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

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

(1) Let L/K be a Galois extension and M_1 and M_2 be two intermediate subfields between L and K. Define the composite field M_1M_2 of M_1 and M_2 as the smallest subfield containing both M_1 and M_2.

(i) Prove that $\Gamma(L/M_1M_2) = \Gamma(L/M_1) \cap \Gamma(L/M_2)$. (2 marks)

Answer: Recall the definition of Galois group, for every intermediate field extension M between L/K,

$$\Gamma(L/M) = \{\sigma \in \Gamma(L/K) \text{ such that } \sigma|_M = \mathrm{Id}_M\}.$$

If $\sigma \in \Gamma(L/M_1M_2)$, then $\sigma|_{M_1M_2} = \mathrm{Id}_{M_1M_2}$. Since both M_1 and M_2 are contained in M_1M_2, we have $\sigma|_{M_1} = \mathrm{Id}_{M_1}$ and $\sigma|_{M_2} = \mathrm{Id}_{M_2}$, and so

$$\Gamma(L/M_1M_2) \subseteq \Gamma(L/M_1) \cap \Gamma(L/M_2). \qquad \text{(1 mark for one inclusion)}$$

To show the reverse inclusion, we let $\Gamma(L/M_1) \cap \Gamma(L/M_2) = \Gamma(L/M)$ for a certain intermediate field extension M/K in L (whose existence is by Galois Correspondence). Notice that $\Gamma(L/M_1) \cap \Gamma(L/M_2)$ is the largest subgroup contained in both $\Gamma(L/M_1)$ and $\Gamma(L/M_2)$. By Galois Correspondence again and also by its order reversing property, M is the smallest subfield containing both M_1 and M_2, so it must be M_1M_2. (1 mark for another) □

(ii) Suppose further that M_1/K is Galois.

(a) Show that M_1M_2/M_2 is Galois. (2 marks)

Answer: We use the fact that a Galois extension is separable and normal.

- Since L/K is Galois, it is separable and by Theorem 10.1, any intermediate sub-extension between L and K, in particular M_1M_2/M_2, is separable. (1 mark)
- To show that it is normal, notice that M_1/K is given to be Galois, so it is normal, and so it is a splitting field of some polynomials $\{f_i\} \subseteq K[X]$. If we view these polynomials as in $M_2[X]$, then the splitting field for these polynomials is M_1M_2 (explained below). Hence M_1M_2/M_2 is normal. (1 mark)
  To show that M_1M_2 is the splitting field of $\{f_i\} \subseteq K[X]$ viewed as in $M_2[X]$, we write $M_1 = K[\alpha_1, \ldots, \alpha_m]$, where $\{\alpha_j\}$ are the set of all roots of $\{f_i\}$. Then the splitting field of $\{f_i\} \subseteq M_2[X]$ is $M_2[\alpha_1, \ldots, \alpha_m]$. Notice that this is the smallest subfield containing both M_1 and M_2, so it must be M_1M_2. (It is fine if you did not show these.)

□

(b) Show that $\Gamma(M_1M_2/M_2)$ is isomorphic to $\Gamma(M_1/M_1 \cap M_2)$. (2 marks)

Answer: Define the restriction homomorphism

$$R : \Gamma(M_1M_2/M_2) \to \Gamma(M_1/M_1 \cap M_2),\ \sigma \mapsto \sigma|_{M_1}.$$

There are three steps we need to check.

- We have to show that we the map is well-defined, which means that $\sigma|_{M_1}$ has to be an automorphism of M_1 fixing $M_1 \cap M_2$. To show that $\sigma(M_1) = M_1$, notice that every $\sigma \in \Gamma(M_1M_2/M_2)$ is in particular in $\Gamma(M_1M_2/K)$ and M_1/K is given to be normal. By Theorem 9.2, we have $\sigma(M_1) = M_1$. The fact that $\sigma|_{M_1}$ fixing $M_1 \cap M_2$ is easy to show. (I did not deduct any mark if you did not show these.)
- We then show that R is injective. Suppose that $R : \sigma \mapsto \sigma|_{M_1} = \mathrm{Id}_{M_1}$, then remember that $\sigma \in \Gamma(M_1M_2/M_2)$ implies that $\sigma|_{M_2} = \mathrm{Id}_{M_2}$. Hence σ is trivial on the field generated by M_1 and M_2, which is M_1M_2. Therefore, $\sigma = \mathrm{Id} \in \Gamma(M_1M_2/M_2)$, and R is injective. (1 mark)
- To show that R is surjective, we consider the image of R, which is a subgroup of $\Gamma(M_1/M_1 \cap M_2)$, say of the form $\Gamma(M_1/M)$ for some intermediate field extension $M/M_1 \cap M_2$ in M_1.

$$\begin{tikzcd}
 & M_1M_2 \\
M_1 \arrow[ur] & M_2M \arrow[u] \\
M \arrow[u] \arrow[ur] & M_2 \arrow[u] \\
M_1 \cap M_2 \arrow[u, "=?"] \arrow[ur] &
\end{tikzcd} \tag{1}$$

Hence if $\sigma \in \Gamma(M_1M_2/M_2)$ with $R(\sigma) = \sigma|_{M_1}$, then $\sigma|M = \mathrm{Id}_M$ and so $\sigma|_{M_2M} = \mathrm{Id}_{M_2M}$. In other words, $\sigma \in \Gamma(M_1M_2/M_2M) \subseteq \Gamma(M_1M_2/M_2)$. But σ is an arbitrary element in $\Gamma(M_1M_2/M_2)$. This forces $M_2M = M_2$, and so $M \subseteq M_2$. We know that $M \subseteq M_1$, so $M \subseteq M_1 \cap M_2$. But we also know that $M_1 \cap M_2 \subseteq M$, so $M_1 \cap M_2 = M$. (1 mark)

□

(2) (Garling Ex. 11.9, modified) Given an arbitrary finite group G, show that there exists a Galois extension L/K, where L is a finite extension over $\mathbb{Q}$, such that $\Gamma(L/K) \cong G$. (2 marks)

(Hint: You may use Theorem 11.7.)

Remark: If L is a finite extension over a finite field $\mathbb{Z}_p$, then the statement is not true. We will see that every Galois group of a finite extension over a finite field is cyclic.

Answer: We view G as a subgroup of Σ_n for some n. By choosing a prime number $p > n$ and view Σ_p as a subgroup of Σ_p , we can view G as a subgroup of Σ_p. (1 mark)

Take a normal extension $L/\mathbb{Q}$ whose Galois group is Σ_p. The existence of such an extension is guaranteed by Theorem 11.7.

Then the field extension $K/\mathbb{Q}$ is the one corresponding to the subgroup G of Σ_p under the Galois Correspondence.

$$\begin{tikzcd}
L & 1 \arrow[d] \\
K \arrow[u] & G \arrow[d] \\
\mathbb{Q} \arrow[u] & \Sigma_p
\end{tikzcd} \tag{2}$$

(1 mark, applying Galois Correspondence is required. Some of you try $L/K = \mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(\{f\})$, where f runs through all symmetric polynomials in $x_1, \ldots, x_n$. The problem for this is that $L/\mathbb{Q}$ is infinite.)

□

(3) (Garling Ex. 11.5) Describe all transitive subgroups of Σ_4, up to conjugacy (which means that we view a subgroup H of Σ_4 being the same as $\sigma H \sigma^{-1}$, for every $\sigma \in \Sigma_4$). (4 marks)

(Hint: First find out the possible orders of such subgroups. Then for each possible order, find out the possible subgroups with this order and explain why these subgroups exhaust all possibilities.)

(More Hint: There are four possible orders, and five transitive subgroups up to conjugacy. So in almost all cases, you only have one choice of transitive subgroup with the chosen order.)

Answer: If H is a transitive subgroup of Σ_4, then every H-orbit of $X_4 = \{1,2,3,4\}$ is X_4 itself. Hence by the fact that $\#(H/\mathrm{Stab}_H(x)) = \#\mathrm{Orb}_H(x) = \#X_4 = 4$, the order $\#H$ of H must be a multiple of 4. Since $\#\Sigma_4 = 4! = 24$, the possible cases are $\#H = 4, 8, 12$ or 24. (1 mark for listing out the possible orders. Some of you list out all orders $1, 2, 3, 4, 6, 8, 12, 24$ and argue that we can exclude the cases of orders $1, 2, 3, 6$. The arguments are usually clumsy but still acceptable.)

(i) When $\#H = 24$, then $H = \Sigma_4$.

(ii) When $\#H = 12$, then H must be isomorphic to A_4, because it is known that A_n is the only subgroup of Σ_n having index 2. It is easy to check that A_4 is transitive by listing the elements. (1/2 mark)

(iii) When $\#H = 8$, then H is a 2-Sylow subgroup of Σ_4. All 2-Sylow subgroups are conjugate (by Sylow's Theorem in group theory), in other words, there is only one such a subgroup up to conjugacy. We have seen in class that the dihedral group D_8 can be realized as a subgroup of Σ_4. Therefore, H is isomorphic to D_8. (1 mark, must show that this is the only realization, either by Sylow's Theorem or some other justified arguments.)

(iv) When $\#H = 4$, then there are only two possibilities: the Klein 4-group $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and the cyclic group $\mathbb{Z}_4$.

(a) If $H \cong V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, we let ρ and τ be two generators of V_4, both of order 2, so that $V_4 = \{\mathrm{Id}, \rho, \tau, \rho\tau\}$. One realization of V_4 in Σ_4 is

$$\rho = (1\ 2)(3\ 4),\ \tau = (1\ 3)(2\ 4), \text{ and so } \rho\tau = (1\ 4)(3\ 2).$$

I claim that this is the possible realization, up to conjugacy (or relabelling). Suppose there is another one. Since ρ and τ have order 2, they are either a transposition or a product of disjoint transpositions. We may assume that one of them, say ρ, is a transposition. (Otherwise, if both ρ and τ are products of disjoint transpositions, then we go back to the above realization.) Assume $\rho = (1\ 2)$ by relabelling. Then we can check case by case that if τ is one of the following:

$$(a\ b) \qquad \text{(with one of } a, b \text{ is 1 or 2)}, \qquad (1\ 3)(2\ 4), \qquad \text{or } (1\ 4)(3\ 2),$$

then the group generated by ρ and τ is not V_4 (in each case, there exists either only $\rho = (1\ 2)$ itself, a 3-cycle, or a 4-cycle). Therefore, τ can only be $(3\ 4)$ or $(1\ 2)(3\ 4)$, and so the group generated by ρ and τ is

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

But this is not a transitive subgroup of Σ_4. (1 mark, must show that there are two realizations and only one of them is transitive.)

(b) If $H \cong \mathbb{Z}_4$, then we know one of the realization is

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

(For example, see the last Homework.) Up to conjugacy, this is the only realization, since $H \cong \mathbb{Z}_4$ must contain a 4-cycle, and up to relabelling (conjugacy) we can assume it to be $(1\ 3\ 2\ 4)$. (1/2 mark)

If you forgot to check the conjugacy of subgroups (especially for $\mathbb{Z}_4$, where two conjugacy classes are allowed), you get at most 2 marks out of 4. □

(4) (Garling Ex. 12.11) Let $p < q$ be two prime numbers such that $(p, q-1) = 1$. Show that there is a unique (up to isomorphism) finite field extension $L/\mathbb{Z}_q$ which is the splitting field extension of *all* polynomials $X^p - a$, where $a \in \mathbb{Z}_q^\times$. (2 marks)

Remark: This statement is not true if $\mathbb{Z}_q$ is replaced by $\mathbb{Q}$. Clearly, we do not have a finite extension containing all the roots of $X^2 - a$, where $a \in \mathbb{Q}$.

Answer: In fact, the given condition implies that for every $a \in \mathbb{Z}_q^\times$, the polynomial $X^p - a$ contains a root in $\mathbb{Z}_q^\times$. Because of the following fact:

Lemma. *The map $a \mapsto a^p$ is a bijection on the set $\mathbb{Z}_q^\times$.* Proof: It is enough to show it is injective. Suppose $a^p = b^p$, then $(a/b)^p = 1$ (remember we are in characteristic p). Also notice that $\mathbb{Z}_q^\times$ is an abelian group of order $q-1$, so that $(a/b)^{q-1} = 1$. Now the given condition $(p, q-1) = 1$ shows that there exists $s, t \in \mathbb{Z}$ such that $sp + t(q-1) = 1$, and so

$$a/b = (a/b)^1 = (a/b)^{sp+t(q-1)} = ((a/b)^p)^s((a/b)^{q-1})^t = 1^s 1^t = 1.$$

Hence $a = b$. Q.E.D. Lemma. (1 mark for this Lemma, or any equivalent statements)

For each $a \in \mathbb{Z}_q^\times$, let $c^p = a$ for some $c \in \mathbb{Z}_q^\times$. Therefore, if we adjoin to $\mathbb{Z}_q$ a primitive pth root of unity $\zeta \in \bar{\mathbb{Z}}_q$, i.e., take $L = \mathbb{Z}_q[\zeta]$, then L contains all roots $c, \zeta c \ldots, \zeta^{p-1}c$ of $X^p - a$. This is true for all a, and so L is the required field extension. (1 mark for identifying L.) □

(5) Compute and simplify

$$\prod_{d|n} \prod_{\substack{f \in \mathbb{Z}_p[X] \\ \deg(f)=d \\ f \text{ is irreducible}}} f,$$

i.e., the factors f runs through all irreducible polynomials in $\mathbb{Z}_p[X]$ of degree d, and d runs through all divisors of n. (2 marks)

Answer: Actually, my intention is to have the answer equal to $X^{p^n} - X$. This requires all polynomials in the product to be monic. I will give the proof below under this condition.

The product is $X^{p^n} - X$. We know from class that the splitting field of $X^{p^n} - X$ is $\mathbb{F}_{p^n}$, and $\mathbb{F}_{p^n}$ is the unique field extension of $\mathbb{F}_p = \mathbb{Z}_p$ of degree n. If we have an irreducible polynomial $f \in \mathbb{F}_p[X]$ whose degree d divides n, then the splitting field of f must be $\mathbb{F}_{p^d}$ by uniqueness, which is contained in $\mathbb{F}_{p^n}$ by degree consideration. Therefore, f must be a factor of $X^{p^n} - X$. (1 mark)

Conversely, if we have an irreducible polynomial $f \in \mathbb{F}_p[X]$ whose degree d does not divide n, then the splitting field $\mathbb{F}_{p^d}$ is not contained in $\mathbb{F}_{p^n}$ and so f cannot be a factor of $X^{p^n} - X$. (1 mark)

It remains to show that each irreducible factor f appears in the factorization of $X^{p^n} - X$ with multiplicity one. It is almost clear because the roots of $X^{p^n} - X$ in $\mathbb{F}_{p^n}$ are all distinct. (Many of you did not check this. I did not deduct marks.)

If we do not have the monic condition as imposed, then for each irreducible polynomial f, each of the multiples $2f$, $3f$, $\ldots$, $(p-1)f$ has the same set of roots has f. Therefore, each irreducible polynomial is multi-counted by $(p-1)$ times. The correct answer for the product is then

$$(1 \cdot 2 \cdot 3 \cdots (p-1))\,(X^{p^n} - X)^{p-1} = -(X^{p^n} - X)^{p-1},$$

where the last constant is computed using the fact $(p-1)! \equiv -1 \mod p$ (Wilson's Theorem in elementary number theory). □