MATH 81/111: RINGS AND FIELDS
FINAL EXAM

Problem 1. Let \( f(X) = (X^4 - 3)(X^2 - 2) \).

(a) Exhibit a splitting field for \( f \).

(b) Give a presentation (in terms of generators and relations) for the Galois group \( \text{Gal}(f) \) and an embedding of \( \text{Gal}(f) \hookrightarrow S_6 \).

Solution. For (a), we have the splitting field
\[
K = \mathbb{Q}(\pm \sqrt{3}, \pm i \sqrt{3}, \sqrt{2}) = \mathbb{Q}(\sqrt{3}, i, \sqrt{2}).
\]

For (b), since \( f \) is reducible, we have \( \text{Gal}(f) \leq S_4 \times S_2 \rightarrow S_6 \). We have generators
\[
\begin{align*}
\sigma : K \rightarrow K & \\
\sqrt{3} & \mapsto i \sqrt{3} \\
i & \mapsto i \\
\sqrt{2} & \mapsto \sqrt{2}
\end{align*}
\]
\[
\begin{align*}
\tau : K \rightarrow K & \\
\sqrt{3} & \mapsto \sqrt{3} \\
i & \mapsto -i \\
\sqrt{2} & \mapsto -\sqrt{2}
\end{align*}
\]
\[
\mu : K \rightarrow K \\
\sqrt{3} & \mapsto \sqrt{3} \\
\sqrt{2} & \mapsto -\sqrt{2}
\]

We have \( \sigma^4 = \tau^2 = \mu^2 = \text{id} \). Because of the direct product, we have commutation relations \( \sigma \mu = \mu \sigma \) and \( \sigma \tau = \tau \sigma \). Finally, we compute that \( \tau \sigma(\sqrt{3}) = -i \sqrt{3} = \sigma^{-1} \tau(\sqrt{3}) \) and \( \sigma \tau(\alpha) = \sigma^{-1}(\alpha) \) for \( \alpha = i, \sqrt{2} \). This gives a presentation
\[
\text{Gal}(f) \cong \langle \sigma, \tau, \mu \mid \sigma^4 = \tau^2 = \text{id}, \tau \sigma = \sigma^{-1} \tau, \mu^2 = \text{id}, \sigma \mu = \mu \sigma, \tau \mu = \mu \tau \rangle \cong D_8 \times \mathbb{Z}/2\mathbb{Z}.
\]

If we label the roots \( \sqrt{3}, i \sqrt{3}, -\sqrt{3}, -i \sqrt{3}, \sqrt{2}, -\sqrt{2} \) in order, then we have a permutation representation
\[
\begin{align*}
\text{Gal}(f) & \rightarrow S_6 \\
\sigma & \mapsto (1 \ 2 \ 3 \ 4) \\
\tau & \mapsto (1 \ 3)(2 \ 4) \\
\mu & \mapsto (5 \ 6)
\end{align*}
\]

Problem 2. Let \( K/F \) be a finite Galois extension with Galois group \( G = \text{Gal}(K/F) \), and let \( L/F \) be a finite extension of degree \( m \) with \( \text{gcd}(m, \#G) = 1 \). Show that \( KL/L \) is Galois with \( \text{Gal}(KL/L) \cong G \).

Solution. From class, we know that \( KL/L \) is Galois with Galois group \( \text{Gal}(KL/L) \cong \text{Gal}(K/(K \cap L)) \leq G \). But \( K \cap L \subseteq K, L \) has degree \( [K \cap L : F] = m = [L : F] \) and \( [K \cap L : F] = [K : F] = n = \#G \), since \( K/F \) is Galois. Since \( \text{gcd}(m, n) = 1 \), we must have \( K \cap L = F \), so \( \text{Gal}(KL/L) \cong \text{Gal}(K/F) = G \).

Problem 3. Let \( F \) be a field. We say that \( \beta \in F \) can be written as a sum of squares in \( F \) if there exist \( \alpha_1, \ldots, \alpha_n \in F \) such that
\[
\alpha_1^2 + \cdots + \alpha_n^2 = \beta.
\]

Let \( F \) be a finite extension of \( \mathbb{Q} \) of odd degree. Show that \(-1\) is not a sum of squares in \( F \).

Solution. By the primitive element theorem, we can write \( F = \mathbb{Q}(\alpha) \) with the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \) of odd degree \( d \geq 1 \). Any polynomial of odd degree has a real root, so by the almighty Proposition 2.2, we may embed \( \sigma : F \hookrightarrow \mathbb{R} \). Now suppose that \( \sum_{i=1}^{n} \alpha_i^2 = -1 \) in \( F \). By properties of homomorphisms, we have in \( \mathbb{R} \) the equality
\[
\sum_{i=1}^{n} \sigma(\alpha_i)^2 = \sigma(-1) = -1;
\]

Date: 13 March 2015.
this is a contradiction, as the quantity on the left is nonnegative whereas the quantity on the right is negative.

**Problem 4.**

(a) Let $G$ be a group, let $H \leq G$ be a subgroup, and let

$$N = \bigcap_{g \in G} gHg^{-1}.$$  

Show that $N \leq G$ is the largest normal subgroup of $G$ contained in $H$.

(b) Let $K/F$ be a Galois extension with Galois group $G = \text{Gal}(K/F)$. Let $F \subseteq M \subseteq K$ be an intermediate extension, corresponding to $H \leq G$. Let $N$ be as in (a). Show that the fixed field of $N$ is the Galois closure of $M$ in $K$, i.e., the smallest extension of $M$ that is Galois over $F$.

**Solution.** First (a). $N$ is normal, for $x \in G$ we have

$$xNx^{-1} = \bigcap_{g \in G} xgx^{-1}g^{-1} = \bigcap_{g \in G} (xg)H(xg)^{-1} = \bigcap_{g \in G} gHg^{-1} = N$$

because the map $g \mapsto xg$ is a permutation of $G$. If $P \leq G$ is a normal subgroup of $G$ with $P \leq H$, then $P = gPg^{-1} \leq gHg^{-1}$ for all $g \in G$ so $K \leq \bigcap_{g \in G} gHg^{-1} = N$.

Now (b); we use the fundamental theorem of Galois theory. First, because $H \geq N$ by inclusion-reversing we have $K^H = M \subseteq K^N$. Next, because $N$ is normal, we have $K^N/F$ Galois. Now suppose that

$$K \supseteq M' \supseteq M \supseteq F$$

and $M'$ is Galois over $F$; then by FTGT $M'$ corresponds to a normal subgroup $H' \leq G$ contained in $H$; by (a), we have $H' \leq N$, so again by inclusion-reversing $M' \subseteq K^N$.

**Problem 5.** Show that a regular 9-gon is not constructible by straightedge and compass.

**Solution.** We showed in class that an $n$-gon is constructible if and only if $\cos(2\pi/n)$ is constructible. So we consider

$$\cos(2\pi/9) = \frac{1}{2} (\zeta_9 + \zeta_9^{-1})$$

where $\zeta_9 = \exp(2\pi i/9)$. The field $K = \mathbb{Q}(\zeta_9)$ has $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$ (it has order 6 and is abelian). Let $K^+ \subseteq K$ be the subfield of $K$ fixed under complex conjugation, the unique element of order 2 in $\text{Gal}(K/\mathbb{Q})$, corresponding to $-1 \in (\mathbb{Z}/9\mathbb{Z})^\times$. Then $[K^+ : \mathbb{Q}] = 6/2 = 3$, and $\cos(2\pi/9) \in K^+$. The conjugates $\zeta_9^2 + \zeta_9^{-2} = \cos(4\pi/9)$ and $\zeta_9^4 + \zeta_9^{-4} = \cos(8\pi/9)$ of $\cos(2\pi/9)$ are all distinct (look at the graph), so $\cos(2\pi/9)$ generates $K^+$ and thus has minimal polynomial of degree 3. (Or just assert that $\cos(2\pi/9) \notin \mathbb{Q}$. Or compute the minimal polynomial for $\cos(2\pi/9)$ using the triple angle formula.) But then $\cos(2\pi/9)$ is not constructible, as its minimal polynomial does not have degree a power of 2.

**Problem 6.**

(a) Give an explicit construction of $\mathbb{F}_4$.

(b) Is the polynomial $f(X) = X^4 + X + T$ separable over $\mathbb{F}_4(T)$?

(c) The polynomial $f(X) = X^4 + X + T$ is irreducible over $\mathbb{F}_4(T)$. Compute the Galois group of $f$ over $\mathbb{F}_4(T)$.

**Solution.** For (a), we take $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.

For (b), the answer is yes: $f$ is not a polynomial in $X^2$. Or $f'(X) = 1$ so $\gcd(f, f') = 1$.

For part (c), we are supposed to think of the homework problem where we considered $X^p - X + a$. Let $K$ be a splitting field of $f$ and let $\alpha$ be a root. Then we claim that $\alpha + c$ is also a root of $f$ for all $c \in \mathbb{F}_4$: we have

$$f(\alpha + c) = (\alpha + c)^4 + (\alpha + c) + T = \alpha^4 + c^4 + \alpha + c + T = 0$$

since $c^4 = c$ for all $c \in \mathbb{F}_4$. Therefore $K = \mathbb{F}_4(T)(\alpha)$ has $[K : F] = 4$, and the elements of the Galois group are $\sigma(\alpha) = \alpha + c$ with $c \in \mathbb{F}_4$ each of which has order 2, so $K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In fact, we have an isomorphism

$$\text{Gal}(K/\mathbb{F}_4(T)) \to \mathbb{F}_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\sigma \mapsto \sigma(\alpha) + \alpha = c.$$
Problem 7. Let $p$ be prime and let $F$ be a field in which $X^p - 1$ splits into distinct linear factors. Let $a \in F^\times \setminus F^{\times p}$, and let $K = F(\sqrt[p]{a}) = F[X]/(X^p - a)$. Show that the polynomial $X^p - b \in F[X]$ splits in $K$ if and only if $b = a^j c^p$ for some $c \in F^\times$ and $j \in \{0, \ldots, p - 1\}$.

Solution. By hypothesis, there exists a primitive $p$th root of unity $\zeta \in F$. By Kummer theory, we have $\text{Gal}(K/F) = \langle \sigma \rangle \cong \mathbb{Z}/p\mathbb{Z}$ where $\sigma(\alpha) = \zeta \alpha$.

The direction $(\Leftarrow)$ is clear, as the roots of $X^p - b$ are $\zeta^i \beta$ for $i = 1, \ldots, n$, where $\beta = c \alpha^r$.

So we prove $(\Rightarrow)$. Suppose that $X^p - b$ splits in $K$, and let

$$\beta = c_0 + c_1 \alpha + \cdots + c_{n-1} \alpha^{n-1} \in K$$

be a root, with $c_i \in F$. Then the other roots of $X^p - b$ are $\zeta^j \beta$ with $j = 0, \ldots, n - 1$, so $\sigma(\beta) = \zeta^j \beta$ for some $j$. But

$$\sigma(\beta) = c_0 + c_1 \zeta \alpha + \cdots + c_{n-1} \zeta^{n-1} \alpha^{n-1} = c_0 \zeta^j + c_1 \zeta^j \alpha + \cdots + \zeta^j \alpha^{n-1}.$$

But $1, \ldots, \alpha^{n-1}$ are a basis for $K$ as an $F$-vector space, so we have $c_i \zeta^i = c_i \zeta^j$ which implies $c_i = 0$ for $i \neq j$; thus $\beta = c_j \alpha^j$ whence $b = \beta^p = c_j^p a^j$ as claimed.