Galois theory — Exercise sheet 3

https://www.maths.tcd.ie/~mascotn/teaching/2019/MAU34101/index.html

Version: November 12, 2019

Answers are due for Tueday November 12th, 3PM.

Exercise 1 *The fifth cyclotomic field (100 pts)*

In this exercise, we consider the primitive 5th root $\zeta = e^{2\pi i/5}$, and we set $L = \mathbb{Q}(\zeta)$. We know that L is Galois over $\mathbb{Q}$, so we define $G = \mathrm{Gal}(L/\mathbb{Q})$. We also let

$$c = \frac{\zeta + \zeta^{-1}}{2} = \cos(2\pi/5) = 0.309\cdots,$$

$$C = \mathbb{Q}(c),$$

and finally

$$c' = \frac{\zeta^2 + \zeta^{-2}}{2} = \cos(4\pi/5) = -0.809\cdots.$$

1. (8 pts) Write down explicitly the minimal polynomial of ζ over $\mathbb{Q}$, and express its complex roots in terms of ζ.
2. (3 pts) Deduce that $\zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$.
3. (12 pts) Prove that G is a cyclic group. What is its order? Find an explicit generator of G.
4. (15 pts) Deduce that $c \notin \mathbb{Q}$.
5. (5 pts) Make the list of all subgroups of G.
6. (12 pts) Draw a diagram showing all the fields E such that $\mathbb{Q} \subset E \subset L$, ordered by inclusion.
7. (20 pts) What are the conjugates of c over $\mathbb{Q}$? Determine explicitly the minimal polynomial of c over $\mathbb{Q}$ (exact computations only, computations with the approximate value of c are forbidden).
8. (5 pts) Deduce that
$$c = \frac{-1+\sqrt{5}}{4}.$$
9. (20 pts) What are the conjugates of ζ over C (as opposed to over $\mathbb{Q}$)? Deduce that
$$\zeta = \frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$

Solution 1

1. The minimal polynomial of ζ over $\mathbb{Q}$ is the 5th cyclotomic polynomial
$$\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1.$$
Its complex roots are the primitive 5-th roots of 1, namely
$$\{\zeta^k \mid k \in (\mathbb{Z}/5\mathbb{Z})^\times\} = \{\zeta, \zeta^2, \zeta^3, \zeta^4\}.$$

2. This follows from the fact that ζ is a root of $\Phi_5(x)$. Alternatively,
$$1+\zeta+\zeta^2+\zeta^3+\zeta^4 = \sum \text{Roots of } x^5-1 = -\text{Coeff. of } x^4 = 0.$$

3. We know that G can be identified to $(\mathbb{Z}/5\mathbb{Z})^\times$, and is thus an Abelian group of order 5. To prove that it is cyclic, we can either notice that $g = 2 \in G$ is a generator since
$$2 \neq 1, \quad 2^2 = 4 \neq 1, \quad 2^3 = 3 \neq 1, \quad 2^4 = 1,$$
or say that since 5 is prime, $\mathbb{Z}/5\mathbb{Z}$ is a finite field, so its multiplicative group is cyclic (but then we still need to find a generator).

4. The element $2 \in G$ acts on L by $\zeta \mapsto \zeta^2$, and thus takes $c = \frac{\zeta+\zeta^{-1}}{2}$ to $\frac{\zeta^2+\zeta^{-2}}{2} = c'$. Since $c' \neq c$ (clear from their numerical values), we have $c \notin L^G$; but $L^G = \mathbb{Q}$ since L is Galois over $\mathbb{Q}$.

5. Since $G \simeq \mathbb{Z}/4\mathbb{Z}$ is cyclic of order 4, its only nontrivial subgroup is $2\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$, and is generated by $g^2 = 4 = -1$. Our list is thus
$$\begin{array}{c} \{1\} \\ | \\ H = \{\pm 1\} \\ | \\ G. \end{array}$$

6. We already know that under the Galois correspondence, $\{1\}$ corresponds to L, and G to $\mathbb{Q}$. It remains to identify L^H.

   We know that $[L^H : \mathbb{Q}] = [G : H] = 2$; besides $-1 \in H$ acts by $\zeta \mapsto \zeta^{-1}$ (i.e. is the complex conjugation) and therefore fixes c, so that $c \in L^H$, whence
$$C = \mathbb{Q}(c) \subseteq L^H.$$
   Since $c \notin \mathbb{Q}$, we have $C \supsetneq \mathbb{Q}$ and so $[C : \mathbb{Q}] \geqslant 2$, so finally
$$L^H = C.$$
   Our diagram is thus
$$\begin{array}{c} L \\ | \\ C \\ | \\ \mathbb{Q}. \end{array}$$

7. The conjugates of c over $\mathbb{Q}$ are the $\sigma(c)$ for $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ (and also for $\sigma \in \mathrm{Gal}(C/\mathbb{Q})$), i.e.

   - c itself for $\sigma = 1$,
   - $\frac{\zeta^2+\zeta^{-2}}{2} = c'$ for $\sigma = 2$,
   - $\frac{\zeta^{-2}+\zeta^2}{2} = c'$ for $\sigma = 3 = -2$,
   - and $\frac{\zeta^{-1}+\zeta}{2} = c$ for $\sigma = 4 = -1$,

   so finally, just c itself and c'. (We can get the same conclusion faster by taking σ in the smaller quotient $\mathrm{Gal}(C/\mathbb{Q}) = G/H = (\mathbb{Z}/5\mathbb{Z})^\times/\pm 1$ of $\mathrm{Gal}(L/\mathbb{Q})$, if we are not afraid to work with this quotient). The minimal polynomial of c over $\mathbb{Q}$ is thus

$$\begin{aligned}\prod_{\beta \text{ conjugate to } c} (x-\beta) &= (x-c)(x-c') \\ &= x^2 - (c+c')x + cc' \\ &= x^2 - \frac{\zeta+\zeta^{-1}+\zeta^2+\zeta^{-2}}{2}x + \frac{(\zeta+\zeta^{-1})(\zeta^2+\zeta^{-2})}{4} \\ &= x^2 - \frac{\zeta+\zeta^4+\zeta^2+\zeta^3}{2}x + \frac{\zeta^3+\zeta^4+\zeta+\zeta^2}{4} \\ &= x^2 + \frac{1}{2}x - \frac{1}{4}.\end{aligned}$$

8. By solving $x^2 + \frac{1}{2}x - \frac{1}{4} = 0$, we find that $\Delta = 5/4$, whence

$$c, c' = \frac{-1 \pm \sqrt{5}}{4}.$$

   Since $c > c'$, we deduce that $c = \frac{-1+\sqrt{5}}{4}$ (and also that $c' = \frac{-1-\sqrt{5}}{4}$).

9. The conjugates of ζ over C are the $\sigma(\zeta)$ for $\sigma \in \mathrm{Gal}(L/C) = H = \{\pm 1\}$, hence $\zeta^{\pm 1}$. Similarly to the previous question, the minimal polynomial of ζ over C is

$$\prod_{\substack{\beta \text{ conjugate} \\ \text{to } \zeta \text{ over } C}} (x-\beta) = (x-\zeta)(x-\zeta^{-1}) = x^2-(\zeta+\zeta^{-1})x+\zeta\zeta^{-1} = x^2-2cx+1 \in C[x],$$

   whose roots are

$$\frac{2c \pm \sqrt{4c^2-4}}{2} = c \pm \sqrt{c^2-1} = \frac{-1+\sqrt{5} \pm i\sqrt{10+2\sqrt{5}}}{4}$$

   using $c = \frac{-1+\sqrt{5}}{4}$. Since ζ (as opposed to ζ^{-1}) is the root with positive imaginary part (draw a regular pentagon; alternatively $\mathrm{Im}\,\zeta = \sin(2\pi/5) > 0$ as $2\pi/5 < \pi$), we conclude that

$$\zeta = \frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$