



Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin

Ollscoil Átha Cliath | The University of Dublin

Faculty of Science, Technology, Engineering and Mathematics

School of Mathematics

JS/SS Maths/TP/TJH

Semester 2, 2021

MAU34101 Galois theory

Never

Nowhere

Ever

Dr. Nicolas Mascot

Instructions to candidates:

Additional instructions for this examination:

This is a mock exam paper for revision purposes only.

You may not start this examination until you are instructed to do so by the Invigilator.

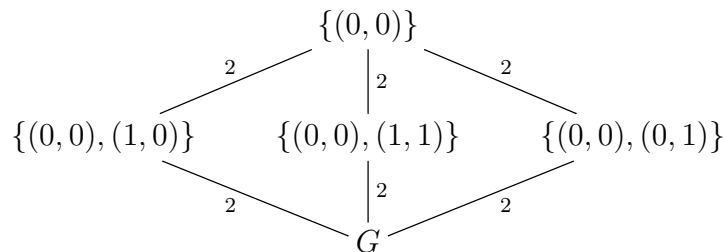
Question 1 *Subgroups for appetiser*

Sketch a diagram showing all the subgroups of G when:

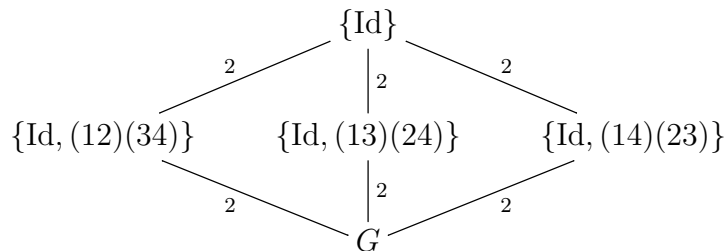
1. $G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$,
2. $G = V_4 = \{\text{Id}, (12)(34), (13)(24), (14)(23)\} < S_4$,
3. $G = S_3$,
4. $G = \mathbb{Z}/n\mathbb{Z}$, for n up to 12.

Solution 1

1. G has order 4, so any nontrivial subgroup must have order 2. A group of order 2 must be of the form $\{1_G, g\}$ where $g^2 = 1_G$ but $g \neq 1_G$, i.e. g has order exactly 2; conversely, if g has order exactly 2, then $\{1_G, g\}$ is a subgroup of G . Since $1_G = (0, 0)$ and since all the other elements of G have order 2:

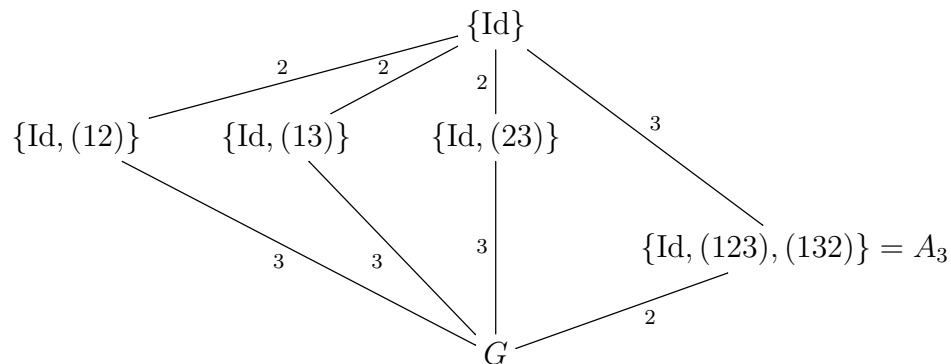


2. Same logic as for $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ (and in fact these two groups are isomorphic).



3. This time $\#G = 6$ so the possible orders for subgroups are 2 and 3. As before, subgroups of order 2 correspond to elements of order 2, i.e. transpositions in this case. Similarly, if H is a subgroup of order 3 and $\text{Id} \neq g \in H$, then by Lagrange g must have order 3

so $H = \{Id, g, g^2 = g^{-1}\}$; and conversely any element of order 3 (i.e. 3-cycle) gives us a subgroup of order 3. So



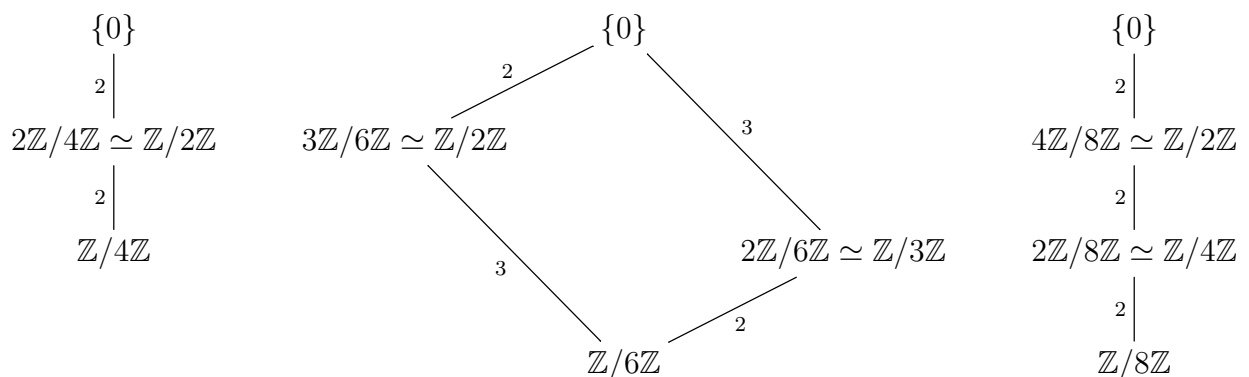
4. Subgroups of cyclic groups are also cyclic. Besides, for each $d \mid n$ we have the subgroup $d\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{d}\mathbb{Z}$, and that's all the subgroups.

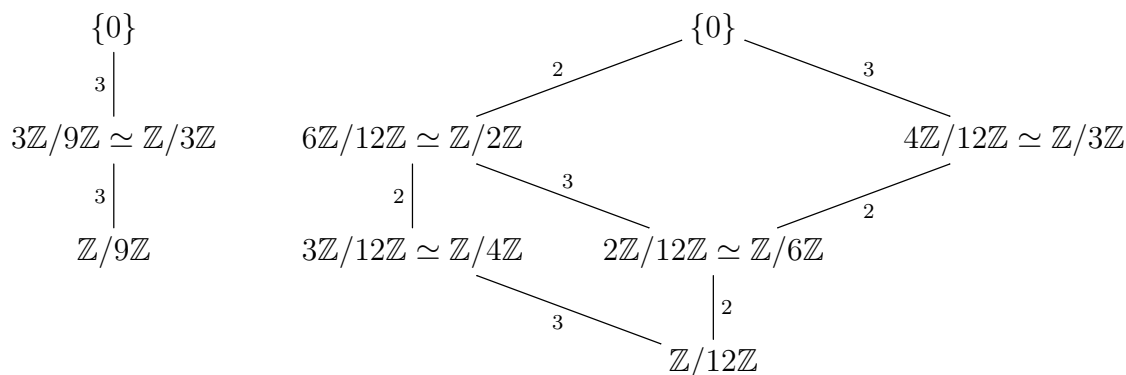
For $n = 1$, G is the trivial group.

For $n = 2, 3, 5, 7, 11$, n is prime, so no nontrivial subgroup:

$$\begin{array}{c} \{0\} \simeq n\mathbb{Z}/n\mathbb{Z} \\ n \mid \\ \mathbb{Z}/n\mathbb{Z} \end{array}$$

The remaining cases are a little more interesting:





Question 2 *Bookwork*

Let $K \subset L$ be a finite extension, and let $\Omega \supset K$ be algebraically closed. Which inequalities do we always have between $[L : K]$, $\# \text{Aut}_K(L)$, $\# \text{Hom}_K(L, \Omega)$? When are they equalities? State equivalent conditions.

Solution 2

We always have

$$\# \text{Aut}_K(L) \leq \# \text{Hom}_K(L, \Omega) \leq [L : K].$$

The left inequality is an equality iff. L is *normal* over K , which means that there exists $F(x) \in K[x]$ such that L is (K -isomorphic to) the splitting field of F over K . An equivalent characterisation is that any *irreducible* $P(x) \in K[x]$ having one root in L must split completely over L .

The right inequality is an equality iff. L is a separable extension of K , which means that the minpoly over K of any element of L is separable.

Question 3 *Correspondence in degree 3*

Let K be a field, and $F(x) \in K[x]$ be separable and of degree 3. Denote its 3 roots in its splitting field L by $\alpha_1, \alpha_2, \alpha_3$.

1. What are the possibilities for $\text{Gal}_K(F)$? How can you tell them apart?

2. For each of the cases found in the previous question, sketch the diagram showing all the fields $K \subset E \subset L$ and identifying these fields. In particular, locate $K(\alpha_1)$, $K(\alpha_2)$, $K(\alpha_3)$, $K(\alpha_1, \alpha_2)$, etc.
3. In which of the cases above is the stem field of F isomorphic to its splitting field?
(Warning: there is a catch in this question.)

Solution 3

Some general remarks first. In any case, $\text{Gal}_K(F)$ is a subgroup of S_3 acting on the roots of F ; the only such subgroups are S_3 , A_3 , $\{\text{Id} \times S_2\}$, and $\{\text{Id}\}$. Besides, we know that $\alpha_1 + \alpha_2 + \alpha_3 \in K$ by Vieta's formulas (it is the negative of the coefficient of x^2 in F), so $\alpha_3 = (\alpha_1 + \alpha_2 + \alpha_3) - \alpha_1 - \alpha_2 \in K(\alpha_1, \alpha_2)$; as a result, we always have

$$K(\alpha_1, \alpha_2) = K(\alpha_1, \alpha_2, \alpha_3).$$

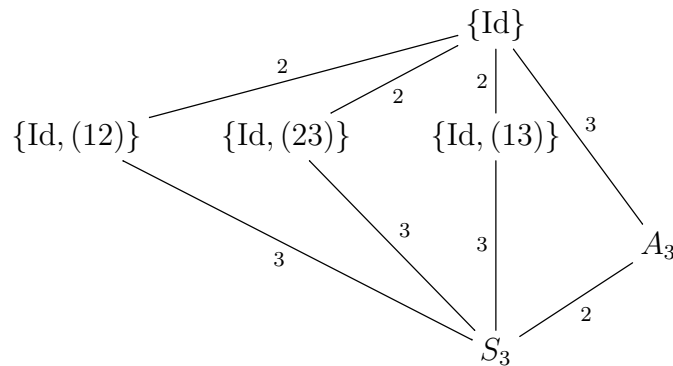
We can also recover this fact by Galois theory: if $\sigma \in \text{Gal}(K(\alpha_1, \alpha_2, \alpha_3)/K(\alpha_1, \alpha_2))$, then $\sigma \in \S_3$ fixes 1 and 2, so it must be the identity. Therefore $K(\alpha_1, \alpha_2, \alpha_3)$ and $K(\alpha_1, \alpha_2)$ both correspond to the same subgroup, namely $\{\text{Id}\}$, so they are the same field.

Similarly, we have

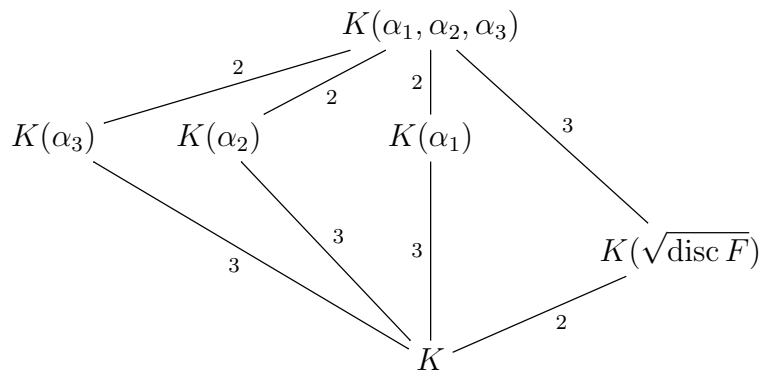
$$K(\alpha_1, \alpha_3) = K(\alpha_2, \alpha_3) = K(\alpha_1, \alpha_2, \alpha_3).$$

Let us now examine the possible cases.

Suppose first that F is irreducible over K , and that $\text{disc } F$ is not a square in K . Then $\text{Gal}_K(F)$ is a transitive subgroup not contained in A_3 , so it is S_3 . To find the intermediate fields, we start with the subgroups:



Since $\{\text{Id}, (23)\}$ is the stabiliser of α_1 , the corresponding field is $K(\alpha_1)$, which is indeed an extension of K of degree 3 since F , being irreducible, is the minpoly of α_1 . Similarly for $K(\alpha_2)$ and $K(\alpha_3)$. Finally, let E correspond to A_3 ; then the extension $E \subset K(\alpha_1, \alpha_2, \alpha_3)$ is Galois of Galois group A_3 , so $\text{disc } F$ is a square in E . Besides $[E : K] = [S_3 : A_3] = 2$ and $\sqrt{\text{disc } F} \notin K$ by assumption, so $E = K(\sqrt{\text{disc } F})$. We thus get



In particular, the stem fields $K(\alpha_1)$, $K(\alpha_2)$, $K(\alpha_3)$, which are all isomorphic (to $K[x]/F(x)$, that's a theorem) but distinct, are smaller than the splitting field $K(\alpha_1, \alpha_2, \alpha_3)$ in this case.

Suppose now that F is irreducible and $\text{disc } F$ is a square in K . Then $\text{Gal}_K(F) = A_3$ since it is transitive and contained in A_3 . Since $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ has prime order, it cannot have any nontrivial subgroup, so by the Galois correspondence the only intermediate fields are

$$\begin{array}{c} K(\alpha_1, \alpha_2, \alpha_3) \\ \downarrow \#A_3=3 \\ K. \end{array}$$

Since F is irreducible over K , it has no root in K , so $\alpha_1 \notin K$, so $K(\alpha_1) \supsetneq K$, so

$$K(\alpha_1) = K(\alpha_1, \alpha_2, \alpha_3).$$

We can also see this by noting that the corresponding subgroup is the stabiliser of 1 in A_3 , which is reduced to $\{\text{Id}\}$. Similarly

$$K(\alpha_2) = K(\alpha_3) = K(\alpha_1, \alpha_2, \alpha_3).$$

So this time, the stem fields $K(\alpha_1)$, $K(\alpha_2)$, $K(\alpha_3)$ are all the same (not only up to isomorphism), and agree with the splitting field $K(\alpha_1, \alpha_2, \alpha_3)$.

Suppose now that F factors as $1 + 2$ over K , and let α_1 be the root of F in K . Then $F(x) = (x - \alpha_1)G(x)$, where $G(x) = (x - \alpha_2)(x - \alpha_3)$ is irreducible over K . In particular $\text{Gal}_K(F) = \text{Id} \times \text{Gal}_K(G) = \text{Id} \times S_2$. Again this does not have any nontrivial subgroups, so the only intermediate fields are

$$\begin{array}{c} K(\alpha_1, \alpha_2, \alpha_3) \\ \left| \begin{array}{c} 2 \end{array} \right. \\ K. \end{array}$$

We have $K(\alpha_1) = K$, but $K(\alpha_2) = K(\alpha_3) = K(\alpha_1, \alpha_2, \alpha_3)$.

Finally, if F factors completely over K , then all the α_i are in K , so the only intermediate field is

$$K = K(\alpha_1, \alpha_2, \alpha_3)$$

which is of course also $K(\alpha_i)$ for any i . This checks out with Galois theory, since in this case $\text{Gal}_K(F) = \{\text{Id}\}$ has only one subgroup (including itself and $\{\text{Id}\}$, which is the same thing in this case).

In the last two cases, there is no stem field anymore since F is not irreducible (that was the catch).

Question 4 *The fundamental theorem of algebra*

The goal of this Question is to use Galois theory to prove by contradiction that \mathbb{C} is algebraically closed.

You may use without proof the following facts:

- If $F(x) \in \mathbb{R}[x]$ is a polynomial of odd degree, then $F(x)$ has at least one root in \mathbb{R} .
- If $G(x) \in \mathbb{C}[x]$ is a polynomial of degree 2, then $G(x)$ has at least one root in \mathbb{C} .
- If G is a finite group of cardinal $\#G = 2^a b$ with b odd, then G has at least one subgroup of cardinal 2^a .
- If H is a finite group whose cardinal $\#H = 2^a$ is a power of 2, then for each integer $0 \leq n \leq a$, H has at least one subgroup of cardinal 2^n .

1. Prove that if \mathbb{C} were not algebraically closed, then there would exist a finite nontrivial extension K of \mathbb{C} (that is to say $K \supsetneq \mathbb{C}$ and $1 < [K : \mathbb{C}] < \infty$).
2. Deduce that there would exist a finite nontrivial extension $\mathbb{C} \subsetneq L$ such that the extension $\mathbb{R} \subsetneq L$ is Galois.
3. Prove that $[L : \mathbb{R}]$ would necessarily be a power of 2.
4. Prove that there would exist an intermediate field $\mathbb{C} \subsetneq F \subseteq L$ such that $[F : \mathbb{C}] = 2$.
5. Derive a contradiction.

Note: the admitted facts at the top of the Question follow respectively from elementary calculus (limits at $\pm\infty$ and then intermediate value theorem), the formula to solve quadratic equations and the fact that every element of \mathbb{C} admits a square root in \mathbb{C} , Sylow's theorem, and Sylow's theorem again.

Solution 4

1. If \mathbb{C} is not algebraically closed, then there exists an irreducible polynomial $P(x) \in \mathbb{C}[x]$ of degree $d \geq 2$. We may then take K to be the stem field $\mathbb{C}[x]/(P)$, which satisfies $[K : \mathbb{C}] = d$.

2. The tower law ensures that $[K : \mathbb{R}] = [K : \mathbb{C}][\mathbb{C} : \mathbb{R}] = 2d$, so K is a finite extension of \mathbb{R} . Its normal closure L (over \mathbb{R}) is thus also a finite extension of \mathbb{R} , which is a nontrivial extension of \mathbb{C} since it contains $K \supsetneq \mathbb{C}$.
3. Let $G = \text{Gal}(L/\mathbb{R})$. This is a finite group of order $[L : \mathbb{R}]$, which we may factor as $2^a b$ with b odd. By the admitted facts above, there exists a subgroup $H \subset G$ of order 2^a and thus of index b . The Galois correspondence attaches to it an intermediate extension $E = L^H$ such that $[E : \mathbb{R}] = b$.

We claim that $E = \mathbb{R}$. Indeed, let $e \in E$. Then e is algebraic over \mathbb{R} since $[E : \mathbb{R}] = b < \infty$, and the degree of its minimal polynomial over \mathbb{R} is $[\mathbb{R}(e) : \mathbb{R}]$, which divides $[E : \mathbb{R}] = b$ by the tower law, and is therefore odd. This polynomial must thus have a root in \mathbb{R} , which contradicts its irreducibility unless it has degree 1; but this means that $e \in \mathbb{R}$.

In conclusion, $b = [E : \mathbb{R}] = 1$, so $\#\text{Gal}(L/\mathbb{R}) = 2^a b = 2^a$.

4. We are in the following situation: $\mathbb{R} \subsetneq \mathbb{C} \subsetneq L$, with L Galois of degree 2^a over \mathbb{R} . In particular, L is also Galois over \mathbb{C} , of degree 2^{a-1} by the tower law (in particular $a \geq 2$); therefore $\text{Gal}(L/\mathbb{C})$ makes sense and is a group of cardinal 2^{a-1} . By the above, it admits a subgroup of order 2^{a-2} , and thus of index 2. The corresponding field F satisfies $\mathbb{R} \subsetneq \mathbb{C} \subsetneq F \subsetneq L$ and $[F : \mathbb{C}] = 2$.
5. Let $f \in F$. As $[F : \mathbb{C}] = 2 < \infty$, f is algebraic over \mathbb{C} , of degree 1 or 2. If that degree were 2, then its minimal polynomial over \mathbb{C} would be an irreducible polynomial of degree 2 over \mathbb{C} , and we have agreed that such a thing does not exist. Therefore this degree is 1, so $f \in \mathbb{C}$.

This proves that $F = \mathbb{C}$, in contradiction with $[F : \mathbb{C}] = 2$.

Question 5 *Galois group computations*

Determine the Galois group over \mathbb{Q} of the polynomials below, and say if they are solvable by radicals over \mathbb{Q} .

1. $x^3 - x^2 - x - 2$,
2. $x^3 - 3x - 1$,
3. $x^3 - 7$,
4. $x^5 + 21x^2 + 35x + 420$,
5. $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Solution 5

1. Looking for rational roots, we find the factorisation $f = (x - 2)(x^2 + x + 1)$. The second factor has $\Delta = -3 < 0$ so is irreducible over \mathbb{R} and hence over \mathbb{Q} . As a result, the polynomial is separable and has Galois group $\{\text{Id}\} \times S_2$. This is Abelian, hence solvable, so this polynomial is solvable by radicals.
2. No rational roots, so irreducible (since degree 3). $\text{disc} = 81 = 9^2$ so A_3 . This group is Abelian, hence solvable, so this polynomial is solvable by radicals.
3. No rational roots, so irreducible (since degree 3). $\text{disc} = -3^3 \cdot 7^2$ is clearly not a square in \mathbb{Q} , so S_3 . This group is solvable because $\text{Id} \triangleleft A_3 \triangleleft S_3$ has Abelian factors, so this polynomial is solvable by radicals.

Note: since S_3 is solvable, any subgroup is also solvable, so any equation of degree 3 is solvable by radicals.

4. Eisenstein at 7 so irreducible, so transitive Galois group. Mod 2, factors as

$$x^5 + x^2 + x = x(x^4 + x + 1).$$

The second factor is irreducible: if not, it would have a factor of degree 1 or 2, but

$$\gcd(x^4 + x + 1, x^{2^2} - 1) = \gcd(x^4 + x + 1, x^4 - 1 - (x^4 + x + 1)) = \gcd(x^4 + x + 1, x) = 1$$

so it has no irreducible factor of degree dividing 2. So we have a 4-cycle.

Mod 3, factors as

$$x^5 - x = (x - 1)x(x + 1)(x^2 + 1)$$

with $x^2 + 1$ irreducible mod 3 (degree ≤ 3 , no roots), so we have a 2-cycle. Conclusion : S_5 . We know that this is not a solvable group, so this polynomial is not solvable by radicals.

5. This is the cyclotomic polynomial $\Phi_{11}(x)$, so Galois group $(\mathbb{Z}/11\mathbb{Z})^\times$. This is Abelian, hence solvable, so this polynomial is solvable by radicals even though it has degree ≥ 5 (indeed, the roots are $\sqrt[11]{1}\dots$)

Question 6 *A cosine formula*

Let $c = \cos(2\pi/17)$.

1. Prove that the group $(\mathbb{Z}/17\mathbb{Z})^\times$ is cyclic, and find a generator for it.
2. Prove that c is algebraic over \mathbb{Q} .
3. Determine the conjugates of c over \mathbb{Q} , and its degree as an algebraic number over \mathbb{Q} .
4. Explain how one could in principle use Galois theory (and a calculator / computer) to find an explicit formula for c .

Solution 6

1. This group is cyclic (of order 16 of course) because 17 is prime. Let us look for a generator. 2 does not work because $2^4 = 16 \equiv -1 \pmod{17}$, so $2^8 = 1$, so 2 has order $8 < 16$. However 3 is a generator since

$$3^2 = 9, 3^4 = 9^2 = 81 \equiv -4, 3^8 \equiv (-4)^2 \equiv -1.$$

2. Let $\zeta = \exp(2\pi i/17)$, a primitive 17-th root of 1. Since ζ is clearly algebraic over \mathbb{Q} (as a root of $x^{17} - 1$ / even better: of $\Phi_{17}(x)$), $\mathbb{Q}(\zeta)$ is a finite extension of \mathbb{Q} . As a

result, it is an algebraic extension of \mathbb{Q} , which means that all its elements are algebraic over \mathbb{Q} . This applies in particular to $c = \frac{\zeta + \zeta^{-1}}{2}$.

3. Let ζ as above, and $L = \mathbb{Q}(\zeta)$. We know that L is Galois over \mathbb{Q} ; since $c \in L$, this implies that the conjugates of c are the $\sigma(c)$ for $\sigma \in \text{Gal}(L/\mathbb{Q})$. It remains to determine them explicitly.

We know that $\text{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/17\mathbb{Z})^\times$. By the first question, $\text{Gal}(L/\mathbb{Q})$ is cyclic of order 16, and generated by $\sigma_3 : \zeta \mapsto \zeta^3$.

In particular, the conjugates of c are its orbit under σ_3 . Using $c = \frac{\zeta + \zeta^{-1}}{2}$ (and some patience), we compute that

$$\begin{aligned}\sigma_3(c) &= \frac{\zeta^3 + \zeta^{-3}}{2} = \cos(6\pi/17), \\ \sigma_3^2(c) &= \frac{\zeta^9 + \zeta^{-9}}{2} = \cos(18\pi/17) = \frac{\zeta^{-8} + \zeta^8}{2} = \cos(19\pi/17), \\ \sigma_3^3(c) &= \frac{\zeta^{27} + \zeta^{-27}}{2} = \frac{\zeta^{-7} + \zeta^7}{2} = \cos(14\pi/17), \\ \sigma_3^4(c) &= \frac{\zeta^{-21} + \zeta^{21}}{2} = \frac{\zeta^{-4} + \zeta^4}{2} = \cos(8\pi/17), \\ \sigma_3^5(c) &= \frac{\zeta^{-12} + \zeta^{12}}{2} = \frac{\zeta^5 + \zeta^{-5}}{2} = \cos(10\pi/17), \\ \sigma_3^6(c) &= \frac{\zeta^{15} + \zeta^{-15}}{2} = \frac{\zeta^{-2} + \zeta^2}{2} = \cos(4\pi/17), \\ \sigma_3^7(c) &= \frac{\zeta^{-6} + \zeta^6}{2} = \cos(12\pi/17), \\ \sigma_3^8(c) &= \frac{\zeta^{-18} + \zeta^{18}}{2} = \frac{\zeta + \zeta^{-1}}{2} = \cos(2\pi/17) = c,\end{aligned}$$

so we stop here (note that since $3^8 \equiv -1$, we already knew that σ_3^8 would fix c , so the orbit would have length ≤ 8): the conjugates of c are

$$c = \cos(2\pi/17), \cos(6\pi/17), \cos(18\pi/17), \cos(14\pi/17),$$

$$\cos(8\pi/17), \cos(10\pi/17), \cos(4\pi/17), \cos(12\pi/17).$$

Using a calculator, one checks that they are all distinct. Since they are the roots of the minimal polynomial of c , we see that the degree of c as an algebraic number is 8.

4. Since $\text{Gal}(L/\mathbb{Q})$ is cyclic of order 16, it has precisely one subgroup of each of the following orders: 1, 2, 4, 8, 16 (and these are all its subgroups). The Galois correspondence shows that there is a succession of extensions of degree 2 starting at \mathbb{Q} and culminating at L . These are all the subfields of L (since these were all the subgroups). The field $\mathbb{Q}(c)$ must be one of them; since this field has degree 8 over \mathbb{Q} by the above, it is actually the second-to-top one (the top one being L).

Starting with \mathbb{Q} , we can now find an explicit generator for each subfield by expressing a generator in terms of ζ , finding its other conjugate over the subfield just below it by using the Galois action (there will be only one other conjugate since each extension step is of degree 2), deducing its minimal polynomial over that subfield, and solving it (which we can since it will have degree 2).

For instance, for the first step, we see that $\alpha = \sum_{k=0}^7 \sigma_3^{2k}(\zeta)$ lies in the extension of degree 2 over \mathbb{Q} since it is fixed by σ_3^2 (which generates the corresponding subgroup of order 8), and has $\alpha' = \sigma_3(\alpha) = \sum_{k=0}^7 \sigma_3^{2k+1}(\zeta)$ as a conjugate. Since one checks with a calculator that $\alpha' \neq \alpha$, we have that α generates the extension of degree 2 (and so does α'), and satisfies its minimal polynomial $A(x) = (x - \alpha)(x - \alpha') \in \mathbb{Q}[x]$. Expressing it in terms of ζ (which is really painful without a computer) yields $A(x) = x^2 + x - 4$, which shows that $\alpha, \alpha' = \frac{-1 \pm \sqrt{17}}{2}$, so this extension is actually $\mathbb{Q}(\sqrt{17})$.

Next, we find similarly that $\beta = \sum_{k=0}^3 \sigma_3^{4k}(\zeta)$ lies in the extension of degree 4, and generates it since it is distinct from its conjugate $\beta' = \sigma_3(\beta)$ over $\mathbb{Q}(\alpha)$; and since it is a root of $B(x) = (x - \beta)(x - \beta')$ which must lie in $\mathbb{Q}(\alpha)[x]$, we can express it in terms of α .

With a lot of courage (or in my case, a good computer program), we find that $B(x) = x^2 - \alpha + 1$ whence $\beta, \beta' = \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2}$. Continuing this way, we finally arrive to the fantastically horrible formula

$$\cos \frac{2\pi}{17} = \frac{-1 + \sqrt{17} + \sqrt{2}\sqrt{17 - \sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{170 + 38\sqrt{17}}}}{16}.$$

Question 7 *Extensions of finite field are Galois*

Let $p \in \mathbb{N}$ be prime, $n \in \mathbb{N}$, and $q = p^n$.

1. Give two proofs of the fact that the extension $\mathbb{F}_p \subset \mathbb{F}_q$ is Galois: one by viewing \mathbb{F}_q as a splitting field, and the other by considering the order of $\text{Frob} \in \text{Aut}(\mathbb{F}_q)$.
2. What does the Galois correspondence tell us for $\mathbb{F}_p \subset \mathbb{F}_q$?
3. Generalise to an arbitrary extension of finite fields $\mathbb{F}_q \subset \mathbb{F}_{q'}$.

Solution 7

1. Recall that

$$\mathbb{F}_q = \{x \in \overline{\mathbb{F}_p} \mid x^q = x\}.$$

In particular, \mathbb{F}_q is the splitting field over \mathbb{F}_p of $F(x) = x^q - x$, so it is normal over \mathbb{F}_p ; besides, $F' = -1$ has no common factor with F , so F is separable, so \mathbb{F}_q is separable over \mathbb{F}_p (we may also argue that \mathbb{F}_p , being finite, is perfect).

Second proof: $\text{Frob} : x \mapsto x^p \in \text{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$. Its iterates are $\text{Frob}^k : x \mapsto x^{p^k}$, so if Frob has order o , then every element of \mathbb{F}_q is a root of $x^{p^o} - x$, whence $p^o \geq q$ by considering the degree, i.e. $o \geq n$. SO Frob has at least n distinct iterates in $\text{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$, so the inequality

$$\# \text{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) \leq [\mathbb{F}_q : \mathbb{F}_p] = n$$

is an equality, so the extension is Galois (cf. question 1). Besides, this proof also show that the Galois group is cyclic and generated by Frob .

2. The subgroups of

$$\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \text{Frob} \rangle \simeq \mathbb{Z}/n\mathbb{Z}$$

are the

$$\langle \text{Frob}^d \rangle \simeq d\mathbb{Z}/n\mathbb{Z}$$

for $d \mid n$ since the former is cyclic by the above. For each d , the corresponding subfield is

$$\mathbb{F}_q^{\langle \text{Frob}^d \rangle} = \{x \in \mathbb{F}_q \mid x^{p^d} = x\} = \mathbb{F}_{p^d}$$

as predicted by the classification of finite fields.

3. By the same arguments as the above, this extension is Galois, with cyclic Galois group generated by $\text{Frob}_q : x \mapsto x^q$ (since it must induce the identity on \mathbb{F}_q). The Galois correspondence then shows that the intermediate fields are the \mathbb{F}_{q^d} for $d \mid m$, where $q' = q^m$, as predicted by the classification of finite fields.