Assignment 10, due April 27 (before class starts).

Corrections

- **April 22** Exercises from the textbook changed.

Assigned Exercises, to hand in

1. Here is a more direct proof of Proposition 16.11.2. Suppose $\mathbb{F} \subset \mathbb{C}$ and $\zeta = e^{2\pi i/p} \in \mathbb{F}$. For any $a \in \mathbb{F}$ with $a \neq 0$, consider the polynomial $f \in \mathbb{F}[t]$ given by $f(t) = t^p - a$.

   (a) Suppose $\alpha \in \mathbb{C}$ satisfies $\alpha^p = a$ (the fundamental theorem of algebra says there is such an α). Show the following formula holds in $\mathbb{F}[\alpha]$:

   $$f(t) = \prod_{k=0}^{p-1} (t - \zeta^k \alpha) \ .$$

   Hint. Show that $f(\zeta t) = f(t)$. If $g(t)$ is the product on the right side, show that $g(\zeta t) = g(t)$. Use this figure out the coefficients $g(t) = t^p + c_{p-1}t^{p-1} + \cdots + c_0$.

   (b) Show that if f has a root in $\mathbb{F}$ then f splits in $\mathbb{F}$.

   (c) Show that if f has no root in $\mathbb{F}$, then f is irreducible in $\mathbb{F}$ and $\mathbb{F}[\alpha]$ is the splitting field of f. Do this by showing directly that $\alpha \to \omega\alpha$ generates an automorphism of $\mathbb{F}[\alpha]$ over $\mathbb{F}$, if $\omega^p = 1$. Consider two general elements of $\mathbb{F}[\alpha]$,

   $$x = \sum_{j=0}^{p-1} \xi_j \alpha^j \ , \quad y = \sum_{k=0}^{p-1} \eta_k \alpha^k$$

   Find expressions for $\sigma(x)$ and $\sigma(y)$ if $\sigma(\alpha) = \omega\alpha$ and verify by direct calculation that $\sigma(xy) = \sigma(x)\sigma(y)$. Explain how this shows the Galois group $G(\mathbb{F}[\alpha]/\mathbb{F})$ is transitive on the roots $\zeta^k\alpha$ and how this implies that f is irreducible.

2. This exercise explores the Galois group of the polynomial $f(t) = t^p - a$ over $\mathbb{Q}$. It reviews the basic aspects of Galois theory by verifying them in a specific example. [Take care in your writeup that τ, the Greek letter "tau", does not look like t or r.] Take $p > 2$ to be prime and $a \in \mathbb{Q}$ that does not have a rational p^{th} root. The relevant fields are the ground field $\mathbb{Q}$, the cyclotomic extension $\mathbb{F} = \mathbb{Q}[\zeta]$ (with $\zeta = e^{2\pi i/p} \in \mathbb{C}$), $\mathbb{L} = \mathbb{Q}[\alpha]$, where $\alpha \in \mathbb{C}$ satisfies $\alpha^p = a$, and $\mathbb{K}$, which is the splitting field of f. Take

r to be a generator of $\mathbb{F}_p^*$ and $s = r^{-1}$ in $\mathbb{F}_p$. You may "abuse notation" by considering r and s to be integers with $rs \equiv 1$ and $r^{p-1} = 1 \bmod p$, etc. Any $x \in \mathbb{K} = \mathbb{Q}[\zeta, \alpha]$ may be written as

$$x = \sum_{i=0}^{p-2} \sum_{j=0}^{p-1} \xi_{ij} \zeta^i \alpha^j \ , \quad \text{simplified to } x = \sum \xi_{ij} \zeta^i \alpha^j \ . \tag{1}$$ $\boxed{\texttt{x}}$

The Galois group $G = \mathit{Gal}(\mathbb{K}/\mathbb{Q})$ is generated by elements $\sigma \colon \alpha \to \zeta\alpha$ and $\tau \colon \zeta \to \zeta^r$. More explicitly, these are given by

$$\begin{aligned} \sigma(x) &= \sum \xi_{ij} \zeta^i \left(\zeta\alpha\right)^j = \sum \xi_{ij} \zeta^{i+j} \alpha^j \\ \tau(x) &= \sum \xi_{ij} \left(\zeta^i\right)^r \alpha^j = \sum \xi_{ij} \zeta^{ir} \alpha^j \end{aligned}$$

(a) Show that $\mathbb{K}$ consists of elements of the form ($\overset{\texttt{x}}{\text{I}}$). Show that the collection of all elements of the form ($\overset{\texttt{x}}{\text{I}}$), with rational coefficients ξ_{ij}, form the splitting field of f. Use ($\overset{\texttt{x}}{\text{I}}$) to determine $[\mathbb{K} : \mathbb{Q}]$.

(b) What is the fixed field of $\langle\tau\rangle \subset G$ ($\mathbb{F}$ or $\mathbb{L}$)? Here, $\langle\tau\rangle$ is the subgroup generated by τ. Is it supposed to be true (why or why not) and is it true that

$$|\langle\tau\rangle| \ [\mathbb{K}^{\langle\tau\rangle} \colon \mathbb{Q}] = [\mathbb{K} \colon \mathbb{Q}] \ ?$$

(c) How many roots does f have in $\mathbb{K}^{\langle\tau\rangle}$? Use the answer to determine whether $\langle\tau\rangle \subset G$ is a normal subgroup.

(d) Identify the fixed field $\mathbb{K}^{\langle\sigma\rangle}$.

(e) Show that $\langle\sigma\rangle \subset G$ is normal by finding an irreducible $g \in \mathbb{Q}[t]$ that splits in $\mathbb{K}^{\langle\sigma\rangle}$.

(f) Verify that $\langle\sigma\rangle \subset G$ is normal by calculating the *action* of τ on σ. Since $\tau\sigma\tau^{-1} \in \langle\sigma\rangle$, this means finding m so that $\tau\sigma\tau^{-1} = \sigma^m$. *Hint.* τ^{-1} involves $\zeta \to \zeta^s$ (why?).

(g) Since $H = \langle\tau\rangle$ is not normal, there are conjugate subgroups $\widetilde{H} = gHg^{-1} \neq H$ for various $g \in G$. The Galois correspondence theorem implies that the fixed fields $\mathbb{K}^{\widetilde{H}}$ are also distinct. Find a one to one correspondence between these fixed fields and the roots of f in $\mathbb{K}$.

3. Exercise 7.2 Chapter 16.

4. Exercise 7.6 Chapter 16.

5. Exercise 8.3 Chapter 16.

6. Exercise 10.2 Chapter 16.

7. Exercise 12.2 Chapter 16.