GALOIS THEORY
Worksheet 7

Q 1. Let K be a field with $\mathrm{char}(K) \neq 3$ and such that $f(X) = X^3 - 3X + 1 \in K[X]$ is irreducible. Let $L = K(\alpha)$ where α is a root of $f(X)$. Show that f splits completely over L.

[*Hint*: Factor f over $L[X]$ as $(X - \alpha)g(X)$. Now solve for $g(X) = 0$ in L observing that $12 - 3\alpha^2 = (-4 + \alpha + 2\alpha^2)^2$.]

Q 2 (†). Suppose that $\mathrm{char}(K) \neq 2$, and let $K \subset L$ be a field extension of degree 4. Prove that the following two conditions are equivalent:

(i) There exists a (nontrivial) intermediate field $K \subset E \subset L$;

(ii) $L = K(\alpha)$ for some $\alpha \in L$ having minimal polynomial over K of the form:

$$f = X^4 + aX^2 + b \in K[X]\,.$$

Q 3. (i) Say $a, b > 1$ are distinct squarefree integers. Prove that $X^2 - a \in \mathbb{Q}[X]$ is irreducible, so $\mathbb{Q}(\sqrt{a})$ has degree 2 over $\mathbb{Q}$. Now prove that $\sqrt{b} \notin \mathbb{Q}(\sqrt{a})$.

(ii) Let F be the splitting field of $(X^2 - a)(X^2 - b)$ over $\mathbb{Q}$. What is the Galois group of the extension $\mathbb{Q} \subset F$? Use the Fundamental Theorem of Galois theory to find all the fields K with $\mathbb{Q} \subseteq K \subseteq F$. Which ones are normal over $\mathbb{Q}$?

(iii) Prove that $F = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

[*Hint*: figure out which subgroup of the Galois group this field corresponds to.]

(iv) Let p, q and r be distinct primes. Prove that $\sqrt{r} \notin \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

[*Hint*: use one of the previous parts.]

(v) Conclude that if $F = \mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$ then $[F : \mathbb{Q}] = 8$. What is the Galois group of the extension $\mathbb{Q} \subset F$?

(vi) Use the Fundamental Theorem of Galois theory to write down all the intermediate subfields between $\mathbb{Q}$ and F. If you can't then just write down the subfields E of F with $[E : \mathbb{Q}] = 2$.

(vii) Show that (notation as in the previous part) $F = \mathbb{Q}(\sqrt{p} + \sqrt{q} + \sqrt{r})$.

(viii) Prove that if p_1, p_2,...,p_n are distinct primes, then $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$ has degree 2^n over $\mathbb{Q}$, and equals $\mathbb{Q}(\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n})$.

Q 4. Let p be an odd prime number, and let F be the splitting field of $X^p - 1 \in \mathbb{Q}[X]$.

(i) What is $[F : \mathbb{Q}]$? What is the Galois group of $\mathbb{Q} \subset F$?

(ii) Prove that there is a unique subfield K of F with $[K : \mathbb{Q}] = 2$.

[*Hint*: Part (i), plus the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic].

(iii) Show that all such extensions are of the form $K = \mathbb{Q}(\sqrt{n})$ where $n \in \mathbb{Z}$ and $|n|$ is squarefree.[1]

(iv) Figure out n when $p = 3$. Figure out n when $p = 5$. [*Hint*: what is $\cos(2\pi \mathtt{i}/5)$?].

(v) What do you think the answer is in general?

(This is a number-theoretic question rather than a field-theoretic one so don't get frustrated if you see a good-looking statement but you can't prove it: there are tricks but they're tough to spot even for me.)

Q 5. In this question we'll find an explicit complex number z such that $\overline{z} \notin \mathbb{Q}(z)$ (by $\overline{z}$ I mean the complex conjugate of z.)

(a) Set $\omega = e^{\frac{2\pi \mathtt{i}}{3}}$, so $\omega^3 = 1$, and say $\alpha = 2^{1/3} \in \mathbb{R}$ the real cube root of 2. Set $z = \omega\alpha$. What is $[\mathbb{Q}(z) : \mathbb{Q}]$?

[*Hint*: minimal polynomial.]

(b) What is $[\mathbb{Q}(\omega) : \mathbb{Q}]$?

(c) Let's assume temporarily that $\overline{z} \in \mathbb{Q}(z)$. Show that this implies $\omega \in \mathbb{Q}(z)$. Why does this contradict the tower law? Deduce $\overline{z} \notin \mathbb{Q}(z)$.

(d) Let's write $z = x + iy$. Prove that none of x, i or y are in $\mathbb{Q}(z)$.

The next question is optional. In it I ask you to prove Theorem 24 of Sec. 6.1 of the GALOIS theory notes.

Q 6. The lexicographic order of monomials of $\mathbb{Z}[X_1, \dots, X_n]$ is defined as follows:

$$X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n} > X_1^{l_1} X_2^{l_2} \cdots X_n^{l_n} \quad \text{if} \quad k_1 = l_1,\ k_2 = l_2,\ \dots k_i = l_i, \text{ and } k_{i+1} > l_{i+1}$$

This is clearly a total ordering on the set of monomials. For a polynomial $f \in \mathbb{Z}[X_1, \dots, X_n]$ the order $\operatorname{ord} f$ of f is the largest monomial that appears in f.

(a) Show that for every symmetric polynomial $f \in \mathbb{Z}[X_1, \dots, X_n]$ there is a polynomial $g \in \mathbb{Z}[X_1, \dots, X_n]$ such that $\operatorname{ord} f = \operatorname{ord} g(\sigma_1, \dots, \sigma_n)$ (where $\sigma_1, \dots, \sigma_n \in \mathbb{Z}[X_1, \dots, X_n]$ are the elementary symmetric polynomials). [*Hint.* If f is symmetric then $\operatorname{ord} f = X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$ with $k_1 \geq k_2 \geq \cdots$.]

(b) Use Part (a) to conclude that for all symmetric $f \in \mathbb{Z}[X_1, \dots, X_n]$ there is $g \in \mathbb{Z}[X_1, \dots, X_n]$ such that $f = g(\sigma_1, \dots, \sigma_n)$.

[1] A natural number is squarefree if it is the product of distinct primes.

(c) (†) Now show that the ring homomorphism

$$\psi\colon \mathbb{Z}[Y_1, \dots, Y_n] \to \mathbb{Z}[X_1, \dots, X_n]^{\mathfrak{S}_n} \quad \text{defined such that for all } i\text{:} \quad \psi(Y_i) = \sigma_i$$

is an isomorphism. (You have shown in Part (b) that ψ is surjective; now you need to show that it is injective.) [*Hint*. Consider the ordering on monomials where $Y_1^{k_1} Y_2^{k_2} \cdots Y_n^{k_n} > Y_1^{l_1} Y_2^{l_2} \cdots Y_n^{l_n}$ if for all $j < i$ $k_j + \cdots k_n = l_j + \cdots + l_n$ and $k_i + \cdots k_n > l_i + \cdots + l_n$. Now let $I = \operatorname{Ker} \psi$. If $g \in I$, then, by examining what happens to $\psi(g)$, show that the largest — according to the ordering just defined — monomial that appears in g is also in I, and hence conclude that $I = (0)$.]