MATH 4E03/6E03 Galois Theory, Fall 2014
Homework 3 Solution

Total: 16 marks. No mark for any unjustified arguments using calculators.

(1) Show that if p is a prime, and if the regular p-gon (the regular polygon with p sides) is constructible, then p is of the form $2^{2^t}+1$ for some integer t. (3 marks)

(Hints: First show that p is of the form 2^k+1, then show that k must be of the form 2^t.)

Remark: A prime of the form $2^{2^t}+1$ is called a Fermat prime.

Remark 2: What is the condition on n (not necessarily a prime) such that a regular n-gon is constructible? We need Galois theory in Sec 19.3 of Garling. Hopefully we can discuss it in the future.

Answer: We first show that p is of the form 2^k+1. If we inscribe the regular p-gon in the unit circle on the plane, with one of the vertices being $(1,0)$, then the next vertex (in the anti-clockwise direction) is

$$(\cos(2\pi/p), \sin(2\pi/p)).$$

If we view the plane as the complex $\mathbb{C}$, then this vertex is just $\cos(2\pi/p)+i\sin(2\pi/p) = e^{2\pi i/p}$. Therefore, if the regular p-gon is constructible, then $e^{2\pi i/p}$ is a constructible number (over $\mathbb{Q}$). (1 mark)

By Theorem 6.1, the degree of extension

$$[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = 2^k$$

for some integer k. We have computed in class that $e^{2\pi i/p}$ is a root of the polynomial

$$X^{p-1} + X^{p-2} + \cdots + X + 1,$$

which is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p-1$ (1 mark) and so $p = 2^k+1$.

Remark: I checked that this polynomial is irreducible in a class before. Many of you re-did the proof, which is not necessary. Stating $[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p-1$ is good enough.

We then show that k must be of the form 2^t. If k has an odd factor, say $k = ab$ with a being odd, then

$$2^k + 1 = 2^{ab} + 1 = (2^b+1)((2^b)^{a-1} - (2^b)^{a-2} + \cdots - 2^b + 1),$$

which implies that p has a proper factor $2^b + 1 > 1$ and leads to a contradiction. (1 mark) □

(2) Using the method covered in class, compute the automorphism group of $\Sigma/\mathbb{Q}$, where Σ is the splitting field of $X^4 + 5X^2 + 5 \in \mathbb{Q}[X]$. (3 marks)

(Hints: The group is not the dihedral group D_8 covered in class. The reason is as follows. Let's recall the example in class: $f(X) = X^4 - 4X^2 + 5$ with roots

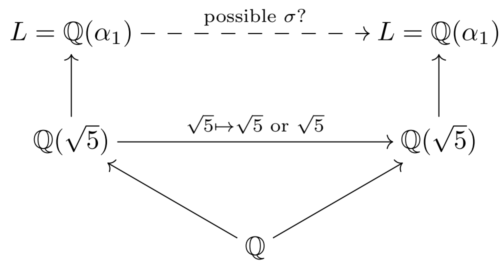
$$\alpha_1, \alpha_2 = \pm\sqrt{2+i}, \qquad \alpha_3, \alpha_4 = \pm\sqrt{2-i}.$$

The splitting field Σ is $\mathbb{Q}(\alpha_1, \alpha_3)$. We can compute $[\Sigma : \mathbb{Q}(\alpha_1)] = 2$ since $\alpha_3 \notin \mathbb{Q}(\alpha_1)$, and $[\mathbb{Q}(\alpha_1) : \mathbb{Q}(i)] = 2$, and so $[\Sigma : \mathbb{Q}] = 8$. However, in our question, the polynomial has roots

$$\alpha_1, \alpha_2 = \pm i\sqrt{\frac{5+\sqrt{5}}{2}}, \qquad \alpha_3, \alpha_4 = \pm i\sqrt{\frac{5-\sqrt{5}}{2}},$$

and $\alpha_3 \in \mathbb{Q}(\alpha_1)$ because $\alpha_1\alpha_3 = -\sqrt{5}$. Therefore we have $\Sigma = \mathbb{Q}(\alpha_1)$ and $[\mathbb{Q}(\alpha_1) : \mathbb{Q}(\sqrt{5})] = 2$.)

Answer: In this question we have the following tower of fields and automorphisms



(1)

Notice that $[L : \mathbb{Q}] = 4$ because we have the extra condition $\alpha_1\alpha_3 = -\sqrt{5}$. We expect the Galois group has order 4. We distinguish between two cases.

Case when $\sigma : \sqrt{5} \mapsto \sqrt{5}$. By arguing as in class, the possible permutations in the Galois group are

$$\text{Id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4).$$

However, under the extra condition $\alpha_1\alpha_3 = -\sqrt{5}$, a qualified permutation should satisfy $\sigma(\alpha_1\alpha_3) = \sigma(-\sqrt{5}) = -\sqrt{5}$. This condition hence cuts down half of the permutations. For example, $\sigma = (1\ 2)$ cannot be in the Galois group because

$$\begin{aligned} \sigma(\alpha_1\alpha_3) &= \sigma(-\sqrt{5}) = -\sqrt{5} \\ &= \sigma(\alpha_1)\sigma(\alpha_3) = \alpha_2\alpha_3 = \sqrt{5}, \end{aligned} \tag{2}$$

which is impossible. Arguing similarly, we find that (3 4) cannot be in the Galois group, and only Id and (1 2)(3 4) can be lying in the Galois group.

Case when $\sigma : \sqrt{5} \mapsto -\sqrt{5}$. The argument is similar to the case above. Just remember in this case a qualified permutation should satisfy $\sigma(\alpha_1\alpha_3) = \sigma(-\sqrt{5}) = \sqrt{5}$. We then find that only (1 3 2 4) and (1 4 2 3) can be lying in the Galois group, but (1 3)(2 4) and (1 4)(2 3) cannot.

Finally, we observe that the group

$$\{\text{Id}, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}$$

is isomorphic to the cyclic group $\mathbf{Z}_4$. Indeed, if we take $\rho = (1\ 3\ 2\ 4)$, then $\rho^2 = (1\ 2)(3\ 4)$, $\rho^3 = (1\ 4\ 2\ 3)$, and $\rho^4 = \text{Id}$. $\square$

(If you fail to use the condition $\alpha_1\alpha_3 = -\sqrt{5}$, you can only receive half of the marks.)

(3) (Garling Ex. 9.5) Let L/K be a normal extension. Suppose that f is a monic irreducible polynomial in $K[X]$ and g, h are monic irreducible factors of f in $L[X]$. Show that there exists a K-automorphism of L such that $\sigma(g) = h$. (3 marks)

(Hints: What are the relations between the roots of g and h?)

Answer: Let α be a root of g and β be a root of h. They are both a root of f, so by Extension Theorem 7.4, there is a K-isomorphism $j : K(\alpha) \to K(\beta)$ mapping $\alpha \mapsto \beta$.

$$\begin{array}{ccc} K(\alpha) & \overset{j}{\underset{\alpha\mapsto\beta}{\dashrightarrow}} & K(\beta) \\ \uparrow & & \uparrow \\ K & \xrightarrow{=} & K \end{array} \tag{3}$$

Let Σ be a normal extension containing both L and the splitting field of f over K; in particular, it contains both $K(\alpha)$ and $K(\beta)$. By applying Corollary 2 of Extension Theorem 7.5 for splitting field extensions successively, we can obtain a K-automorphism $k : \Sigma \to \Sigma$ extending $j : K(\alpha) \to K(\beta)$. In particular, $k(\alpha) = \beta$.

$$\begin{array}{ccc} \Sigma & \overset{k}{\dashrightarrow} & \Sigma \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow{j} & K(\beta) \end{array} \tag{4}$$

(1 mark for choosing appropriate Σ and k.)

Since L/K is normal, by Theorem 9.2, we have $k(L) = L$. Let σ be $k|_L$, which is now a K-automorphism of L.

$$\begin{array}{ccc} \Sigma & \xrightarrow{k} & \Sigma \\ \uparrow & & \uparrow \\ L & \overset{\sigma}{\dashrightarrow} & L \end{array} \tag{5}$$

(1 mark for defining σ.)

It remains to show that $\sigma(g) = h$. Now the above K-isomorphisms induce the following diagram

$$\begin{array}{ccccccc} L[X]/(g) & \xrightarrow[\text{evaluate at } \alpha]{\cong} & L(\alpha) & \xrightarrow{k|_{L(\alpha)}} & L(\beta) & \xleftarrow[\text{evaluate at } \beta]{\cong} & L[X]/(h) \\ \uparrow & & & & & & \uparrow \\ L & & & \xrightarrow{\sigma} & & & L \end{array} \tag{6}$$

The top compositions of isomorphisms is induced from the surjection

$$L[X] \xrightarrow[\cong]{\sigma} L[X] \to L[X]/(h),$$

where g is mapped to $0 \in L[X]/(h)$; in other words, $\sigma(g)$ lies in the ideal generated by h, which means that $\sigma(g)$ is a $L[X]$-multiple of h. Apply the same argument to $\sigma^{-1}(h)$, then $\sigma^{-1}(h)$ is a $L[X]$-multiple of g. But we know that the pair of polynomials g and $\sigma(g)$ have the same degree, and so are the pair h and $\sigma^{-1}(h)$. The arguments above forces that g and h have the same degree, i.e. $\sigma(g)$ is a L-multiple of h. Since both are assumed to be monic, we have $\sigma(g) = h$. (1 mark) $\square$

Remark: Most of you did this question remarkably well, like choosing the correct splitting field Σ and use the various Extension Theorems appropriately.

Remark 2: Many of you assumed something like $\deg(g) \leq \deg(h)$, which is not necessarily. Is it a coincidence?

(4) (Garling Ex. 9.6) Suppose that L/K is algebraic. Show that the following are equivalent.

(i) L/K is normal;

(ii) if j is a K-monomorphism from L to $\bar{L}$ (the algebraic closure of L), then $j(L) \subset L$;

(iii) if j is a K-monomorphism from L to $\bar{L}$, then $j(L) = L$.

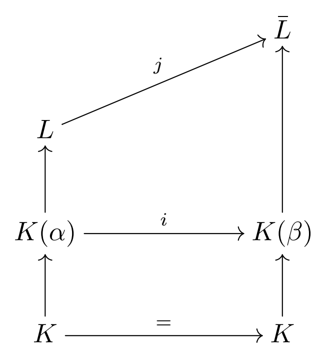
(4 marks)

(Hints: You may want to copy the proof of Theorem 9.3. However, here $[L : K]$ could be ∞, so that some arguments of the proof of Theorem 9.3 do not apply here. You may take the proof there as a reference, but eventually you need to produce a new proof for the above question.)

Answer: (i)⇒(ii). Given (i) that L/K is normal, and $j : L \to \bar{L}$ is a K-monomorphism, we want to show that $j(L) \subseteq L$. It is the same to show that given every $\alpha \in L$, we have $j(\alpha) \in L$. We know that $j(\alpha)$ is also a root of the minimal polynomial $m_\alpha \in K[X]$, by the argument similar to the proof of Theorem 9.2. Hence $j(\alpha) \in L$ by the normality of L/K. (1 mark)

(ii)⇒(iii). Given (ii) that every K-monomorphism $j : L \to \bar{L}$ satisfies $j(L) \subseteq L$, so that $j : L \to L$ is defined. We want to show that $j(L) = L$, which is the same as to show that $j : L \to L$ is surjective, or the same as to show that for every $\beta \in L$, there is $\alpha \in L$ such that $j(\alpha) = \beta$. Let Σ/K be the splitting field extension of $m_\beta \in K[X]$. Since (i)⇒(ii) is proved above, we apply it to the normal extension Σ and the K-monomorphism $j|_\Sigma : \Sigma \to \bar{L} = \bar{\Sigma}$, so that we have $j|_\Sigma(\Sigma) \subseteq \Sigma$. Since Σ/K has finite degree, we actually have $j|_\Sigma(\Sigma) = \Sigma$. Since $\beta \in \Sigma$, we can find $\alpha \in \Sigma$ such that $\beta = j|_\Sigma(\alpha)$. Since $\Sigma \subseteq L$, we have $\alpha \in L$ and $j(\alpha) = j|_\Sigma(\alpha) = \beta$. Therefore j is surjective. (1.5 marks)

(iii)⇒(i). Given (iii) that every K-monomorphism $j : L \to \bar{L}$ satisfies $j(L) = L$, to show L/K is normal, it is enough to show that if $\alpha \in L$ and β is a root of $m_\alpha \in K[X]$, then $\beta \in L$. We now prove by contradiction: suppose that $\beta \notin L$. Suppose that $i : K(\alpha) \to K(\beta)$ is a K-isomorphism mapping $\alpha \mapsto \beta$ (whose existence is due to Extension Theorem 7.4). Then any K-monomorphism $j : L \to \bar{L}$ extending i (if there exists any such j, see the remark below) does not satisfy $j(L) = L$, because $j(\alpha) = k(\alpha) = \beta \notin L$. This contradicts the given condition (iii). (1.5 marks)



(7)

Remark: If you really want to argue that such a K-monomorphism j exists, you require Zorn's Lemma, which is Theorem 8.3 I have not covered in class. I did not deduct any mark if you did not use this Lemma. Usually I avoid using it. □

(5) Recall that $\mathbb{Z}_p$ is a finite field of p elements. Take our base field to be $K = \mathbb{Z}_p(T)$, the field of rational polynomials with variable T. Explicitly,

$$K = \left\{ \frac{f}{g}, \text{ where } f, g \in \mathbb{Z}_p[T] \text{ and } g \neq 0 \right\}.$$

Consider the polynomial ring $K[X] = \mathbb{Z}_p(T)[X]$.

(i) Show that the polynomial $f(X) = X^p - T \in K[X]$ is irreducible. (1 mark) (Hints: Remember one of the exercise in the previous homework.)

Answer: We apply Exercise 3 of Homework 2, which states that $F(X) - YG(X)$ is irreducible in $L(Y)[X]$ if $\gcd(F(X), G(X)) = 1$ in $L[X]$ (notice that some notations are changed from the Exercise). In above question we take $L = \mathbb{Z}_p$, $Y = T$, $F(X) = X^p$ and $G(X) = 1$. $\square$

Remark: Some of you did not use Exercise 3 of Homework 2. They mentioned that T is a prime in the 'ring of integers' $\mathbb{Z}_p[T]$ of the field $\mathbb{Z}_p(T)$, so that the given polynomial $X^p - T$ is T-Eisenstein. This is also a nice proof.

(ii) Describe the roots of f. (Since $\deg(f) = p$, there are p roots.) Show your work. (2 marks)

Answer: Suppose that one of the root of $X^p - T$ is α, so that $\alpha^p = T$. Then we have

$$X^p - T = X^p - \alpha^p = (X - \alpha)^p. \qquad \text{(1 mark)}$$

The last equality is valid in characteristic p. Therefore, α is a repeated root of multiplicity p. In other words, all p roots are equal. (1 mark) $\square$

Remark: this is a typical example of an inseparable polynomial.