# PROBLEM SET 11: DUE WEDNESDAY, APRIL 15

**Problem 11.1.** Let $\theta_1, \theta_2, \ldots, \theta_n$ be algebraic numbers such that $[\mathbb{Q}(\theta_j) : \mathbb{Q}] \leq 5$ for all $j$. Let $\phi$ be an algebraic number with minimal polynomial $f$ over $\mathbb{Q}$; let $L$ be the splitting field of $f$ over $\mathbb{Q}$ and suppose that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_6$. Show that $\phi \notin \mathbb{Q}(\theta_1, \ldots, \theta_n)$.

**Problem 11.2.** Let $p$ be an odd prime. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree $p$, let $L$ be the splitting field of $f$ and suppose that $\mathrm{Gal}(L/\mathbb{Q})$ is the dihedral group of order $2p$, embedded in $S_p$ in the usual way. Show that $f$ has either 1 real root or else $p$ real roots.

**Problem 11.3.** Let $F/K$ be a separable extension of finite degree and let $L$ be the Galois closure of $F$. Let $G = \mathrm{Gal}(L/K)$ and let $H = \mathrm{Stab}(F)$. Let $\theta \in F$. Show that $T_{F/K}(\theta) = \sum_{g \in G/H} g(\theta)$ and $N_{F/K}(\theta) = \prod_{g \in G/H} g(\theta)$. Here we sum over cosets of $G/H$, choosing one element from each coset, and $N$ and $T$ are the norm and trace.

**Problem 11.4.** (**Implicit Differentiation**) Let $k$ be a field, let $d : k \to k$ be a derivation (see Problem 10.7) and let $f(y) = \sum_j f_j y^j$ be an irreducible polynomial in $k[y]$. Define $\frac{\partial f}{\partial y} = \sum j f_j y^{j-1}$ and assume that $\frac{\partial f}{\partial y} \neq 0$. Let $K$ be the field $k[y]/f(y)k[y]$.

(1) Show that there is precisely one derivation $D : K \to K$ which restricts to $d$ on $k$. (Problem 10.7 was meant to be useful, but I accidentally made its conclusion too weak. You may pretend you proved the following instead: Let $k$ be a field, let $M$ be a $k[y]$-module and let $d : k \to M$ be a derivation. Let $a \in M$. Then there is a unique derivation $D : k[y] \to M$ which restricts to $d$ on $k$ and has $D(y) = a$.)

(2) (**Problem 8, Math 115 Exam 2, Fall 2017**) To check that you understand what you just did, we do a special case: Let $k = \mathbb{R}(x)$, the field of rational functions in $x$. Let $d$ be the derivation $\frac{d}{dx} : k \to k$. Let $K = k[y]/((y^2 + x^2)^2 + 2xy^2 - 81)k[y]$. Compute $D(y)$ for the unique $D$ extending $d$.

**Problem 11.5.** This problem provides a Galois theory proof of the fundamental theorem of algebra. Thus, you may not assume in this question that $\mathbb{C}$ is algebraically closed. Suppose, for the sake of contradiction, that there is a polynomial $f(x) \in \mathbb{C}[x]$ which does not have a root in $\mathbb{C}$.

(1) Under the assumption that there is such a polynomial, show that there is a finite degree field extension $\mathbb{R} \subset \mathbb{C} \subsetneq K$ with $K/\mathbb{R}$ Galois.

Let $G = \mathrm{Gal}(K/\mathbb{R})$ and let $\#(G) = 2^k m$ with $m$ odd.

(2) Show that there is a field $F$ with $\mathbb{R} \subseteq F \subseteq K$ such that $[F : \mathbb{R}] = m$.

(3) Show that $m = 1$. You may assume that any odd degree polynomial in $\mathbb{R}[x]$ has a root in $\mathbb{R}$. [1]

You have now shown that $G$ is a 2-group.

(4) Show that there is a field $F'$ with $\mathbb{C} \subseteq F' \subseteq K$ with $[F' : \mathbb{C}] = 2$ and derive a contradiction. You may assume that every element of $\mathbb{C}$ has a square root. [2]

**Problem 11.6.** Let $\zeta$ be a primitive $n$-th root of unity and let $L = \mathbb{Q}(\zeta)$. In problem 8.1, you showed that $\mathrm{Gal}(L/\mathbb{Q})$ was a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, with $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting by $\zeta \mapsto \zeta^a$. Let this subgroup be $A$. In this problem, we will show that $A = (\mathbb{Z}/n\mathbb{Z})^\times$. For each $u \in (\mathbb{Z}/n\mathbb{Z})^\times$, put $f_u(z) = \prod_{a \in A}(z - \zeta^{au})$.

(1) Show that all the $f_u(z)$ have integer coefficients.

In the next parts, let $p$ be a prime not dividing $n$.

(2) Let $u$ and $v$ lie in different cosets of $(\mathbb{Z}/n\mathbb{Z})^\times/A$. Show that $f_u(z)$ and $f_v(z)$ are relatively prime in $\mathbb{F}_p[z]$.
(3) Show that $f_u(z) \equiv f_{pu}(z) \mod p\mathbb{Z}[x]$.
(4) Show that the class of $p$ modulo $n$ lies in $A$.

You have now shown that every prime not dividing $n$ lies in $A$ modulo $n$.

(5) Show that $A = (\mathbb{Z}/n\mathbb{Z})^\times$. (This is much easier than Dirichlet's theorem on primes in an arithmetic progression, so please don't use that.)

---

[1] Proof: Use the intermediate value theorem.

[2] Proof: For two of the four sign choices, we have $\sqrt{a + b\,i} = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} \pm \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\; i$.