Homework 5 (Due: June 14)

Problem 1 (Section 14.1, Exercise 1)**.** (1) Show that if the field K is generated over F by the elements $\alpha_1, \ldots, \alpha_n$ then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. In particular show that an automorphism fixes K if and only if it fixes a set of generators for K.

(2) Let $G \leq \mathrm{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \ldots, \sigma_k$ are generators for G. Show that the subfield E/F is fixed by G if and only if it is fixed by the generators $\sigma_1, \ldots, \sigma_k$.

Solution.

(1) (a) Let $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$ be a set of generators for K/F.
Then, any element of K can be expressed uniquely as

$$m_0 + m_1\alpha_1 + \cdots + m_n\alpha_n$$

with $m_i \in F$.
An automorphism for K which fixes F must take $m_i \mapsto m_i$ for any $m_i \in F$ (since it fixes F).
Therefore it must take,

$$m_0 + m_1\alpha_1 + \cdots + m_n\alpha_n \mapsto m_0 + m_1\sigma(\alpha_1) + \cdots + m_n\sigma(\alpha_n)$$

and the automorphism is uniquely determined by $\sigma(\alpha_1),\ \sigma(\alpha_2),\ \cdots,\ \sigma(\alpha_n)$ as claimed.

(b) So if an automorphism fixes K then $\alpha_i \mapsto \alpha_i$ by σ for any basis element α_i.
Conversely, if σ fixes a basis for K/F then σ fixes all of K.

(2) ($\Rightarrow$) If all of G fixes some subfield E/F then it is in particular fixed by generators for G $\sigma_1,\ \sigma_2, \cdots,\ \sigma_k$ as claimed.

($\Leftarrow$) If the generators $\sigma_1,\ \sigma_2,\ \cdots,\ \sigma_k$ fix all of E/F then it fixes the entire subgroup G, any member of G can be written as a combination of the generators and such combinations fix all of E/F if each does.

□

Problem 2 (Section 14.1, Exercise 5)**.** Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.

Solution.

.
The automorphisms of $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$ are completely determined by where they take $\sqrt[4]{2}$.
Since the subfield $\mathbb{Q}\left(\sqrt{2}\right)$ is fixed, it follows that

$$\left(\sqrt[4]{2}\right)^2 = \varphi\left(\left(\sqrt[4]{2}\right)^2\right) = \left(\varphi\left(\sqrt[4]{2}\right)\right)^2$$

holds in φ homomorhism. .
Therefore $\varphi\left(\sqrt[4]{2}\right) = \sqrt[4]{2}$ and $\varphi\left(\sqrt[4]{2}\right) = -\sqrt[4]{2}$ are the only automorphism of $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$.
Namely, $a + b\sqrt[4]{2} \mapsto a + b\sqrt[4]{2}$ and $a + b\sqrt[4]{2} \mapsto a - b\sqrt[4]{2}$ for $a,\ b \in \mathbb{Q}\left(\sqrt{2}\right)$

□

Problem 3 (Section 14.1, Exercise 10)**.** Let K be an extension of the field F. Let $\varphi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\mathrm{Aut}(K/F) \xrightarrow{\sim} \mathrm{Aut}\,(K'/F')$.

Solution.

Let σ and τ be arbitrary elements of $\mathrm{Aut}(K/F)$.
$\sigma \mapsto \varphi\sigma\varphi^{-1}$ is a homomorphism since $\varphi(\sigma+\tau)\varphi^{-1} = \varphi\sigma\varphi^{-1} + \varphi\tau\varphi^{-1}$ and $\varphi\sigma\tau\varphi^{-1} = \varphi\sigma\varphi^{-1}\varphi\tau\varphi^{-1}$.
And this map is injective since $\varphi\sigma\varphi^{=1} = \varphi\tau\varphi^{-1}$ implies $\varphi\sigma = \varphi\tau$, hence $\sigma = \tau$.
And this map is surjective since for every $\sigma \in \mathrm{Aut}(K'/F')$ if we set $\tau = \varphi^{-1}\sigma\varphi$, then we get $\varphi\tau\varphi^{-1} = \varphi\varphi^{-1}\sigma\varphi\varphi^{-1} = \sigma$.
Therefore the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ is an isomorphism.

□

Problem 4 (Section 14.2, Exercise 3)**.** Determine the Galois group of $(x^2-2)(x^2-3)(x^2-5)$. Determine all the subfields of the splitting field of this polynomial.

Solution.

.
We know that $F = \mathbb{Q}\left(\sqrt{2},\ \sqrt{3},\ \sqrt{5}\right)$ is the splitting field of the polynomial $(x^2-2)(x^2-3)(x^2-5)$ over $\mathbb{Q}$, an order 8 extension since 2, 3, 5 are all prime.
So the group of automorphism is generated by

$$\begin{aligned}\sigma &: \sqrt{2} \mapsto -\sqrt{2}\\ \tau &: \sqrt{3} \mapsto -\sqrt{3}\\ \varphi &: \sqrt{5} \mapsto -\sqrt{5}\end{aligned}$$

this is the entire Galois group since it is of order 8.
Therefore it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
[
(Another way)
Since $\left\{1,\ \sqrt{2},\ \sqrt{3},\ \sqrt{5},\ \sqrt{2}\sqrt{3},\ \sqrt{2}\sqrt{5},\ \sqrt{3}\sqrt{5},\ \sqrt{2}\sqrt{3}\sqrt{5}\right\} = \left\{1,\ \sqrt{2},\ \sqrt{3},\ \sqrt{5}.\ \sqrt{6},\ \sqrt{10},\ \sqrt{15}.\ \sqrt{30}\right\}$ is a $\mathbb{Q}-$basis for F,
hence $[F:\mathbb{Q}] = 8$.
Thus $|\mathrm{Gal}(F/\mathbb{Q})| = 8$ and $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
]
Since this group is abelian, every subgroup of it is normal.
Therefore by The Fundamental Theorem of Galois Theory, every normal subgroup H of $\mathrm{Gal}(F/\mathbb{Q})$ corresponds to a subfield F_H a splitting field over $\mathbb{Q}$.
Since $|H|$ divides 8, if we let $F_H := \{\alpha \in F : \sigma(\alpha) = \alpha \quad \text{for all } \sigma \in H\}$ then

(1) $|H| = 1$:
$F_H = F = \mathbb{Q}\left(\sqrt{2},\ \sqrt{3},\ \sqrt{5}\right)$
(2) $|H| = 2$:
$F_H = \mathbb{Q}\left(\sqrt{2},\ \sqrt{3}\right),\ \mathbb{Q}\left(\sqrt{2},\ \sqrt{5}\right),\ \mathbb{Q}\left(\sqrt{3},\ \sqrt{5}\right),\ \mathbb{Q}\left(\sqrt{5},\ \sqrt{6}\right),\ \mathbb{Q}\left(\sqrt{2},\ \sqrt{15}\right),\ \mathbb{Q}\left(\sqrt{3},\ \sqrt{10}\right),\ \mathbb{Q}\left(\sqrt{6},\ \sqrt{10}\right)$
(3) $|H| = 4$:
$F_H = \mathbb{Q}\left(\sqrt{2}\right),\ \mathbb{Q}\left(\sqrt{3}\right),\ \mathbb{Q}\left(\sqrt{5}\right),\ \mathbb{Q}\left(\sqrt{6}\right),\ \mathbb{Q}\left(\sqrt{10}\right),\ \mathbb{Q}\left(\sqrt{15}\right),\ \mathbb{Q}\left(\sqrt{30}\right)$
(4) $|H| = 8$:
$F_H = \mathbb{Q}$

□

Problem 5 (Section 14.2, Exercise 5)**.** Prove that the Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p, a \neq 0$.

Solution.

.
Let θ be a real p^{th} root of 2, and let ζ be a primitive p^{th} root of unity.
Then every element of the group is $\sigma_{x,y}$ where

$$\sigma_{x,y} = \begin{cases} \zeta \mapsto \zeta^x \\ \theta \mapsto \zeta^y \theta \end{cases}$$

for $0 \leq x,\ y \leq p-1$ with $x \neq 0$.
And for such $x,\ y$, define a map

$$\varphi : \sigma_{x,y} \mapsto \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix},$$

then it is bijective.
And since

$$\begin{aligned} \sigma_{x_1,y_1}\sigma_{x_2,y_2}(\zeta) &= \zeta^{x_1 x_2} \\ \sigma_{x_1,y_1}\sigma_{x_2,y_2}(\theta) &= \sigma_{x_1,y_1}(\zeta^{y_2}\theta) \\ &= \zeta^{y_1 + x_1 y_2}\theta \end{aligned}$$

holds and since

$$\begin{bmatrix} x_1 & y_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x_2 & y_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x_1 x_2 & y_1 + x_1 y_2 \\ 0 & 1 \end{bmatrix}$$

holds, φ is a homomorphism
Therefore φ is an isomorphism, hence Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ where $a,\ b \in \mathbb{F}_p$ with $a \neq 0$.

□

Problem 6 (Section 14.2, Exercise 9)**.** Give an example of fields F_1, F_2, F_3 with $\mathbb{Q} \subset F_1 \subset F_2 \subset F_3, [F_3 : \mathbb{Q}] = 8$ and each field is Galois over all its subfields with the exception that F_2 is not Galois over $\mathbb{Q}$.

Solution.

By The Fundamental Theorem of Galois Theory, to find fields

$$\mathbb{Q} \subset F_1 \subset F_2 \subset F_3$$

s.t. they are all Galois over their subfields with the exception of F_2 is equivalent to find the groups

$$G_3 \supset G_2 \supset G_1 \supset 1$$

s.t. they are all normal in a group containing them except that G_1 is not normal in G_3.
We already know that there are 5 groups of order $8(\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ D_8,\ Q_8)$ and every abelian group has subgroup normal.
If $G_3 = Q_8$, then there is only possible subgroup $G_1 = \langle -1 \rangle$ which is not normal, hence we only need to consider D_8.

Let τ be the automorphism which fixes $\sqrt[4]{2}$ and sends i to $-i$.
And non-normal subgroup of the Galois group is $\langle \tau \rangle$.
Hence if we take,

$$\begin{aligned} F_3 &= \mathbb{Q}\left(\sqrt[4]{2},\ i\right) \\ F_2 &= \mathbb{Q}\left(\sqrt[4]{2}\right) \\ F_1 &= \mathbb{Q}\left(\sqrt{2}\right) \end{aligned}$$

then subgroups will be normal, so F_i will be Galois except F_2.

□

Problem 7 (Section 14.2, Exercise 13)**.** Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.

Solution.

Suppose that the Galois group of the splitting field K of a cubic is cyclic of order 3.
Assume that the cubic has complex roots.
Let $z \in \mathbb{C}$ be a root of the cubic and
Then $\exists \tau \in Gal(K/\mathbb{Q})$ s.t. $\tau(z) = \tau(\bar{z})$.
and then $|\langle \tau \rangle| = 2$.
$\therefore 2 \mid |Gal(K/\mathbb{Q})|$ ↯ ($\because 2 \nmid 3$)

□

Problem 8 (Section 14.2, Exercise 15)**.** (Biquadratic Extensions) Let F be a field of characteristic $\neq 2$.

(1) If $K = F\left(\sqrt{D_1}, \sqrt{D_2}\right)$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2 or $D_1 D_2$ is a square in F, prove that K/F is a Galois extension with $\mathrm{Gal}(K/F)$ isomorphic to the Klein 4-group.
(2) Conversely, suppose K/F is a Galois extension with $\mathrm{Gal}(K/F)$ isomorphic to the Klein 4-group. Prove that $K = F\left(\sqrt{D_1}, \sqrt{D_2}\right)$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2 or $D_1 D_2$ is a square in F.

Solution.

Proof. (1): Since D_1 and D_2 are not square in F, $[F(\sqrt{D_1}) : F] = [F(\sqrt{D_2}) : F] = 2$. And we can say that $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = [F(\sqrt{D_1}, \sqrt{D_2}) : F(\sqrt{D_1})][F(\sqrt{D_1}) : F] \leq 4$. I want to show that we must hit the inequality. Since $[F(\sqrt{D_1}) : F] = 2$, it's enough to show $[F(\sqrt{D_1}, \sqrt{D_2}) : F(\sqrt{D_1})] \neq 1$. This situation is impossible by the assumption that D_2 and $D_1 D_2$ are not square. So $[K : F] = 4$ and K is the splitting field of $(x^2 - D_1)(x^2 - D_2)$. It is a Galois extension, and it is easy to check that $Gal(K/F) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

(2): It is the converse of the problem (1). Since the Klein 4-group is abelian, all subgroup is normal. With these two different subgroups $\mathbb{Z}_2 \times \{0\}$ and $\{0\} \times \mathbb{Z}_2$, by the fundamental theorem, we can think the correspond two extension field over F; $E_1 = F(D_1)$, $E_2 = F(D_2)$ with degree 2. It says D_1 and D_2 are not square. Since $E_1 \neq E_2$, $D_1 D_2$ is not square too. Finally, $K = F(D_1, D_2)$ since they have order 4.

□

Problem 9 (Section 14.2, Exercise 16)**.** (1) Prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.

(2) Show the roots of this quartic are

$$\alpha_1 = \sqrt{1+\sqrt{3}} \quad \alpha_3 = -\sqrt{1+\sqrt{3}}$$
$$\alpha_2 = \sqrt{1-\sqrt{3}} \quad \alpha_4 = -\sqrt{1-\sqrt{3}}.$$

(3) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$, and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.
(4) Prove that K_1, K_2 and $K_1 K_2$ are Galois over F with $\mathrm{Gal}(K_1 K_2/F)$ the Klein 4-group. Write out the elements of $\mathrm{Gal}(K_1 K_2/F)$ explicitly. Determine all the subgroups of the Galois group and give their corresponding fixed subfields of $K_1 K_2$ containing F.

(5) Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group.

Solution.

Proof. (1): By Eisenstein's criterion with $p = 2$, it is irreducible.

(2): $(\pm\sqrt{1 \pm \sqrt{3}})^2 = 1 \pm \sqrt{3}$ and so$(\pm\sqrt{1 \pm \sqrt{3}})^2 - 1 = \sqrt{3}$, we can get $[(\pm\sqrt{1 \pm \sqrt{3}})^2 - 1]^2 = 3$.

(3): Clearly, $k_1 \neq K_2$ since K_2 is subfild of $\mathbb{C}$ but K_1 is not. Since $K_1 \neq K_2$ and $K_1 \bigcap K_2$ is properly bigger than $\mathbb{Q}$ containing $\sqrt{3}$. We can say that $K_1 \bigcap K_2 = \mathbb{Q}(\sqrt{3})$.

(4): First, K_1 is a splitting field of $(x^2 - 1 - \sqrt{3}) \in F(x)$. Similarly, K_2 is a splitting field of $(x^2 - 1 + \sqrt{3}) \in F(x)$. Since these two are separable, both are Galois extension.

And K_1K_2 is the splitting(separable) field of $x^4 - 2x^2 - 2$ over F and so K_1K_2 is Galois over F. $Gal(K_1K_2/F)$, it is generated by two automorphisms, send α_1 to α_3 and send α_2 to α_4. Hence $Gal(K_1K_2/F)$ is Klein 4-group and there are nontrivial three (normal)subgroup correspond to the fixed subfields of K_1K_2 containing F.; K_1, K_2 and $F(\sqrt{-2})$.

(5): From the problems above, K_1K_2 is a separable splitting field of $\mathbb{Q}$ with polynomial $x^4 - 2x^2 - 2$ with degree 8.

So there is a automorphism in $Gal(K_1K_2/\mathbb{Q})$ that sends each $\alpha_i \mapsto \alpha_{i+1}$.$(\alpha_4 \mapsto \alpha_1)$ It only fix $\mathbb{Q}$ and does not commute with the element in problem 4. Hence $Gal(K_1K_2/\mathbb{Q})$ is a nonabelian group with order 8. It is well known fact that there are only two nonabelian group with order 8, quaternian group and dihedral group. And we can check that only the dihedral group D_8 has a subgroup of order 2 more that 3.(we have seen that (4)) So $Gal(K_1K_2/\mathbb{Q}) \cong D_8$. □

□

Problem 10 (Section 14.2, Exercise 28)**.** Let $f(x) \in F[x]$ be an irreducible separable polynomial of degree n over the field F, let L be the splitting field of $f(x)$ over F and let α be a root of $f(x)$ in L. If K is any Galois extension of F contained in L, show that the polynomial $f(x)$ splits into a product of m irreducible polynomials each of degree d over K, where $m = [F(\alpha) \cap K : F]$ and $d = [K(\alpha) : K]$ (cf. also the generalization in Exercise 4 of Section 4). [If H is the subgroup of the Galois group of L over F corresponding to K then the factors of $f(x)$ over K correspond to the orbits of H on the roots of $f(x)$. Then use Exercise 9 of Section 4.1.]

Solution.

.
Let L be a splitting field of an irreducible polynomial $f(x)$ of degree n over F.
And Let K be a Galois extension of F containing L.
Let H be a subgroup of the Galois group of L over F corresponding to K.
Let α be a root of $f(x)$.
And let $f(x) = f_1(x)f_2(x)\cdots f_m(x)$ be the factorization of $f(x)$ over K into irreducible polynomials.

If α is a root of $f_i(x)$, i.e., $f_i(\alpha) = 0$, then $\sigma(f_i(x)) = f_j(x)$ holds for some $1 \leqslant i,\ j \leqslant m$.
So we can know that the orbits of roots of $f(x)$ correspond to the irreducible factors of $f(x)$.

And we already know that H is normal in $G = \mathrm{Gal}(L/K)$ since K is Galois over F, and G acts transitively on the roots of $f(x)$ clearly.

Therefore every orbits of H have the same cardinality by Exercise 9 of section 4.1, hence every irreducible polynomials has same degree.
So by Exercise 9 of section 4.1, we get

$$\begin{aligned} m &= |G : HG_\alpha| \\ d &= |H : H \cap G_\alpha| \end{aligned}$$

And G_α is the subgroup of G which has $F(\alpha)$ as its fixed field.
Thus we get the correspondences

$$\begin{aligned} G &\longleftrightarrow F \\ H &\longleftrightarrow K \\ G_\alpha &\longleftrightarrow F(\alpha) \end{aligned}$$

And by The Fundamental Theorem of Galois Theory,

$$\begin{aligned} HG_\alpha &\longleftrightarrow K \cap F(\alpha) \\ H \cap G_\alpha &\longleftrightarrow KF(\alpha) = K(\alpha) \end{aligned}$$

Therefore,

$$\begin{aligned} m &= |G : HG_\alpha| = [K \cap F(\alpha) : F] \\ d &= |H : H \cap G_\alpha| = [K(\alpha) : K] \end{aligned}$$

□