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 **Michaelmas 2023–24**

MAU34101 Galois theory — Revision paper (NOT REAL EXAM)

Never Nowhere Ever

Dr. Nicolas Mascot

Instructions to candidates:

This is a mock exam paper for revision purposes only.
Question 1 is for warmup. Questions 2–8 are more or less representative of what to expect at the exam. Questions 5 and 9–11 are more difficult and are included here for practice.

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

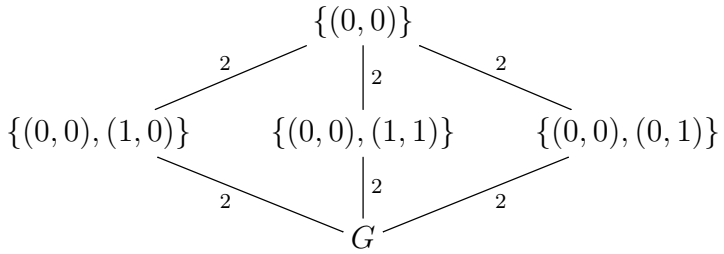
Question 1 *Subgroups for appetiser*

Sketch a diagram showing all the subgroups of G when:

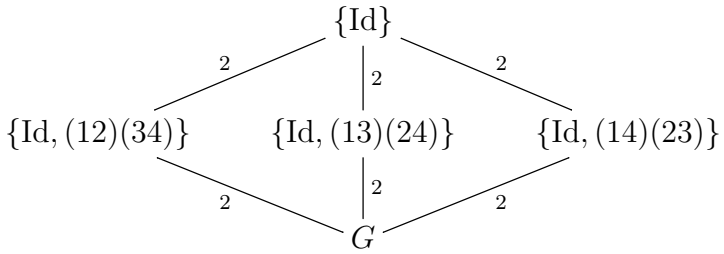
1. $G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$,
2. $G = V_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} < S_4$,
3. $G = S_3$,
4. $G = \mathbb{Z}/n\mathbb{Z}$, for n up to 12.

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:

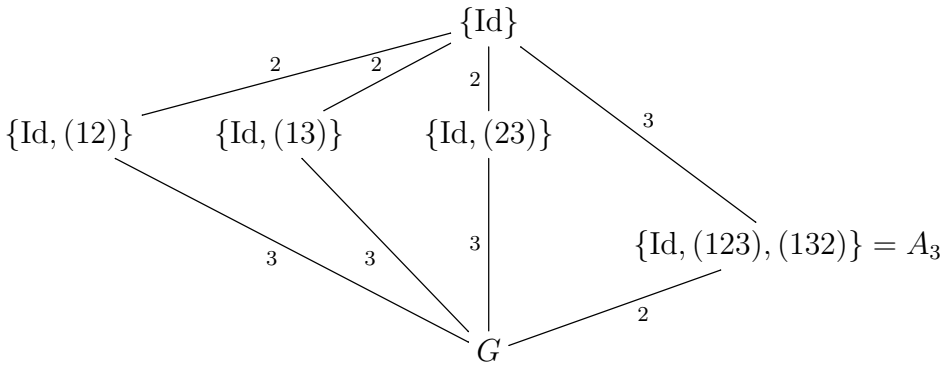


2. Same logic as for $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ (and in fact these two groups are isomorphic).



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 $\mathrm{Id} \neq g \in H$, then by Lagrange g must have order 3

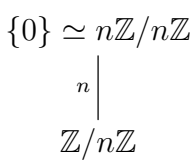
so $H = \{Id, g, g^2 = g^{-1}\}$; and conversely any element of order 3 (i.e. 3-cycle) gives us a subgroup of order 3. So



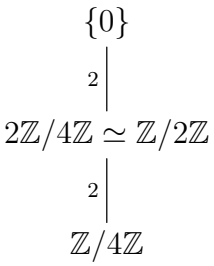
4. Subgroups of cyclic groups are also cyclic. Besides, for each $d \mid n$ we have the subgroup $d\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{d}\mathbb{Z}$, and that's all the subgroups.

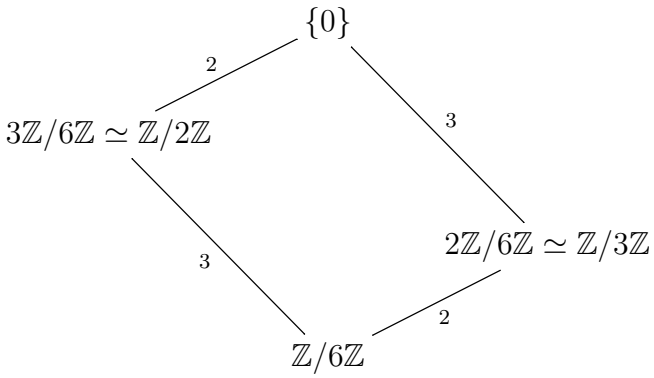
   For $n = 1$, G is the trivial group.

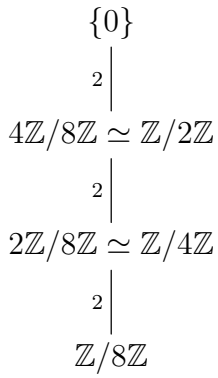
   For $n = 2, 3, 5, 7, 11$, n is prime, so no nontrivial subgroup:

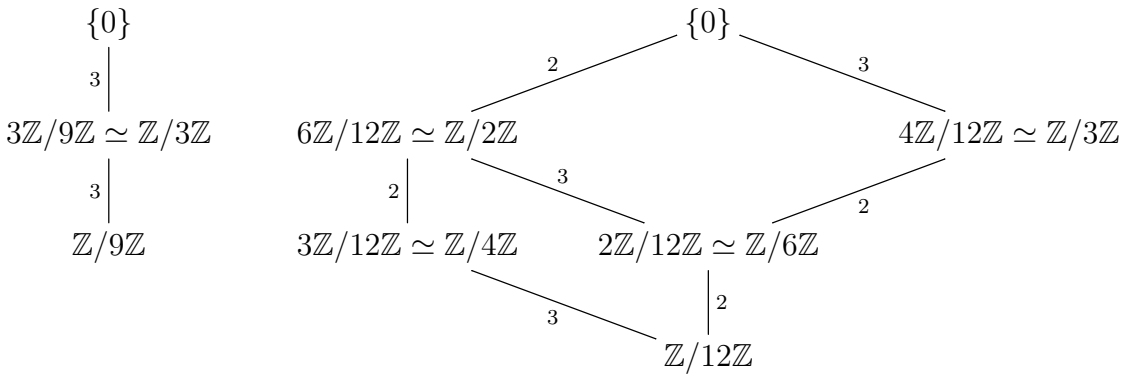


   The remaining cases are a little more interesting:









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 $[L : K]$, $\#\operatorname{Aut}_K(L)$, $\#\operatorname{Hom}_K(L, \Omega)$? When are they equalities? State equivalent conditions.

Solution 2

We always have

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

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 *Yoga with the Galois correspondence*

Let L/K be a finite Galois extension with Galois group $G = \operatorname{Gal}(L/K)$. Let $K \subseteq E_1, E_2 \subseteq L$ be intermediate extensions, and let $H_1, H_2 \leqslant G$ be the corresponding subgroups.

We denote by E_1E_2 the subfield of L generated by E_1 and E_2, and by H_1H_2 the subgroup of G spanned by H_1 and H_2.

Find the intermediate extensions corresponding to H_1H_2 and to $H_1 \cap H_2$, and the subgroups corresponding to E_1E_2 and to $E_1 \cap E_2$.

Solution 3

Let E correspond to $H_1 \cap H_2$, and let H correspond to E_1E_2. The Galois correspondence being inclusion-reversing, we know that E will be bigger than E_1 and E_2, and that H will be bigger than H_1H_2. We are actually going to prove that $E = E_1E_2$ and that $H = H_1H_2$.

First, a "down-to-earth" proof. We will be relying a lot on the Galois correspondence being inclusion-reversing.

Since $E_1E_2 \supseteq E_1$, we have $\mathrm{Gal}(L/E_1E_2) \leqslant \mathrm{Gal}(L/E_1) = H_1$; similarly, $\mathrm{Gal}(L/E_1E_2) \leqslant H_2$, whence $\mathrm{Gal}(L/E_1E_2) \leqslant H_1 \cap H_2$. The reverse inclusion $\mathrm{Gal}(L/E_1E_2) \geqslant H_1 \cap H_2$ is proved by noticing that any element of $H_1 \cap H_2$ acts trivially on E_1 and on E_2, and therefore of E_1E_2.

Similarly, $H_1H_2 \geqslant H_1$ so $L^{H_1H_2} \subset L^{H_1} = E_1$, and $L^{H_1H_2} \subseteq E_2$ by the same logic, so $L^{H_1H_2} \subseteq E_1 \cap E_2$. The reverse inclusion $L^{H_1H_2} \supseteq E_1 \cap E_2$ is trickier to prove directly; however, it is equivalent by the Galois correspondence to the statement that $H_1H_2 \leqslant \mathrm{Gal}(L/E_1 \cap E_2)$, which we are now going to prove: $E_1 \supseteq E_1 \cap E_2$ so $H_1 = \mathrm{Gal}(L/E_1) \leqslant \mathrm{Gal}(L/E_1 \cap E_2)$, and by the same logic $H_2 \leqslant \mathrm{Gal}(L/E_1 \cap E_2)$. Therefore $H_1 \cup H_2 \subseteq \mathrm{Gal}(L/E_1 \cap E_2)$, so $H_1H_2 \leqslant \mathrm{Gal}(L/E_1 \cap E_2)$ since the RHS is a subgroup whereas the LHS is the smallest subgroup containing $H_1 \cup H_2$. This completes this proof.

However, a much more conceptual proof is possible: $H_1 \cap H_2$ (respectively H_1H_2) is the largest subgroup contained both in H_1 and H_2 (respectively, containing both H_1 and H_2), i.e. they are the places where H_1 and H_2 merge (above and below) in the diagram of subgroups of $\mathrm{Gal}(L/K)$. Similarly, E_1E_2 and $E_1 \cap E_2$ are the places where E_1 and E_2 merge in the diagram of intermediate extensions. But the Galois correspondence says that these two diagrams are the same, whence the result.

Question 4 *Galois group computations*

Determine the Galois group over $\mathbb{Q}$ of the polynomials below, and say if they are solvable by radicals over $\mathbb{Q}$: $x^3 - x^2 - x - 2$, $x^3 - 3x - 1$, $x^3 - 7$, $x^5 + 21x^2 + 35x + 420$, $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Solution 4

Note: By Exercise 6, we have a general method for degree 3, based on whether the polynomial has a rational root, and whether its discriminant is a square in $\mathbb{Q}$. This allows us to deal with the first 3 polynomials.

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 $\{\mathrm{Id}\} \times S_2$. This is Abelian, hence solvable, so this polynomial is solvable by radicals.

2. No rational roots, so irreducible (since degree 3). $\mathrm{disc} = 81 = 9^2$ 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). $\mathrm{disc} = -3^3 \cdot 7^2$ is clearly not a square in $\mathbb{Q}$, so S_3. This group is solvable because $\mathrm{Id} \triangleleft A_3 \triangleleft S_3$ 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 $\sqrt[11]{1}$...)

Question 5 *From the 2019 exam*

Let K be a field, let $F(x) \in K[x]$ be separable and irreducible over K, and let α be a root of $F(x)$ (in some extension of K). Suppose that $\mathrm{Gal}_K(F)$ is Abelian. Prove that $K(\alpha)$ is a splitting field of $F(x)$ over K.

Show that all the hypotheses are necessary (give counter-examples).

Solution 5

First proof: Let L be the splitting field of F over K, so that $\mathrm{Gal}(L/K) = \mathrm{Gal}_K(F)$ is Abelian, and let $H = \mathrm{Gal}(L/K(\alpha))$ be the subgroup corresponding to the subextension $K(\alpha)$. We want to prove that $K(\alpha)$ contains all the roots of F. But since $\mathrm{Gal}(L/K)$ is Abelian, all its subgroups are automatically normal, so $H \triangleleft G$, so $K(\alpha)/K$ is Galois and therefore normal. As $F(x) \in K[x]$ is irreducible over K and has a root in the normal extension $K(\alpha)$, it actually has all its roots in $K(\alpha)$ by one of the characterisations of normal extensions.

Second proof: Let $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_d$ be the roots of F in L, where $d = \deg F$ since F is separable. Then $G = \mathrm{Gal}_K(F)$ should be thought of as a subgroup of S_d permuting these roots. Let α_j be any of the roots of F; then the subgroup H_j of G corresponding to the subextension $K(\alpha_j)$ of L is the stabiliser of α_j. As F is irreducible, G is transitive, so we can find a $\sigma \in G$ such that $\alpha_j = \sigma(\alpha_1)$; but then the stabiliser H_j is the conjugate $\sigma H_1 \sigma^{-1}$ of H_1, and therefore agrees with H_1 as conjugation does nothing in the Abelian group G.

As $H_j = H_1$, the Galois correspondence shows that $K(\alpha_j) = K(\alpha_1)$; it follows that $K(\alpha_1)$ contains all the roots of F.

Variant of the second proof (more focused on the Galois correspondence): α_1 and α_j are conjugate over K as they have the same minimal polynomial over K (namely $F(x)$), so $K(\alpha_1)$ and $K(\alpha_j)$ are conjugate, so the corresponding subgroups of G are conjugate in G. But conjugacy in G does nothing since G is Abelian, so these subgroups are the same, so $K(\alpha_1) = K(\alpha_j)$.

As for counterexamples: G being Abelian is of course crucial, as shown by the counterexample $K = \mathbb{Q}$, $F(x) = x^3 - 2$. But $F(x)$ being irreducible is also important, as shown by the counterexample $K = \mathbb{Q}$, $F(x) = (x^2 - 2)(x^2 - 3)$.

Question 6 *Correspondence in degree 3*

Note: This exercise has a lot of overlap with the next one.

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 $\mathrm{Gal}_K(F)$? 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 6

Some general remarks first. In any case, $\mathrm{Gal}_K(F)$ is a subgroup of S_3 acting on the roots of F; the only such subgroups are S_3, A_3, $\{\mathrm{Id} \times S_2\}$, and $\{\mathrm{Id}\}$. 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

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

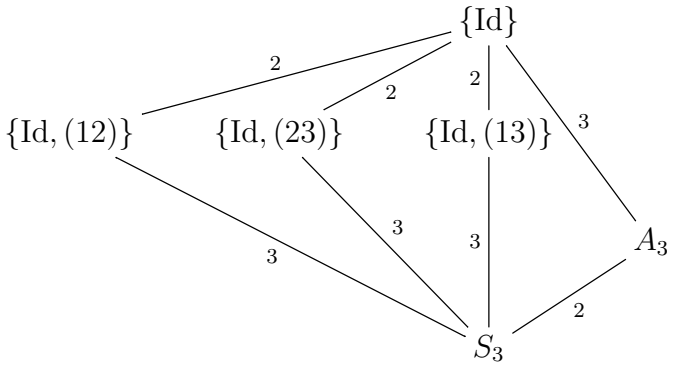
We can also recover this fact by Galois theory: if $\sigma \in \mathrm{Gal}(K(\alpha_1, \alpha_2, \alpha_3)/K(\alpha_1, \alpha_2))$, then $\sigma \in \S_3$ fixes 1 and 2, so it must be the identity. Therefore $K(\alpha_1, \alpha_2, \alpha_3)$ and $K(\alpha_1, \alpha_2)$ both correspond to the same subgroup,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

Similarly, we have

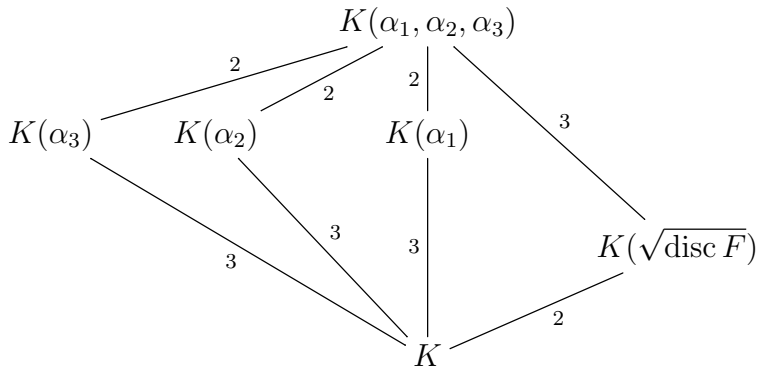
$$K(\alpha_1, \alpha_3) = K(\alpha_2, \alpha_3) = K(\alpha_1, \alpha_2, \alpha_3).$$

Let us now examine the possible cases.

Suppose first that F is irreducible over K, and that $\mathrm{disc}\, F$ is not a square in K. Then $\mathrm{Gal}_K(F)$ 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 $\{\mathrm{Id}, (23)\}$ 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 $\mathrm{disc}\, F$ is a square in E. Besides $[E : K] = [S_3 : A_3] = 2$ and $\sqrt{\mathrm{disc}\, F} \notin K$ by assumption, so $E = K(\sqrt{\mathrm{disc}\, F})$. 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 $\operatorname{disc} F$ is a square in K. Then $\mathrm{Gal}_K(F) = A_3$ 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

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

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 $\{\mathrm{Id}\}$. 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 $\mathrm{Gal}_K(F) = \mathrm{Id} \times \mathrm{Gal}_K(G) = \mathrm{Id} \times S_2$. Again this does not have any nontrivial subgroups, so the only intermediate fields are

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

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 $\mathrm{Gal}_K(F) = \{\mathrm{Id}\}$ has only one subgroup (including itself and$\{\mathrm{Id}\}$, 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 7 *Cube roots (From the 2021 exam)*

Note: This exercise has a lot of overlap with the previous one.

Let K be a subfield of $\mathbb{C}$. Let $0 \neq a \in K$, and let $\alpha \in \mathbb{C}$ be such that $\alpha^3 = a$. Let

$$f(x) = x^3 - a \in K[x],$$

and let $S \subset \mathbb{C}$ be the splitting field of $f(x)$ over K.
Finally, let $\zeta = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$.

Note that a may or may not be a cube in K, and that ζ may or may not lie in K.

1. (a) Prove that if a is not a cube in K, then $f(x)$ is irreducible over K.

   (b) Prove that $[K(\zeta) : K] \leqslant 2$.

   (c) Express the complex roots of $f(x)$ in terms of α and ζ.

   In what follows, we denote these roots by $\alpha_0 = \alpha$, α_1, and α_2.

   (d) Prove that $S \ni \zeta$.

   (e) Prove that S is a Galois extension of K.

   In what follows, we write G for $\mathrm{Gal}(S/K)$, and we view G as a subgroup of S_3 acting on $\alpha_0, \alpha_1, \alpha_2$.

2. In each of the following situations:

   (a) a is not a cube in K and $\zeta \notin K$,

   (b) a is not a cube in K but $\zeta \in K$,

   (c) a is a cube in K but $\zeta \notin K$,

   (d) a is a cube in K and $\zeta \in K$,

   determine $[S : K]$, explain how G acts on $\alpha_0, \alpha_1, \alpha_2$, explain how G acts on ζ, draw a diagram showing all the intermediate fields $K \subseteq E \subseteq S$, and say which of these E are Galois over K. Justify your answers.

Solution 7

1. (a) Since $f(x)$ has degree 3, if it were reducible, then it would have a root in K.

   (b) ζ is a root of the polynomial $\Phi_3(x) = x^2+x+1 \in K[x]$, and is therefore algebraic of degree at most 2 over K.

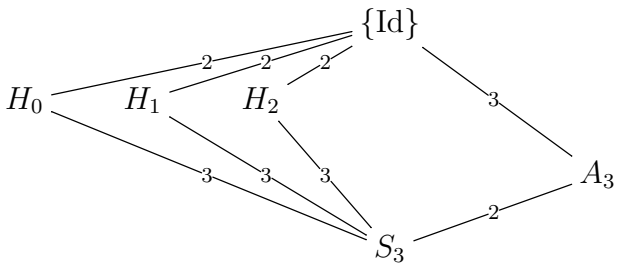
   (c) Since $\zeta^3 = 1$, clearly $\alpha_j = \zeta^j\alpha$ is a root of $f(x)$ for $j = 0, 1, 2$. These roots are pairwise distinct, e.g. since $\alpha_2 = \alpha_1$ would force $0 = \zeta(\zeta-1)\alpha$, whence $\alpha = 0$ as $\zeta, \zeta - 1 \neq 0$, in contradiction with our assumption that $a \neq 0$.

   (d) By definition, $S = K(\alpha_0, \alpha_1, \alpha_2)$. Therefore, $\zeta = \alpha_1/\alpha_0 \in S$.

   (e) Since S/K is a splitting field, it is normal. Besides, it is separable since K, being a subfield of $\mathbb{C}$, has characteristic 0 and is therefore perfect.

2. (a) $f(x)$ is irreducible over K by question 1a, so $[K(\alpha) : K] = 3$, so $3 \mid [S : K(\alpha)][K(\alpha) : K] = [S : K] = \#G$. Besides, question 1b forces $[K(\zeta) : K] = 2$, so $2 \mid \#G$ by the same argument. Therefore $\#G \geqslant 6$; but since $G \leqslant S_3$, necessarily G is the whole of S_3, so in particular $[S : K] = 6$.

   The non-trivial subgroups of G are the ones of order 2, formed of Id and of a transposition, and the alternating group A_3. The subgroup lattice is thus

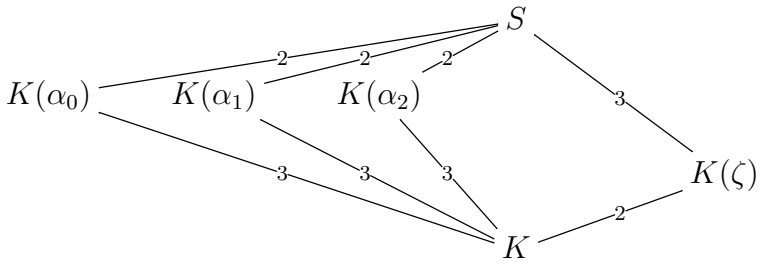


   where for each $j = 0, 1, 2$, H_j is the subgroup spanned by the transposition that fixes j.

   We have $[S^{H_j} : K] = [G : H_j] = 3$, and $\alpha_j \in S^{H_j}$ so $K(\alpha_j) \subseteq S^{H_j}$, whence $S^{H_j} = K(\alpha_j)$ by degrees since $f(x)$ is the minimal polynomial of α_j over K.

   The 3-cycles fix $\zeta = \frac{\alpha_1}{\alpha_0} = \frac{\alpha_2}{\alpha_1} = \frac{\alpha_0}{\alpha_2}$, so $K(\zeta) \subseteq S^{A_3}$, and again that's an equality since $[S^{A_3} : K] = [G : A_3] = 2$.

We deduce the following diagram:



In particular, an element of G fixes ζ iff. it lies in A_3; else, it takes it to its other conjugate, which is ζ^2 since it is the other root of x^2+x+1, whose roots multiply to 1.

The only normal subgroups of G are the trivial group, G, and A_3; therefore the only intermediate extensions which are Galois over K are S, K, and $K(\zeta)$.

(b) By the same logic as in the previous question, $[K(\alpha_0) : K] = 3$. However, since $\zeta \in K$, we then have $\alpha_j \in K(\alpha_0)$ for all j. It follows that $K(\alpha_0) \subseteq S = K(\alpha_0, \alpha_1, \alpha_2) \subseteq K(\alpha_0)$, so $S = K(\alpha_0)$. In particular, G is a subgroup of S_3 of order $[S : K] = 3$, so $G = A_3$. This means that G permutes the α_j cyclically; besides, it fixes ζ since $\zeta \in K$. Finally, since G has no proper subgroups, there is no intermediate field strictly between S and K. Obviously, both S and K are Galois over K.

(c) Let $b \in K$ such that $b^3 = a$. Then b is a root of $f(x)$, so it is one of the α_j; WLOG $\alpha_0 = b \in K$. If we had $\alpha_1 \in K$, then $\zeta = \alpha_1/\alpha_0 \in K$, absurd; similarly, if $\alpha 2 \in K$, then $\zeta = \alpha_0/\alpha_2 \in K$, absurd. So $f(x)$ has exactly one root and one irreducible factor of degree 2, so $G \leqslant S_1 \times S_2$ whence $\#G \leqslant 2$. On the other hand, $\#G = [S : K] > 1$ since $\zeta \in S$. Therefore $[S : K] = \#G = 2$, so $G \simeq \mathbb{Z}/2\mathbb{Z}$ swapping the two roots α_1, α_2 of $f(x)$ which do not lie in K, and swapping ζ and its conjugate ζ^2. Since G has no nontrivial subgroups, there are no nontrivial intermediate fields. Obviously, both S and K are Galois over K.

(d) Again let $b \in K$ such that $b^3 = a$. Then b is one of the α_j, which thus lies in K, so they all lie in K since $\zeta \in K$. Therefore $S = K$, $[S : K] = 1$, and G is the trivial group. Obviously, $S = K$ is Galois over itself.

Note: One may also point out that $\operatorname{disc} f = -27a^2 = -3(3a)^2$, so that $G \leqslant A_3$ iff. -3 is a square in K iff. $\sqrt{-3} \in K$ iff. $\zeta = \frac{-1+\sqrt{-3}}{2}$ lies in K.

Question 8 *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 $0 \leqslant n \leqslant a$, 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 8

1. If $\mathbb{C}$ is not algebraically closed, then there exists an irreducible polynomial $P(x) \in \mathbb{C}[x]$ of degree $d \geqslant 2$. 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 $G = \mathrm{Gal}(L/\mathbb{R})$. 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 $\#\,\mathrm{Gal}(L/\mathbb{R}) = 2^a b = 2^a$.

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 $a \geqslant 2$); therefore $\mathrm{Gal}(L/\mathbb{C})$ 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 9 *A cosine formula*

1. Prove that the group $(\mathbb{Z}/17\mathbb{Z})^\times$ is cyclic, and find a generator for it.
2. Let $c = \cos(2\pi/17)$. 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 9

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 $2^4 = 16 \equiv -1 \bmod 17$, 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 $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. It remains to determine them explicitly.

   We know that $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/17\mathbb{Z})^\times$. By the first question, $\mathrm{Gal}(L/\mathbb{Q})$ 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

$$\sigma_3(c) = \frac{\zeta^3 + \zeta^{-3}}{2} = \cos(6\pi/17),$$

$$\sigma_3^2(c) = \frac{\zeta^9 + \zeta^{-9}}{2} = \cos(18\pi/17) = \frac{\zeta^{-8} + \zeta^8}{2} = \cos(19\pi/17),$$

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

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 $\leqslant 8$): 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 $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic of order 16, it has precisely one subgroup of the each of the following orders: 1, 2, 4, 8, 16 (and these all all its subgroups). The Galois correspondence show that there is a succession of extensions of degree 2 starting at $\mathbb{Q}$ an culminating at L. This 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 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. Sine 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 10 *Another cosine formula*

Let $L = \mathbb{Q}(z)$ where $z = e^{i\pi/10}$ which is a primitive 20-th root of unity, and let $c = z + z^{-1} = 2\cos(\pi/10)$. We admit without proof that $(\mathbb{Z}/20\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, the first factor being generated by $-9 \bmod 20$, and the second factor being generated by $-3 \bmod 20$.

1. What is the minimal polynomial of z over $\mathbb{Q}$?

2. Figure out the diagram of subgroups of $(\mathbb{Z}/20\mathbb{Z})^\times$.

   You may use without proof the fact that any group of order 4 is isomorphic either to $\mathbb{Z}/4\mathbb{Z}$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. You should find 8 subgroups in total.

3. Deduce the diagram of intermediate fields between $\mathbb{Q}$ and L.

   You may want to use a calculator / computer.

4. Find a radical expression for c.

Solution 10

Let $L = \mathbb{Q}(z)$ where $z = e^{i\pi/10}$ which is a primitive 20-th root of unity, and let $c = z + z^{-1} = 2\cos(\pi/10)$. We admit without proof that $(\mathbb{Z}/20\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, the first factor being generated by $-9 \bmod 20$, and the second factor being generated by $-3 \bmod 20$.

1. As z is a primitive 20-th root of unity, its minpoly over $\mathbb{Q}$ is the cyclotomic polynomial $\Phi_{20}(x)$. We know that its degree is $\phi(20) = \#(\mathbb{Z}/20\mathbb{Z})^\times$ which is $4 \times 2 = 8$ from the information we are given.

   In order to actually calculate $\Phi_{20}(x)$, we rely on the formula

   $$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

   (filtration of the n-th roots of unity by their order in the group μ_n). We could use this formula iteratively, but here we can save some work:

   $$\Phi_{20}(x) = \frac{x^{20}-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_5(x)\Phi_{10}(x)} = \frac{x^{20}-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_5(x)\frac{x^{10}-1}{\Phi_1(x)\Phi_2(x)\Phi_5(x)}} = \frac{x^{10}+1}{\Phi_4(x)}$$

   but $\Phi_4(x) = (x+i)(x-i) = x^2+1$, so by the formula for the sum of a geometric progression,

   $$\Phi_{20}(x) = \frac{x^{10}+1}{x^2+1} = x^8 - x^6 + x^4 - x^2 + 1.$$

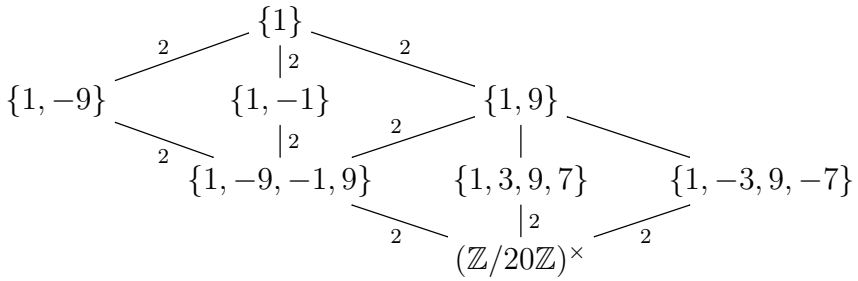
2. *Note: the isomorphism $(\mathbb{Z}/20\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ comes from the Chinese remainder theorem, which informs us that $(\mathbb{Z}/20\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$. As 5 is prime, $(\mathbb{Z}/5\mathbb{Z})^\times$ is cyclic of order $\phi(5) = 5-1 = 4$; the fact that $(\mathbb{Z}/4\mathbb{Z})^\times$ is cyclic is a happy accident. The chosen generators satisfy $-9 \equiv -1$ generates $(\mathbb{Z}/4\mathbb{Z})^\times$ but is trivial in $(\mathbb{Z}/5\mathbb{Z})^\times$, and vice-versa for -3.*

   Subgroups of order 2 correspond bijectively to elements of order 2. In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, these are $(1,0), (1,2), (0,2)$, which correspond in $(\mathbb{Z}/20\mathbb{Z})^\times$ to $(-9)^1(-3)^0 = -9$, $(-9)^1(-3)^2 = -1$, and $(-9)^0(-3)^2 = 9$, where the subgroups $\{1,-9\}$, $\{1,-1\}$, and $\{1,9\}$.

A subgroup of order 4 isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ must consist of 1 and of 3 elements of order 2. By the above, the only choice is $\{1, 9, -1, -9\}$.

Finally, a subgroup $\{1, x, x^2, x^3 = x^{-1}\}$ of order 4 isomorphic to $\mathbb{Z}/4\mathbb{Z}$ must contain an element $x \in (\mathbb{Z}/20\mathbb{Z})^\times$ of order 4, but beware that this is no longer a bijection since the same group is also generated by x^{-1}. As $(\mathbb{Z}/20\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, its elements have order either 1 or 2 or 4, so we can find all the elements of order 4 by taking all the non-identity elements of $(\mathbb{Z}/20\mathbb{Z})^\times$ and discarding the elements of order 2, which we conveniently have already listed. We thus find two subgroups, namely $\{1, 3, 9, 7\}$ and $\{1, -3, 9, -7\}$.

It remains to spot which subgroups of order 2 are contained in which subgroups of order 4. Final answer:



3. We know that $(\mathbb{Z}/20\mathbb{Z})^\times \simeq \mathrm{Gal}(L/\mathbb{Q})$, where $x \in (\mathbb{Z}/20\mathbb{Z})^\times$ corresponds to $\sigma_x : z \mapsto z^x$.

   Thus $L^{\{1,-3,9,-7\}} \ni z + z^{-3} + z^9 + z^{-7}$, which according to a calculator evaluates to $-i$ (a more rigorous but more painful check would involve checking that the relation $z^8 - z^6 + z^4 - z^2 + 1 = 0$ implies that $(z + z^{-3} + z^9 + z^{-7})^2 = -1$). As this field is an extension of $\mathbb{Q}$ of degree 2, it must be $\mathbb{Q}(i)$.

   Similarly, we observe that $(z + z^3 + z^9 + z^7)^2 = -5$, so $L^{\{1,3,9,7\}} = \mathbb{Q}(i\sqrt{5})$.

   Let us move on to $H = \{1, -1, 9, -9\}$. Unfortunately, $z + z^{-1} + z^{-9} + z^9 = 0$ and $zz^{-1}z^{-9}z^9 = 1$, so this does not help us determine $E = L^H$. But E also contains $\alpha = (1 + z)(1 + z^{-1})(1 + z^9)(1 + z^{-9})$ whose value is apparently more complicated and therefore more promising. In order to identify α, we observe that H is a subgroup of

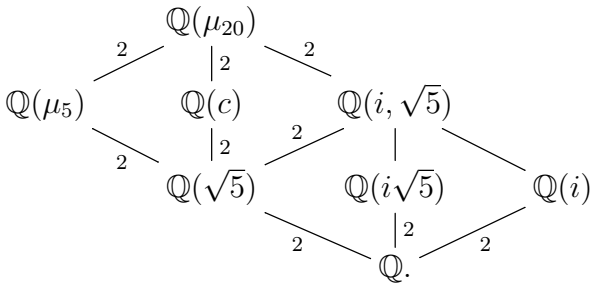
index 2, so that $\mathrm{Gal}(L/\mathbb{Q})/H = \{1, x\} \simeq \mathbb{Z}/2\mathbb{Z}$ for any $x \notin H$, for example $x = 3$. Therefore, $\alpha' = \sigma_3(\alpha) = (1+z^3)(1+z^{-3})(1+z^7)(1+z^{-7})$ is the only other Galois conjugate of α over $\mathbb{Q}$; in particular, the polynomial $(x-\alpha)(x-\alpha') = x^2-(\alpha+\alpha')x+\alpha\alpha'$ has coefficients in $\mathbb{Q}$. Indeed, we find $\alpha+\alpha' = 3$ and $\alpha\alpha' = 1$, whence $\alpha = \frac{3\pm\sqrt{5}}{2}$ and finally $E = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$ by degree.

By Exercise 3 (or by looking at the subfield diagram), we immediately deduce that $L^{\{1,9\}} = \mathbb{Q}(\sqrt{5}, i, i\sqrt{5}) = \mathbb{Q}(i, \sqrt{5})$.

Furthermore, $L^{1,-9} \ni zz^{-9} = z^-8$ which is a root of unity of order $20/\gcd(20,-8) = 5$, so $L^{1,-9} = \mathbb{Q}(\mu_5) = \mathbb{Q}(z^4)$ by degree as $\phi(5) = 4$.

Finally, we observe that $c \in E' = L^{1,-1}$. By hitting c with the elements of $(\mathbb{Z}/20\mathbb{Z})^\times$)or even better, by its quotient by $\{1,-1\}$), we find that the Galois conjugates of c over $\mathbb{Q}$ are $c_1 = c, c_3, c_7, c_9$, where $c_m = z^m + z^{-m} = 2\cos\frac{m\pi}{10}$. That is 4 conjugates (on checks with a calculator that they are really pairwise distinct) so the minpoly of c over $\mathbb{Q}$ has degree 4, so $E' = \mathbb{Q}(c)$ by degree (and this also agrees with $\mathbb{Q}(c_3) = \mathbb{Q}(c_7) = \mathbb{Q}(c_9)$).

Conclusion:



4. On the previous diagram, we spot that $\mathbb{Q}(c)/\mathbb{Q}(\sqrt{5})$ is Galois (all is Abelian, so all subgroups are normal) of degree 2 with Galois group $\{1,-9,-1,9\}/\{1,-1\} = \{\pm1, \pm9\} \simeq \mathbb{Z}/2\mathbb{Z}$, so the only other conjugate of c over $\mathbb{Q}(\sqrt{5})$ is c_9. Therefore $P(x) = (x-c)(x-c_9) = x^2 - ax + b \in Q(\sqrt{5})[x]$, and we can use this to find c if we can determine its coefficients $a = c + c_9$ and $b = cc_9$ explicitly. For this, we use that $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \simeq \mathbb{Z}/frm-e\mathbb{Z}$ is generated by any $x \notin \{1, 9, -1, -9\}$, e.g. $x = 3$. So the only other conjugate of a (resp. b) is $a' = c_3 + c_7$ (resp. $b' = c_3c_7$). Therefore

$(x-a)(x-a') \in \mathbb{Q}[x]$ so we can solve for a, and similarly for b (see how we are climbing down the subfield diagram?). We thus find that $(x-a)(x-a') = x^2$ whence $a = a' = 0$ and $(x-b)(x-b') = x^2 - 5x + 5$ so $b = \frac{5+\sqrt{5}}{2}$, $b' = \frac{5-\sqrt{5}}{2}$ (in this order, as one checks with approximated values), whence finally

$$\cos\frac{\pi}{10} = \frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}.$$

Question 11 *Extensions of finite fields 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 $\mathrm{Frob} \in \mathrm{Aut}(\mathbb{F}_q)$.

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 11

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

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

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

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

are the

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

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

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

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 $\mathrm{Frob}_q : x \mapsto x^q$ (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.