MA-414 (Galois Theory)
Tutorial-7

March 15, 2023

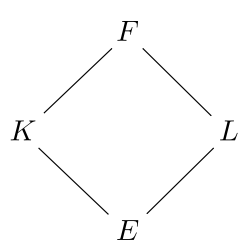
1. Let L be a finite extension of E. Suppose there is a field homomorphism $\psi : L \to L$ such that $\psi(a) = a$ for all $a \in E$. Show that ψ is surjective.

2. Let L be an algebraic extension of E (not necessarily finite). Suppose there is a field homomorphism $\psi : L \to L$ such that $\psi(a) = a$ for all $a \in E$. Show that ψ is surjective.

3. On several occasions we used the following statement. Let $i : E \subset \bar{E}$ be an embedding. Let $\psi : \bar{E} \to \bar{E}$ be a field homomorphism such that $\psi(a) = a$ for all $a \in E$. Then ψ is an isomorphism. We will show that the condition "$\psi(a) = a$ for all $a \in E$" is necessary for this to happen.

   Find a field E and a homomorphism $\sigma : E \to E$ such that E is not algebraic over $\sigma(E)$. Recall that if L/E is algebraic and K is any algebraically closed field then any homomorphism $\phi : E \to K$ can be extended to a homomorphism $L \to K$. Applying this by taking $L = K = \bar{E}$ and $\phi = i \circ \sigma$, we get a map $\psi : \bar{E} \to \bar{E}$. Show that ψ is not surjective.

4. Let

   be fields. Define

   $$KL := \{\sum_{i=1}^{m} \alpha_i \beta_i \,|\, m \geqslant 1, \alpha_i \in K, \beta_i \in L\}\,.$$

   Apriori, this is only a subring of F. Show that if K is a finite extension of E then the dimension of KL as a vector space over L is $\leqslant [K : E]$. Use this to show that KL is a field. Finally conclude that KL is the smallest subfield of F containing both K and L.

5. Let notation be as in the preceding problem. If both $[K : E]$ and $[L : E]$ are finite, show that $[KL : E] \leqslant [K : E] \cdot [L : E]$.

6. Let K/F be a finite separable extension. Show that there are only finitely many fields E such that $F \subset E \subset K$. Compare this with the last exercise in the previous tutorial sheet.

7. Show that $\mathbb{Q}[\sqrt{2}, e^{2\pi i/4}]/\mathbb{Q}$ is a Galois extension. What is $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}, e^{2\pi i/4}]/\mathbb{Q})$?

8. Let $F \subset E \subset K$ be fields such that both E and K are Galois extensions of F. Show that there is a natural map $\mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$ which is surjective. (HINT: We have used a slightly more general version of this map earlier.)

9. Consider the following statement from group theory. Let $\phi : G \to H$ be a ***surjective*** homomorphism of groups and let N be the ***kernel***. (This is often written as: Let
$$1 \to N \to G \xrightarrow{\phi} H \to 1$$
be a short exact sequence of groups.) Assume that there is a subgroup $M \subset G$ such that the restriction of ϕ to M is an isomorphism $M \xrightarrow{\sim} H$. Then every element of G can be written uniquely as nm where $n \in N$ and $m \in M$ (why?). In this case we say that G is the semi-direct product of N and M. The "semi" is because although G is a product of N and M as sets, it may not be a product as groups. Show that S_n is the semi-direct product of A_n and $\mathbb{Z}/2\mathbb{Z}$, but it is not the product of these groups.

   Continuing with the above, if further, elements of M and N commute with each other, then G is a direct product of M and N as groups. Prove this by showing that the set map (what is the map?) $N \times M \to G$ is a group homomorphism. Since it is a bijection of sets, it follows that G is the product of these two groups.

10. Let $n > 1$. Show that there is a group of size $2n$ which has the following properties

    (a) It has a cyclic subgroup H_n of size n
    (b) It has a cyclic subgroup H_2 of size 2
    (c) If r is a generator of H_n and f is a generator of H_2 then $rf = fr^{-1}$.

    Show that any two groups, of size $2n$ and having the above properties, are isomorphic.

11. In this exercise, we compute $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$.

    (a) Let $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ be such that $\sigma(a) > 0$, for all real numbers $a > 0$. Show that for any $a, b \in \mathbb{R}$ with $a < b$, we have $\sigma(a) < \sigma(b)$.
    (b) Let $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$. Then $-\frac{1}{n} < a-b < \frac{1}{n}$ implies $-\frac{1}{n} < \sigma(a)-\sigma(b) < \frac{1}{n}$. Conclude that $\sigma : \mathbb{R} \to \mathbb{R}$ is continuous.
    (c) If $f : \mathbb{R} \to \mathbb{R}$ is a continuous map with $f\big|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$, then $f = \mathrm{Id}_{\mathbb{R}}$. Conclude that $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{Id}_{\mathbb{R}}\}$.

12. Let k be a field. Let $k(t)$ be the field of fractions of the polynomial ring $k[t]$. Let $X = \frac{p(t)}{q(t)} \in k(t)$, with relatively prime polynomials $p(t), q(t) \in k[t] \setminus \{0\}$. In this exercise, we compute the degree of the field extension $k(t)/k(X)$.

(a) Show that $p(Y) - Xq(Y) \in k(X)[Y]$ is irreducible and t is root of it. (Hint: Use Gauss' lemma to conclude irreducibility.)

(b) Show that $\deg_Y(p(Y) - Xq(Y)) = \max\{\deg(p(Y)), \deg(q(Y))\}$.

(c) Show that $[k(t) : k(X)] = \big[k(t) : k\big(\frac{p(t)}{q(t)}\big)\big] = \max\{\deg(p(t)), \deg(q(t))\}$.

13. Let k be a field. Show the following.

(a) The maps $t \mapsto \frac{1}{t}$ and $t \mapsto at + b$ (for all $a, b \in k$ with $a \neq 0$) defines elements of $\mathrm{Aut}(k(t)/k)$. Hence their compositions are also in $\mathrm{Aut}(k(t)/k)$.

(b) Show that, $\mathrm{Aut}(k(t)/k) = \{t \mapsto \frac{at+b}{ct+d} : a, b, c, d \in k,\ ad - bc \neq 0\}$.

(c) Find the fixed field of the automorphism $t \mapsto t + 1$ of $k(t)$.

14. Let E/F be a field extension. Let $\varphi : E \to E'$ be an isomorphism of E with a field E' which maps F to a subfield F' of E'. Show that the map $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ defines a group homomorphism $\mathrm{Aut}(E/F) \xrightarrow{\simeq} \mathrm{Aut}(E'/F')$.

15. Let E/F be a finite Galois extension. Let H be a subgroup of $\mathrm{Gal}(E/F)$. Show that there is an element $\alpha \in E$ such that $H = \{\sigma \in \mathrm{Gal}(E/F) : \sigma(\alpha) = \alpha\}$.