Math 121. Homework 3

An *automorphism* of a field is a isomorphism from the field to itself. For example, complex conjugation is a non-trivial automorphism of $\mathbf{C}$. By using the notion of "transcendence basis" that we'll discuss at the end of the course, it can be shown that $\mathbf{C}$ has uncountably many other non-trivial automorphisms (though none of these others is *continuous* with respect to the usual topology on $\mathbf{C}$, and none of them fix the subfield $\mathbf{R}$ — that is, there exist zillions of embeddings of $\mathbf{R}$ into $\mathbf{C}$ as an abstract subfield!). Galois theory arises from the problem of studying certain types of automorphisms of fields. The first three exercises are concerned with some basic examples.

1. (i) For a field k, show that the set $\mathrm{Aut}(k)$ of automorphisms of k forms a group under composition.

(ii) If $f \in \mathbf{Z}[X]$ and $a \in k$ satisfies $f(a) = 0$, then show that for any $\sigma \in \mathrm{Aut}(k)$, $f(\sigma(a)) = 0$. If L is an extension of k and $\sigma \in \mathrm{Aut}(L)$ acts trivially on k (i.e., $\sigma(x) = x$ for all $x \in k \subseteq L$), then for any $h \in k[X]$ and $a \in L$ satisfying $h(a) = 0$, prove that $h(\sigma(a)) = 0$.

2. Prove that $\mathrm{Aut}(\mathbf{Q})$ and $\mathrm{Aut}(\mathbf{F}_p)$ are trivial. Also, show that $\mathrm{Aut}(\mathbf{R})$ is trivial. For this latter one, do *not* make any a priori continuity assumptions, but you may use the fact from basic analysis that every positive real number has a square root in $\mathbf{R}$.

3. Prove that $\mathrm{Aut}(\mathbf{Q}(\sqrt{2}))$ is cyclic of order 2 and $\mathrm{Aut}(\mathbf{Q}(2^{1/3}))$ is trivial, where $2^{1/3}$ denotes the unique solution to $X^3 = 2$ in $\mathbf{R}$ (or you can think of this as the abstract field $\mathbf{Q}[X]/(X^3 - 2)$).

4. Let $f(X) = X^4 - 2X^2 + 9 \in \mathbf{Q}[X]$, and $g(Y) = Y^2 - 2Y + 9$, so $f(X) = g(X^2)$.

(i) Show that f has splitting field $K = \mathbf{Q}(u, v)$ with $u^2 = 2$ and $v^2 = -1$, where the roots of f in K are $\pm r, \pm s$ with $r = u + v$ and $s = u - v$.

(ii) By considering possible monic factorizations, use (i) to show that f is irreducible over $\mathbf{Q}$.

(iii) For all $c \in \mathbf{Z}$, show $f(X + c)$ is not Eisenstein with respect to any prime p (i.e., f has no "Eisenstein translate"). In other words, Eisenstein's criteria can't always be used to prove irreducibility.

5. Let $A = \mathbf{Z}[\sqrt{5}]$ and let $K = \mathbf{Q}(\sqrt{5})$ be the fraction field of A.

(i) Show that $X^2 - X - 1$ is irreducible in $A[X]$ but is reducible in $K[X]$. Deduce that A cannot be a UFD.

(ii) (Extra credit) For $x = a + b\sqrt{5}$ with $a, b \in \mathbf{Q}$, define $\overline{x} = a - b\sqrt{5}$. Show that $x \mapsto \overline{x}$ is multiplicative and that the multiplicative "norm" $N : K \to \mathbf{Q}$ defined by $x \mapsto x\overline{x} = a^2 - 5b^2$ carries A into $\mathbf{Z}$. Using this, prove that 2 and $\sqrt{5} \pm 1$ are irreducible in A. Deduce that $4 \in A$ admits two irreducible factorizations *not* related through $A^\times$-multiplication, thereby exhibiting failure of the UFD property for A explicitly.

6. Factor all eight (monic) cubic polynomials in $\mathbf{F}_2[X]$ into a product of (monic) irreducibles.

7. Let p be a prime. Choose $a \in \mathbf{F}_p$ and consider $f_a(t) = t^p - t - a \in \mathbf{F}_p[t]$.

(*i*) If $a = 0$, show that $f_a = \prod_{r \in \mathbf{F}_p}(t - r)$.

(*ii*) Suppose $a \neq 0$ and let $k/\mathbf{F}_p$ be a splitting field of f_a (so k really depends on a too). If r_1 and r_2 are two roots of f_a in k, prove $r_1 - r_2 \in \mathbf{F}_p$.

(*iii*) Suppose $a \neq 0$. Using (ii), show that f_a is irreducible in $\mathbf{F}_p[t]$. (Hint: consider how a monic factor of f_a appears in $k[t]$.)

(*iv*) Show that $t^p - t - 4 \in \mathbf{Q}[X]$ is irreducible for all primes p.

(we'll see later that a splitting field of f_{a_0} for any single $a_0 \in \mathbf{F}_p^\times$ is also a splitting field for f_a for all $a \in \mathbf{F}_p^\times$, so k is sort of "independent" of $a \in \mathbf{F}_p^\times$).

8. Find the cubic minimal polynomial over $\mathbf{Q}$ for $a = 2\cos(2\pi/7)$. (Note $a = \zeta + 1/\zeta$ for $\zeta := e^{2\pi i/7}$.)