Course: M3/4/5P11 Galois Theory, Progress Test 1, 12/02/2020

This test is worth 20 marks. You are allowed to use any and all results proven in class, provided that you state them correctly.

Q 1 Consider the polynomial

$$f(X) = X^4 + 3X^2 + 3X + 9 \in \mathbb{Q}[X]$$

(a) Does $f(X)$ have a root $\alpha \in \mathbb{Q}$? **3 mks**

(b) Denote by $\overline{f}(X)$ the class of $f(X)$ in $\mathbb{F}_2[X]$. Factorize $\overline{f}[X] \in \mathbb{F}_2[X]$. **3 mks**

(c) Now combine (a) and (b) to show that $f(X)$ is irreducible in $\mathbb{Q}[X]$. **4 mks**

Q 2 In this question, we denote by $\mathbb{Q} \subset K$ the splitting field of the polynomial $X^5 - 1 \in \mathbb{Q}[X]$.

(a) What is the degree $[K : \mathbb{Q}]$? **2 mks**

(b) Write $\zeta = \exp\left(\frac{2\pi\,\mathtt{i}}{5}\right)$ and let $\alpha = \zeta + \frac{1}{\zeta}$. Find an explicit degree 2 polynomial $g(X) \in \mathbb{Q}[X]$ such that $g(\alpha) = 0$. Solve the quadratic equation and hence find a formula for $\cos\left(\frac{2\pi}{5}\right)$. **4 mks**

(c) What is the Galois group G of the extension $\mathbb{Q} \subset K$? (HINT: G acts as automorphisms of the *group* μ_5 of the 5th roots of 1.) Hence describe all fields F, $\mathbb{Q} \subset F \subset K$. **4 mks**

ANSWERS

A 1 (a) $f(x)$ has no roots in $\mathbb{Q}$; indeed by the Gauss Lemma the possible linear factors of $f(x)$ in $\mathbb{Z}[X]$ are $X \pm 1$, $X \pm 3$, $X \pm 9$[1] and by easy direct inspection none of ± 1, ± 3, ± 9 are roots.

(b) $\overline{f}(X) \equiv X^4 + X^2 + X + 1 \mod 2$ hence $X = 1$ is a root in $\mathbb{F}_2$. Long division in $\mathbb{F}_2[X]$ (or a bit of trial and error) gives:

$$\overline{f}(X) = (X + 1)(X^3 + X^2 + 1)$$

Now the polynomial $X^3 + X^2 + 1$ has no roots in $\mathbb{F}_2$ and it has degree 3; therefore it is irreducible.

(c) I claim that $f(X) \in \mathbb{Q}[X]$ is irreducible. Indeed suppose for a contradiction that f is reducible. Because f has no roots and hence no linear factors, it must split into two quadratic factors, and by the Gauss lemma we may assume that both factors have integer coefficients. To summarise: if $f(X)$ is reducible then there are degree-two polynomials $g_1(X), g_2(X) \in \mathbb{Z}[X]$ such that $f = g_1 g_2$. Reducing modulo 2 we would get

$$\overline{f} = \overline{g}_1 \overline{g}_2 \in \mathbb{F}_2[X]$$

[1] You may have learned in school that if $f(X) = a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ is a polynomial with integer coefficients, then any rational root $\alpha = \frac{p}{q}$ in lowest terms is such that $q|a_0$ and $p|a_n$. This fact is easy to prove directly but it is also a (very) special case of the Gauss Lemma.

but we know from (b) above that $\overline{f}$ has no quadratic factor. This is a contradiction, and hence f is irreducible.

A 2 (a) $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$ and we have seen in class as an application of the Eisenstein criterion that the polynomial $g(X) = X^4 + X^3 + X^2 + X + 1$ is irreducible. If ζ is as in Part (b) of the question, then $g(\zeta) = 0$ hence by what we said in class $\mathbb{Q}(\zeta) \cong \mathbb{Q}[X]/g$ as field extensions and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg g = 4$. The other roots of $g(X)$ are ζ^2, ζ^3 and ζ^4 and they are all in $\mathbb{Q}(\zeta)$ hence $K = \mathbb{Q}(\zeta)$ is the splitting field of $g(X)$ and hence also of $X^5 - 1$ and hence $[K : \mathbb{Q}] = 4$.

(b) Compute:

$$\alpha^2 = (\zeta + \frac{1}{\zeta})^2 = \zeta^2 + \frac{1}{\zeta}^2 + 2 = \zeta^2 + \zeta^3 + 2$$

hence using the identity $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$ (after all ζ is a root of g!) we get:

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

hence α is a root of the quadratic polynomial $X^2 + X - 1 \in \mathbb{Q}[X]$. Solving the quadratic equation we get

$$\alpha = \frac{-1 + \sqrt{5}}{2}$$

(It is clear that $\alpha > 0$ and hence it can not equal the other root of the quadratic equation.) From this we also by the way get $\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$.[2]

(c) The Galois group has order $4 = [K : \mathbb{Q}]$. Because G respects multiplication, $G \subset \operatorname{Aut}\mu_5 = (\mathbb{Z}/5\mathbb{Z})^\times \cong C_4$, a cyclic group of order 4. Hence $G \cong C_4$, generated by the automorphism that sends ζ to ζ^2 (for example).[3] G has only one nontrivial subgroup, and hence by the Galois correspondence $\mathbb{Q} \subset K$ has only one nontrivial intermediate field. But we already know from Part (b) a nontrivial intermediate field, and it is $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

[2] Did they tell you this in school?

[3] I expect that the previous two lines are not super-easy for you to digest. I strongly advise you to make sure that you understand this argument.