MATH 4E03/6E03 Galois Theory, Fall 2014
Homework 6, Due Monday, December 8, 12:00 noon

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

(1) (Garling Ex 16.4) Suppose that q is a prime, that $\mathrm{char}(K) \neq q$, and that $X^q - \theta$ is irreducible in $K[X]$. Let ω be a primitive qth root of unity and let $j = [K(\omega) : K]$. Also let L/K be the splitting field extension of $X^q - \theta$. Show that the Galois group of can be generated by two elements σ and τ such that

$$\text{the orders are given by } \sigma^q = \tau^j = \mathrm{Id}_L, \text{ with relation } \sigma^k \tau = \tau\sigma,$$

where $k \in \mathbb{Z}_q^\times$ whose multiplicative order is j. (2 marks)

Answer: Let L be the splitting field of $X^q - \theta$, such that we have a tower $K \hookrightarrow K(\omega) \hookrightarrow L = K(\omega, \alpha)$, where $\alpha^n = \theta$ and $\omega = \zeta_q$. We know from Theorem 15.4 that $\Gamma(K(\omega)/K) \hookrightarrow \mathbb{Z}_q^\times$. Since q is a prime, we know that $\mathbb{Z}_q^\times$ is a cyclic group of order $q-1$, so $\Gamma(K(\omega)/K)$ is also cyclic if we view it as a subgroup of $\mathbb{Z}_q^\times$. We choose a generator $\rho \in \Gamma(K(\omega)/K)$ and a number $k \in \mathbb{Z}_q^\times$ with multiplicative order $j = \#\Gamma(K(\omega)/K) = [K(\omega) : K]$. The above isomorphism can be explicitly written as

$$\Gamma(K(\omega)/K) \hookrightarrow \mathbb{Z}_q^\times,\ \rho \mapsto k,$$

which means that $\rho(\omega) = \omega^k$. We then extend the automorphism ρ of $K(\omega)$ to an automorphism τ of L by defining

$$\tau|_{K(\omega)} = \rho \text{ and } \tau(\alpha) = \alpha,$$

so that τ also has order j.

Many of you did not mention that τ is an extension of ρ. To be rigorous, we have to do so because we want τ to be an automorphism of L, while ρ is only an automorphism of the subfield $K(\omega)$.

Now we consider the Galois group $\Gamma(L/K(\omega))$. It is given that $X^q - \theta$ is irreducible over K. Suppose we know that $X^q - \theta$ is irreducible over $K(\omega)$ (which will be shown below), then by Theorem 16.1, we know that $\Gamma(L/K(\omega))$ is a cyclic group of order q. Explicitly, if we choose a generator $\sigma \in \Gamma(L/K(\omega))$, then we have $\sigma(\alpha) = \omega\alpha$. Therefore, we know that (explained in class)

$$\Gamma(L/K) \cong \langle\sigma\rangle \rtimes \langle\tau\rangle .$$

In class, I showed the conjugacy relation $\tau\sigma\tau^{-1} = \sigma^k$. I now provide the argument again. It is enough to show that $\tau\sigma$ and $\sigma^k\tau$ define the same automorphism on L. Remember that $L = K(\omega, \alpha)$, so we compute directly that

$$\tau\sigma(\omega) = \tau(\omega) = \omega^k,\ \tau\sigma(\alpha) = \tau(\omega\alpha) = \omega^k\alpha;$$

and

$$\sigma^k\tau(\omega) = \sigma^k(\omega^k) = \omega^k,\ \sigma^k\tau(\alpha) = \sigma^k(\alpha) = \omega^k\alpha.$$

Therefore, we conclude that $\Gamma(L/K) \cong \left\langle \sigma,\, \tau \text{ where } \sigma^q = 1,\, \tau^j = 1, \text{ and } \tau\sigma\tau^{-1} = \sigma^k \right\rangle .$ □

To be rigorous, we have to show that $X^q - \theta$ is irreducible over $K(\omega)$. (I did not deduct any marks if you did not show this.) The arguments proceed as follows. Suppose β is a root of $X^q - \theta$ and m_β is its minimal polynomial over $K(\omega)$. Then $[K(\omega, \beta) : K(\omega)] = \deg m_\beta > 1$, but it must be a divisor of q by Theorem 16.1. Hence $\deg m_\beta = q$ and m_β must equal $X^q - \theta$.

(2) Let G be a finite group. We call G *nilpotent* if there is a finite series of subgroups

$$\{1\} = G_n \subsetneq G_{n-1} \subsetneq \cdots \subsetneq G_0 = G$$

such that G_i is normal in G for all i and G_i/G_{i+1} lies in the center of G/G_{i+1} for all i. (Remark: It seems that the definition of nilpotent groups in Ex 17.1 of the book is wrong or outdated. If you check Dummit-Foote or some other algebra textbooks, you will find the definition the same as or equivalent to the one above.)

(a) Show that if a finite group G is nilpotent, then it is solvable. (2 marks) (Hint: You may need to know the structure of a finite abelian group.)

Answer: Suppose G is nilpotent, so there is a finite series of subgroups

$$\{1\} = G_n \subsetneq G_{n-1} \subsetneq \cdots \subsetneq G_0 = G$$

such that G_i is normal in G for all i and G_i/G_{i+1} lies in the center of G/G_{i+1} for all i. Hence G_i/G_{i+1} is in particular abelian. By the Structure Theorem of finite abelian groups, we write

$$G_i/G_{i+1} \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_{m_i}}.$$

Let $H_{i,j}$ be an intermediate subgroup between G_i and G_{i+1} such that

$$H_{i,j}/G_{i+1} \cong \mathbb{Z}_{d_{j+1}} \oplus \cdots \oplus \mathbb{Z}_{d_{m_i}}.$$

Therefore, we have a tower of subgroups

$$G_{i+1} = H_{i,m_i} \subsetneq \cdots \subsetneq H_{i,1} \subsetneq H_{i,0} = G_i$$

such that $H_{i,j}/H_{i,j+1} \cong \mathbb{Z}_{d_j}$ is cyclic. The enlarged tower

$$\begin{aligned}&\{1\} = G_n = H_{n-1,m_{n-1}} \subsetneq H_{n-1,m_{n-1}-1} \subsetneq \cdots \subsetneq G_{i+1} = H_{i,m_i} \subsetneq \\ &\cdots \subsetneq H_{i,1} \subsetneq H_{i,0} = G_i \subsetneq \cdots \subsetneq H_{0,0} = G_0 = G\end{aligned}$$

implies that G is solvable. □

(b) Give an example of a finite solvable group which is not nilpotent, and justify your answer. (1 mark) (Hint: One example of such a group has order 6.)

Answer: The permutation group of 3 elements $G_0 = \Sigma_3$ is solvable but is not nilpotent. Notice that the only normal subgroup of G_0 is A_3, so the only normal series of $G_0 = \Sigma_3$ is

$$G_2 = \{1\} \subsetneq G_1 = A_3 \subsetneq G_0 = \Sigma_3.$$

However, $G_1/G_2 \cong A_3$ is not contained in the center of $G/G_2 = \Sigma_3$, which is just trivial. Hence Σ_3 is not nilpotent. □

(c) (Garling Ex 17.2) Show that if the order of a group G is a power of a prime number, then G is nilpotent. (2 marks) (Hint: Check one of the questions in Homework 1.)

Answer: In the simplest case if G has order p, then it must be isomorphic to the additive cyclic group $\mathbb{Z}_p$, which is clearly nilpotent. In general, if the order of a group G is a power of a prime number, say p, then the center ZG of G is non-trivial by one of the exercises in Homework 1, and so it has order also a power of p. The quotient group $\bar{G} = G/ZG$ has order also a power of p, but it strictly smaller than that of G. Hence we can apply induction and claim that $\bar{G}$ is nilpotent, so by definition there is a tower of subgroups

$$\{1\} = \bar{G}_n \subsetneq \bar{G}_{n-1} \subsetneq \cdots \subsetneq \bar{G}_0 = \bar{G} = G/ZG$$

such that $\bar{G}_i$ is normal in $\bar{G}$ for all i and $\bar{G}_i/\bar{G}_{i+1}$ lies in the center of $\bar{G}/\bar{G}_{i+1}$ for all i. Now let G_i be the subgroup of G whose quotient by ZG is $\bar{G}_i$ (such a subgroup exists by a consequence of the Isomorphism Theorem in Group theory). Then $G_n = ZG$ and we have a tower

$$\{1\} = G_{n+1} \subsetneq ZG = G_n \subsetneq G_{n-1} \subsetneq \cdots \subsetneq G_0 = G$$

such that G_i is normal in G for all i and $G_i/G_{i+1} \cong \bar{G}_i/\bar{G}_{i+1}$ lies in the center of $G/G_{i+1} \cong \bar{G}/\bar{G}_{i+1}$ for all i. Therefore, G is nilpotent by definition. □

These questions are done poorly. I think the main reason is that I don't have enough time in class to cover the techniques about solvability. However, the questions reveal that a number of you do not have solid background in group theory. There are a few serious mistakes (among others not listed).

- Many of you stated Sylow's Theorem wrongly. Even though some of you could state the theorem correctly, it was used in incorrect ways. (Actually, all the questions above have nothing to do with Sylow's Theorem.)
- Many of you defined some basic concepts (center of a group, normal subgroup, etc.) wrongly. Something like $G/Z(G) \lhd G$ or $Z(G/Z(G)) \lhd Z(G)$ is unacceptable.
- Some of you wrote something like $\Sigma_3/\mathbb{Z}_2$ and claim it is a group. Strictly speaking, there is no relation between Σ_3 and $\mathbb{Z}_2$. You should first realize $\mathbb{Z}_2$ as a subgroup of Σ_3; but even though you had done so, you cannot take quotient because there is no normal subgroup of Σ_3 of order 2. This is important, as we have seen that there are two realizations of V_4 in Σ_4 where one realizes V_4 as a normal subgroup of Σ_4 and another does not.

Another problem is that many of you used definition of solvable group which is not covered in class, or used definition of nilpotent group different from the given one (probably adopted from some textbooks or some online texts). Many of you did not show that your definition is equivalent to the one given in class or in the assignment, and I really doubt if you know how to show it.

(3) This question shows that the condition in Theorem 17.3, that $\mathrm{char}(K)$ does not divide $\Gamma(L/K)$, is crucial.

(a) Show that $f = X^p - X - 1 \in \mathbb{Z}_p[X]$ is irreducible. (Hint: Part of the hint is in Garling Ex 16.9. Let β be a root of f and suppose that $f = m_\beta h$, where $m_\beta \in \mathbb{Z}_p[X]$ is the minimal polynomial of β with $\deg(m_\beta) \lneq \deg(f)$. Consider the sum of roots of m_β and see if you can get a contradiction.) (2 marks)

Answer: I first explain that if β is a root of f, then $\beta+1$, $\beta+2$, $\beta+p-1$ are the remaining roots of f. This comes from direct computation:

$$f(\beta+a) = (\beta+a)^p - (\beta+a) - 1 = \beta^p + a^p - \beta - a - 1$$
$$\text{since } (\beta+a)^p = \beta^p + a^p \text{ in char } p.$$

Now $a \in \mathbb{Z}_p$, so $a^p = a$. Also $\beta^p - \beta - 1 = 0$. Therefore $f(\beta + a) = 0$.

Suppose that $f = m_\beta h$, where $m_\beta \in \mathbb{Z}_p[X]$ is the minimal polynomial of β with $\deg(m_\beta) = d \lneq \deg(f)$. Consider the sum of roots of m_β, which is of the form $\sum(\beta + k_i) = d\beta + e$ for some $e \in \mathbb{Z}_p$. Since $d \in \mathbb{Z}_p^\times$ and the sum of roots is in $\mathbb{Z}_p$, this forces $\beta \in \mathbb{Z}_p$, a contradiction. □

A few of you used an argument from HW3 Q3 that $f = X^p - X - 1$ should break up into polynomials of same degree, and since p is a prime, it either breaks up into linear factors or irreducible. This argument is wrong. If you check the conditions from HW3 Q3, you need to have the irreducibility of f in advance. This is what I ask you to show and you cannot assume it.

(b) Show that f is not solvable by radical, although its Galois group is solvable. (Hint: The second statement is easy. The first statement may need some thinking. As a starting point: what if the root of f depends on a radical α, so that $\alpha^m \in \mathbb{Z}_p$? What can be the possible m?) (3 marks)

Answer: We know that every Galois group of a finite extension over a finite field is cyclic, hence solvable. So the second statement is clear. For the first statement, suppose that the extension L/K is solvable by radical, then by definition L/K lies in a tower of extensions by radicals as the following diagram.

$$\begin{tikzcd}
 & & L \arrow[rrd] & & \\
\mathbb{Z}_p \arrow[rru] \arrow[r] & L_1 \arrow[r] & L_2 \arrow[r] & \cdots \arrow[r] & L_r
\end{tikzcd}$$

There are various arguments showing that this tower is problematic. Below is one of those. Since $[L_r : \mathbb{Z}_p]$ is divisible by $[L : \mathbb{Z}_p] = p$, there is an intermediate extension L_i/L_{i-1} whose degree is divisible by p. Let $m = [L_i : L_{i-1}]$, so that $L_i = L_{i-1}[\alpha]$ with $\alpha \notin L_{i-1}$ but $\alpha^m \in L_{i-1}$. We now apply a reduction: let $L'_{i-1} = L_{i-1}[\alpha^{m/p}]$, then we have the following tower of extensions by radicals

$$L_{i-1} \hookrightarrow L'_{i-1} = L_{i-1}[\alpha^p] = L_i = L_{i-1}[\alpha] = L'_{i-1}[\alpha].$$

It is clear that $[L'_{i-1} : L_{i-1}] = m/p$ and $[L_i : L'_{i-1}] = p$. We now look at the extension L_i/L'_{i-1} and see how we get a contradiction. Since $\alpha \notin L'_{i-1}$ but $\alpha^p \in L'_{i-1}$, the minimal polynomial $m_\alpha \in L'_{i-1}[X]$ is divisible by $X^p - \alpha^p$. But in characteristic p we have $X^p - \alpha^p = (X - \alpha)^p$. Hence $m_\alpha = X - \alpha$, i.e., the minimal polynomial is linear. It forces that $\alpha \in L'_{i-1}$ which is a contradiction. □

Remark: The given polynomial is called Artin-Schreier polynomial. You may check the Wikipedia entry ‘Artin-Schreier theory’ for more details.

(4) This question shows that even though a field extension is solvable, it may not be an extension by any radicals, i.e. a field extension L of K is not of the form $K(\alpha)$ where α has some power in K, even though $\Gamma(L/K)$ is solvable.

(a) (Garling Ex 17.4) Let f be an irreducible cubic in $K[X]$, where K is a subfield of $\mathbb{R}$. Show that f has three real roots if and only if its discriminant is positive. (2 marks)

Answer: This can be proved by direct calculation. If f has three distinct roots $\alpha_1, \alpha_2, \alpha_3$ which are all real, then $\delta = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$ is real and $\Delta = \delta^2$ is clearly positive. Otherwise, if $\alpha_1 = c$ is real but $\alpha_2 = a + bi$ and $\alpha_3 = a - bi$ are complex (with $b \neq 0$), then

$$\delta = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) = (a + bi - c)(a - bi - c)(a - bi - (a + bi)).$$

The product of first two factors is positive as they are conjugates of each other. The last factor is $-2bi$ which is purely imaginary, so its square is negative. □

(b) (Garling Ex 17.7) Give an example of a polynomial in $\mathbb{Q}[X]$ which is solvable by radicals, but its splitting field is not an extension by radicals. Justify your answer. (2 marks) (You don't need to use Ex 17.5 or 17.6, but if you use them, you have to prove them.)

Answer: Take a cubic polynomial whose discriminant is a positive square, so that its Galois group is a solvable group A_3 and all roots of f are real by (a). Recall the formula: if $f(X) = X^3 + bX + c$, then $\Delta = -4b^3 - 27c^2$. Take $(b, c) = (-3, 1)$ for example, then $f = X^3 - 3X + 1$ is a required polynomial, with $\Delta = 81$. (Another example, given by one of you, is $X^3 - 21X + 7$, with $\Delta = 35721 = 189^2$.)

Now suppose that $L/\mathbb{Q}$ is an extension by radicals, i.e., there is a tower of extension generated by radicals: $\mathbb{Q} \hookrightarrow L_1 \hookrightarrow \cdots \hookrightarrow L_r = L$. However, since Δ is a square in $\mathbb{Q}$, we have $\Gamma(L/\mathbb{Q}) \cong A_3$ and so $[L : \mathbb{Q}] = 3$. This forces that $r = 1$ and $L_r = L_1 = L$. Hence we suppose that $L = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{R}$ such that $\theta = \alpha^3$ is in $\mathbb{Q}$. We know that the other two roots are $e^{2\pi i/3}\alpha, e^{4\pi i/3}\alpha \in \mathbb{C} - \mathbb{R}$, but they are in the normal extension L which is totally real. We have a contradiction. □

Suggested Exercises (no need to hand in): 16.1, 16.2, 16.3, 16.5, 16.9, 16.10, 16.11. 16.12, 16.13, 16.14, 16.15, 16.16, 17.3, 17.5, 17.6.