{C}_2$
Order 2:{1,σ }	$S \cong \mathbf{C}_2$
{1,τ }	$T \cong \mathbf{C}_2$
{1,$\sigma\tau$ }	$U \cong \mathbf{C}_2$
Order 1:{1 }	$I \cong \mathbf{C}_1$

6 The inclusion relations between the subgroups of G can be summed up by the following *lattice diagram*:



7 Under the Galois correspondence we obtain the intermediate fields. Since the correspondence reverses inclusions this gives a lattice diagram of fields as follows:



8 We now describe the elements of these intermediate fields.

There are three obvious subfields of **K** degree 2 over Q,namely $Q(\frac{\sqrt{7}}{2}+\frac{1}{2}), Q(\frac{\sqrt{7}}{2}+i\frac{1}{2}), Q(\frac{\sqrt{7}}{2}-i\frac{1}{2})$.These are clearly the fixed fields $S^\dagger, T^\dagger and\ U^\dagger$ (respectively).The other fixed fields are less obvious. Now any element of K can be expressed in the form

$$x = a_0 + a_1(\frac{\sqrt{7}}{2}+\frac{1}{2}) + a_2(\frac{\sqrt{7}}{2}+i\frac{1}{2}) + a_3(\frac{\sqrt{7}}{2}-i\frac{1}{2})\ where\ a_0, ..., a_3 \in \mathbf{Q}.$$

We have

$$S^\dagger = \mathbf{Q}(\frac{\sqrt{7}}{2}+\frac{1}{2}).$$

$T^\dagger = \mathbf{Q}(\frac{\sqrt{7}}{2}+\frac{1}{2}, i).$
$U^\dagger = \mathbf{Q}(\frac{-\sqrt{7}}{2}+\frac{1}{2}, i).$

It is now easy to verify the inclusion relations determined by the lattice diagram of section 7.

9 If we check by hand that these are indeed the only intermediate fields.

10 The normal subgroups of G are G,T,U,I.By the theory,$G^\dagger, T^\dagger, U^\dagger, I^\dagger$ should be the only normal extensions of **Q** which are contained in **K**.Since these are all splitting fields over **Q**.for the polynomial $t, t^2 - (\frac{\sqrt{7}}{2} - i\frac{1}{2}), t^2 - (\frac{\sqrt{7}}{2} + i\frac{1}{2}), t^2 + t + 1$ (respectively)they are normal extensions of **Q**.On the other hand $S^\dagger : \mathbf{Q}$ is not normal,since

$(t^2 - (\frac{\sqrt{7}}{2} + \frac{1}{2})^2)$ has a zero, namely $(\frac{-\sqrt{7}}{2} + \frac{1}{2})$ in $S^\dagger$ but does not split in $S^\dagger$.
Similarly by fixing

$$\sigma(-\frac{\sqrt{7}}{2} + \frac{1}{2}) = -\frac{\sqrt{7}}{2} + i\frac{1}{2}$$

and

$$\tau(-\frac{\sqrt{7}}{2} + \frac{1}{2}) = -\frac{\sqrt{7}}{2} - i\frac{1}{2}$$

we the Polynomials $t, t^2 - (-\frac{\sqrt{7}}{2} + i\frac{1}{2})^2, t^2 - (-\frac{\sqrt{7}}{2} - i\frac{1}{2})^2, t^2 - t + 1$, (respectively).
They are also normal extensions of $\mathbf{Q}$.

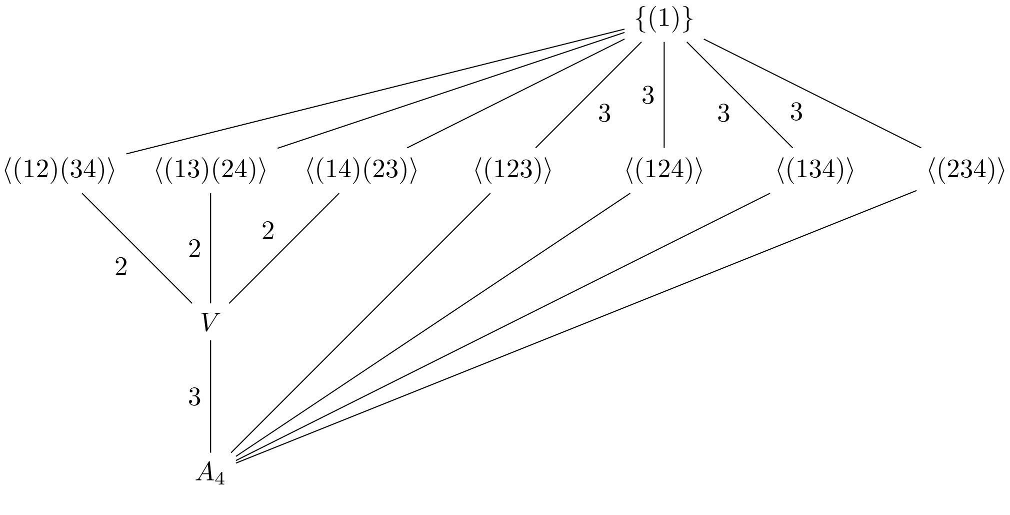
3.7 Problem G

We determine the Galois group of $X^4 + 8X + 12$ over $\mathbf{Q}$. This is reducible mod p for all small p, so the reduction mod p test doesn't help us prove the polynomial is irreducible over Q. (In fact, the polynomial factors mod p for all p, so the reduction mod p test really doesn't apply. It's not an artifact of only looking at small primes.) Let's look at how the polynomial factors into irreducibles modulo different primes:

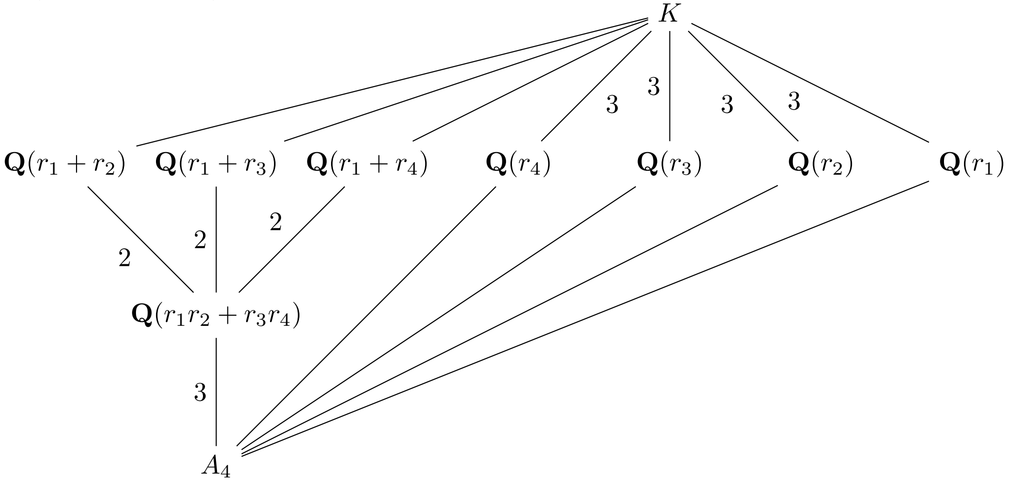
$$X^4 + 8X + 12 \equiv (X + 1)(X^3 + 4X^2 + X + 2) \ mod\ 5;$$

$$X^4 + 8X + 12 \equiv (X^2 + 4X + 7)(X^2 + 13X + 9) \ mod\ 17 :$$

These are only consistent with $X^4 + 8X + 12$ being irreducible over $\mathbf{Q}$. By the irreducibility of the polynomial, the Galois group of $X^4 + 8X + 12$ over $\mathbf{Q}$ has size divisible by 4. The discriminant of $X^4 + 8X + 12$ is $331776 = 5762$, a rational square, so the Galois group is a subgroup of A_4 and therefore has size 4 or 12. From the factorization of the polynomial mod 5 above, the Galois group contains a permutation of the roots whose cycle type is $(1, 3)$, which is a 3-cycle, so the Galois group has order divisible by 3, and thus its size is 12. So the Galois group of $X^4 + 8X + 12$ over $\mathbf{Q}$ is isomorphic to A_4 : the even permutations of the roots extend to automorphisms of the splitting field over $\mathbf{Q}$, while the odd permutations do not. Let's list all the subfields of the splitting field of $X^4 + 8X + 12$ over $\mathbf{Q}$. Here is the lattice (upside down) of subgroups of A_4.



The corresponding subfield lattice of $\mathbf{K} = Q(r_1, r_2, r_3, r_4)$ is as follows.



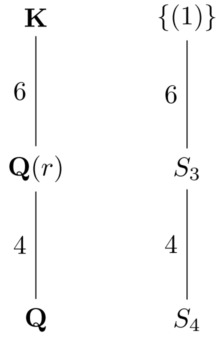
The normal subgroups of A_4 are 1, V , and A_4, so the only subfield of $\mathbf{K}$ that is Galois over $\mathbf{Q}$ other than $\mathbf{K}$ and $\mathbf{Q}$ is $\mathbf{Q}(r_1r_2 + r_3r_4)$. Since $[\mathbf{K} : \mathbf{Q}(r_1)] = 3$ is prime and $r_2 \notin \mathbf{Q}(r_1)$, we have $\mathbf{K} = \mathbf{Q}(r_1; r_2)$, so $[\mathbf{Q}(r_1; r_2) : \mathbf{Q}] = 12$. The sums $r_1 + r_2$, $r_1 + r_3$, and $r_1 + r_4$ are roots of $X^6 - 48X^2 - 64$ and $r_1r_2 + r_3r_4$ is a root of $X^3 - 48X - 64$. Roots of $X^3 - 48X - 64$ are squares of roots of $X^6 - 48X^2 - 64$.

3.8 Problem G

We compute the Galois group of $X^4 - X - 1$ over $\mathbf{Q}$ using Dedekind Theorem .This polynomial is irreducible mod 2, so it is irreducible over $\mathbf{Q}$. Let its roots be r_1, r_2, r_3, r_4. The extension $Q(r_1)/Q$ has degree 4, so the Galois group of $X^4 - X - 1$ over $\mathbf{Q}$ has order divisible by 4. Since the Galois group embeds into S_4, its size is either 4,8, 12, or 24. The discriminant of $X^4 - X - 1$ is -283, which is not a rational square, so the Galois group is not a subgroup of A_4. This eliminates the possibility of the Galois group having order 12, because the only subgroup of S4 with order 12 is A_4. (Quite generally, the only subgroup of index 2 in S_n is An for $n \geq 2$.) There are subgroups of S_4 with orders 4, 8, and (of course) 24 outside of A_4, so no other size but 12 is eliminated yet. We will use Dedekind Theorem to show the Galois group has order divisible by 3, and this will prove the Galois group is S_4 since 4 and 8 are not divisible by 3. Using Dedekind Theorem with $p = 7$,

$$X^4 - X - 1 \equiv (X + 4)(X^3 + 3X^2 + 2X + 5) \ \mathit{mod}\ 7 :$$

This is an irreducible factorization, so the Galois group of $X^4 - X - 1$ over $\mathbf{Q}$ contains a permutation of the roots with cycle type $(1, 3)$, which means there is a 3-cycle in the Galois group. Any 3-cycle has order 3. This Galois group computation has an application to constructible numbers. A necessary condition for a complex number to be constructible (using only an unmarked straightedge and compass) is that the number has 2-power degree over Q. This necessary condition is not sufficient: if r is a root of $X^4 - X - 1$ then $[\mathbf{Q}(r) : \mathbf{Q}] = 4$ and we will show r is not a constructible number by showing there is no quadratic field in Q(r). Let $\mathbf{K}$ be a splitting field of $X^4 - X - 1$ over $\mathbf{Q}$, so the permutations of its roots by $G^{\dagger}(\mathbf{K/Q})$ is an isomorphism with S_4. The subgroup $G^{\dagger}(\mathbf{K/Q}(r))$ corresponds to a sub-group of S_4 fixing one of the four numbers, which is a group isomorphic to S_3. (The subgroups of any S_n fixing one number are all conjugate to each other, and in fact are all of the subgroups of index n in S_n.)



There is no subgroup of S_4 strictly between S_3 and S_4 : if there were it would be a subgroup of index 2 and thus has to be A_4, but $S_3 \not\subset A_4$. (There is no subgroup of order 6 in A_4.) So by the Galois correspondence, there is no field properly between Q and Q(r).

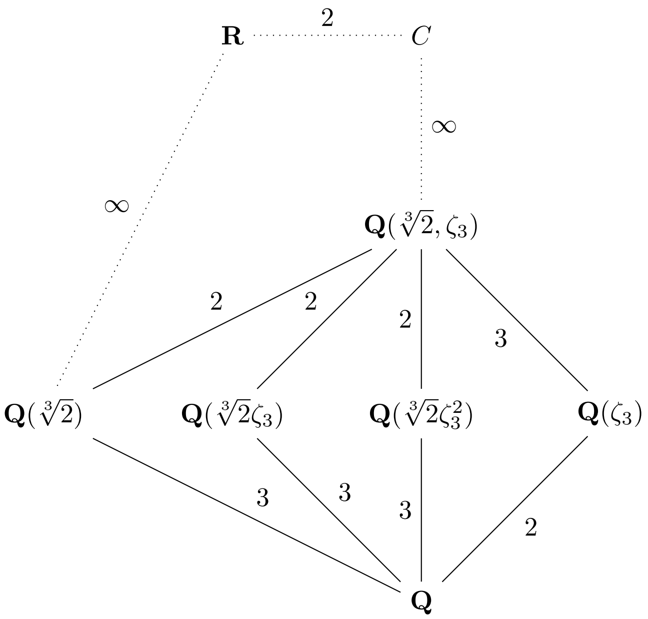
3.9 Problem H

A splitting field $\mathbf{K}/\mathbf{Q}$ for $p(X) = X^3 - 2$ over $\mathbf{Q}$ and determine $[\mathbf{K} : \mathbf{Q}]$. By the Eisenstein Criterion , p(X) is irreducible over $\mathbf{Q}$. One root of p(X) is $\sqrt[3]{2} \in \mathbf{R}$ so we adjoin this to $\mathbf{Q}$ to form an extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ of degree 3. Now

$$p(X) = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + (\sqrt[3]{2})^2)$$

and the second factor has the non-real complex roots $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$ lying in the extension $\mathbf{Q}(\sqrt[3]{2}\zeta_3)/\mathbf{Q}(\sqrt[3]{2})$ of degree 2. So the splitting subfield of $X^3 - 2$ in $\mathbf{C}$ over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ with $[\mathbf{Q}(\sqrt[3]{2}, \zeta_3) : \mathbf{Q}] = 6$.

An alternative strategy would have been to adjoin one of the other roots $\sqrt[3]{2}\zeta_3$ or $\sqrt[3]{2}\zeta_3^2$ first. We could also have begun by adjoining ζ_3 to form the extension $\mathbf{Q}(\zeta_3)/\mathbf{Q}$ but none of the roots of p(X) lie in this field so the extension $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)/\mathbf{Q}(\zeta_3)$ of degree 3 is obtained by adjoining one and hence all of the roots. Figure shows all the subfields of the extension $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)/\mathbf{Q}$


$\mathbf{R}$
2
C
∞
∞
$\mathbf{Q}(\sqrt[3]{2}, \zeta_3)$
2
2
2
3
$\mathbf{Q}(\sqrt[3]{2})$
$\mathbf{Q}(\sqrt[3]{2}\zeta_3)$
$\mathbf{Q}(\sqrt[3]{2}\zeta_3^2)$
$\mathbf{Q}(\zeta_3)$
3
3
3
2
$\mathbf{Q}$

We will build up the list of monomorphisms in stages. First consider monomorphisms that fix $\sqrt[3]{2}$ and hence fix the subfield $\mathbf{Q}(\sqrt[3]{2})$.These form the subset

$$Mono_{\mathbf{Q}(\sqrt[3]{2})}(\mathbf{Q}((\sqrt[3]{2}, \zeta_3), \mathbf{C}) \subseteq Mono_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}, \zeta_3), \mathbf{C}).$$

We know that $\mathbf{Q}((\sqrt[3]{2}, \zeta_3) = \mathbf{Q}(\sqrt[3]{2})(\zeta_3)$ and that ζ_3 is a root of the irreducible cyclotomic polynomial $\Phi_3(X) = X^2 + X + 1 \in \mathbf{Q}(\sqrt[3]{2})[X]$. So there are two monomorphisms id, a_0 fixing $\mathbf{Q}(\sqrt[3]{2})$, where ?0 has the effect

$$\alpha_0 : \begin{pmatrix} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3^2 \end{pmatrix}.$$

Next we consider monomorphisms that send $\sqrt[3]{2}$ to $\sqrt[3]{2}\zeta_3$. This time we have 2 distinct ways to extend to elements of $Mono_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}, \zeta_3), \mathbf{Q}(\sqrt[3]{2}, \zeta_3))$ since again we can send ζ_3 to either ζ_3 or ζ_3^2 The possibilities are

$$\alpha_1 : \begin{pmatrix} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3 \\ \zeta_3 \mapsto \zeta_3 \end{pmatrix},$$

$$\alpha_1' : \begin{pmatrix} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3 \\ \zeta_3 \mapsto \zeta_3^2 \end{pmatrix}.$$

Finally we consider monomorphisms that send $\sqrt[3]{2}$ to $\sqrt[3]{2}\zeta_3^2$. There are again two possibilities

$$\alpha_2 : \left(\begin{array}{c} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2 \\ \zeta_3 \mapsto \zeta_3 \end{array} \right),$$

$$\alpha_2' : \left(\begin{array}{c} \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2 \\ \zeta_3 \mapsto \zeta_3^2 \end{array} \right).$$

These are all 6 of the required monomorphisms. It is also the case here that

$$Mono_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}, \zeta_3), \mathbf{C}) = Mono_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}, \zeta_3), \mathbf{Q}(\sqrt[3]{2}, \zeta_3)) = Aut_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}, \zeta_3)),$$

so these form a group. It is a nice exercise to show that $Aut_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}, \zeta_3)) \cong S_3$, the symmetric group on 3 objects. It is also worth remarking that $[Aut_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}, \zeta_3))] = [\mathbf{Q}(\sqrt[3]{2}, \zeta_3) : \mathbf{Q}]$

First take the 3 roots of the polynomial $X^3 - 2$ for which E is the splitting field over Q; these are $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$ which we number in the order they are listed. Then the monomorphisms $id, \alpha_0, \alpha_1, \alpha_1', \alpha_2, \alpha_2'$ extend to automorphisms of E,each of which permutes these 3 roots in the following ways given by cycle notation:

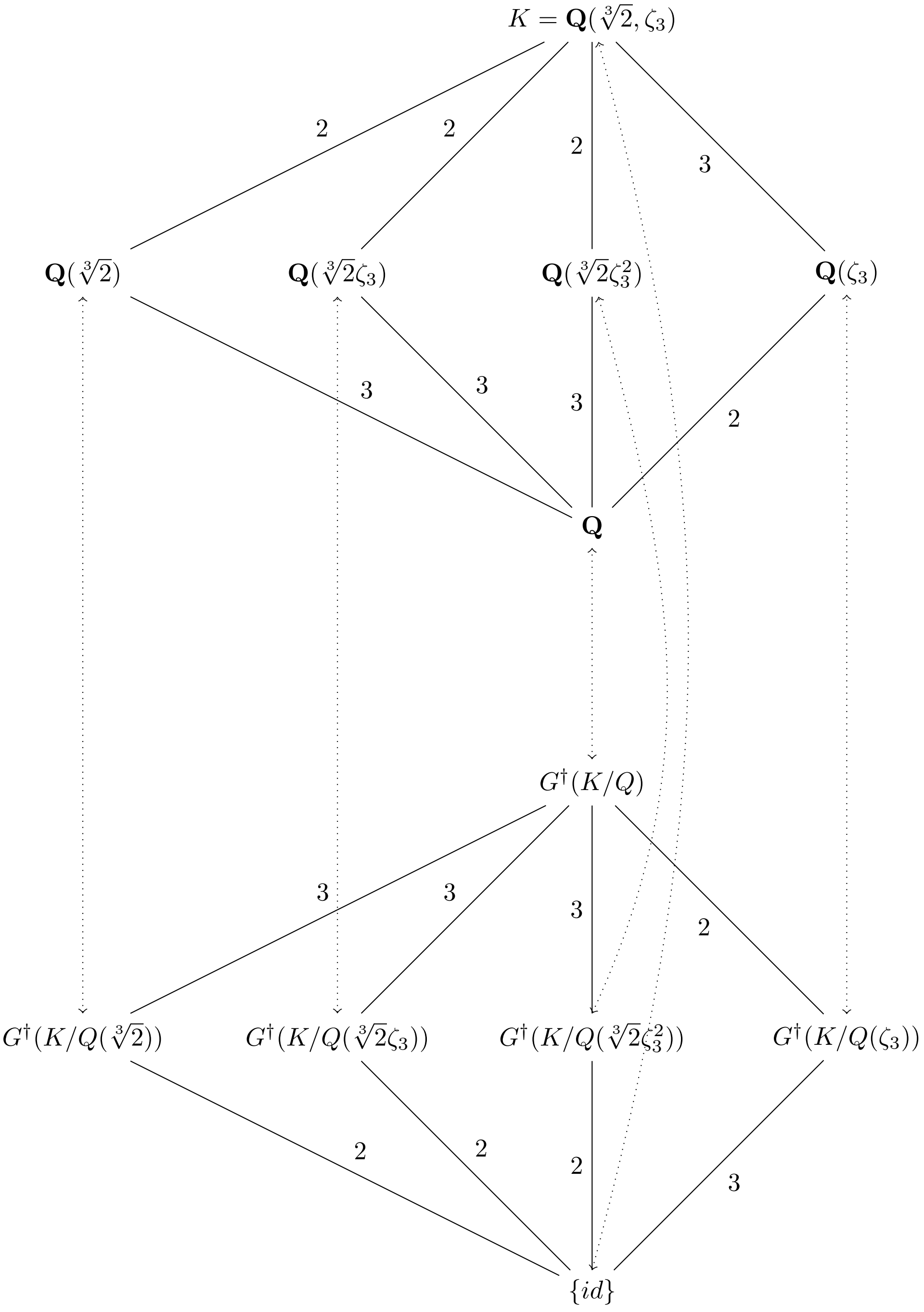

$K = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$
2
2
2
3
$\mathbf{Q}(\sqrt[3]{2})$
$\mathbf{Q}(\sqrt[3]{2}\zeta_3)$
$\mathbf{Q}(\sqrt[3]{2}\zeta_3^2)$
$\mathbf{Q}(\zeta_3)$
3
3
3
2
$\mathbf{Q}$
$G^\dagger(K/Q)$
3
3
3
2
$G^\dagger(K/Q(\sqrt[3]{2}))$
$G^\dagger(K/Q(\sqrt[3]{2}\zeta_3))$
$G^\dagger(K/Q(\sqrt[3]{2}\zeta_3^2))$
$G^\dagger(K/Q(\zeta_3))$
2
2
2
3
$\{id\}$

Figure The Galois Correspondence for $\mathbf{K} = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)/\mathbf{Q}$

We find that
$G^\dagger(K/Q(\zeta_3)) = \{id, \alpha_1, \alpha_2\} \cong \{id, (123), (132)\}$
$G^\dagger(K/Q(\sqrt[3]{2})) = \{id, \alpha_0\} \cong \{id, (23)\}$
$G^\dagger(K/Q(\sqrt[3]{2}\zeta_3)) = \{id, \alpha_2'\} \cong \{id, (13)\}$
$G^\dagger(K/Q(\sqrt[3]{2}\zeta_3^2)) = \{id, \alpha_1'\} \cong \{id, (12)\}$
Notice that $\{id, (123), (132)\} \lhd S_3$ and so $\mathbf{Q}(\zeta_3)/\mathbf{Q}$ is a normal extension.Of course $\mathbf{Q}(\zeta_3)$ is the splitting field of $X^3 - 1$ over $\mathbf{Q}$. [3] [4] [7] [8]

4 Conclusion

Galois Theory is a showpiece of Mathematical unification,bringing together several different branches of the subject and creating a powerful machine for the study of problems of considerable historical and mathematical importance.

Here, some problems are are presented in the context of Galois theory to illustrate the importance of this theory with respect to field extensions.

References

[1] A. C. David, *Galois Theory,*Wiley, ISBN$978-1-11807205-9$, 2012.

[2] I. Stewart, *Galois Theory*, Chapman and Hall, 1989.

[3] A. Baker, *An Introduction to Galois Theory*, School of Mathematics and Statistics, University of Glasgow, 2013.

[4] J. A. Beachy and W. D. Blair, *Abstract Algebra,*Online Study Guide, Chapter 8, 2000

[5] H. M. Edwards,*Galois Theory,*Graduate Texts in Mathematics, 1984.

[6] M. Postnikov,*Foundations of Galois Theory*, New York, Pegamon, 2004.

[7] J. Swallow, Exploratory Galois Theory,ISBN $0-521-54499-8$,2004.

[8] J.S. Milne, *Fields and Galois Theory,*Version 4.40,2013.