SOLUTIONS TO HOMEWORK 7

1. For a field k, show that the set $\mathrm{Aut}(k)$ of automorphisms of k forms of group under composition. 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 $f \in k[X]$ and $a \in L$ satisfying $f(a) = 0$, prove that $f(\sigma(a)) = 0$.

The first part is straightfoward. As for the other parts, if $f = \sum c_i X^i$ and $\sigma(c_i) = c_i$, then for all $a \in L$,

$$f(\sigma(a)) = \sum c_i \sigma(a)^i = \sum \sigma(c_i)\sigma(a^i) = \sigma(f(a)).$$

Thus, $f(\sigma(a)) = \sigma(0) = 0$ when $f(a) = 0$.

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 $\mathbf{R}$.

The first two follow from Homework 1, Exercise 8(*ii*). As for $\mathrm{Aut}(\mathbf{R})$, note that any automorphism fixes the subfield $\mathbf{Q}$ (by Homework 1, Exercise 8(*ii*) again!). Since each real number is uniquely determined by the set of rationals greater than it, essentially by the definition of $\mathbf{R}$ (or its construction, depending on your point of view), it suffices to prove an automorphism of $\mathbf{R}$ must be order-preserving. So for $\sigma : \mathbf{R} \simeq \mathbf{R}$ an automorphism, we need to show that $\sigma(x) > 0$ if $x > 0$. But the positive elements of $\mathbf{R}$ are exactly the non-zero squares, from which we deduce the result.

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 $\mathbf{Q}[X]/(X^3 - 2)$).

It is clear that an automorphism of $k(a)$ which fixes k is completely determined by where a goes. By Exercise 1, an automorphism of $\mathbf{Q}(\sqrt{2})$ must send $\sqrt{2}$ to another solution to $X^2 = 2$ in the field. There are two such solutions (since $\sqrt{2}$ and $-\sqrt{2}$ work and a degree d equation over a field has at most d solutions in the field). Thus, there are at most two automorphisms. We verify by hand that the set-theoretic map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is a ring map and so is a field automorphism. Thus, $\mathrm{Aut}(\mathbf{Q}(\sqrt{2}))$ is a group of order 2.

We now check that $\mathbf{Q}[X]/(X^3 - 2)$ contains a *unique* solution to $T^3 = 2$. You can do this 'by hand', but here is a more enlightening approach: say u and v are two such solutions, so both are non-zero. Then u/v is a cube root of unity. The field admits an embedding into $\mathbf{R}$, which has no non-trivial cube roots of unity. Thus, $u/v = 1$.

4. Show that $f(X) = X^4 - 2X^2 + 9 \in \mathbf{Q}[X]$ is irreducible, but for all $c \in \mathbf{Z}$, $f(X + c)$ is not Eisenstein with respect to any prime p (i.e., f has no 'Eisenstein translates'). In other words, Eisenstein's criteria can't always be used to prove irreducibility.

First note that if f is reducible, it must factor into a product of two monic quadratics over $\mathbf{Q}$ (even over $\mathbf{Z}$), and these are given by standard formulas (i.e., symmetric functions of roots) in terms of the roots of f in a splitting field. So the first thing to do is to describe a splitting field K of f over $\mathbf{Q}$. Let $r, -r, s, -s$ be the roots of f in K. We claim that the four roots are of the form $u + v$, $u - v$, $-u - v$, $-u + v$ with $u^2 = 2$, $v^2 = -1$ (i.e., K is a splitting field of $(X^2 - 2)(X^2 + 1)$). To see this, note that r^2 is a root of $Y^2 - 2Y + 9$, so by the quadratic formula, K contains an element a with $a^2 = -2$ and $r^2 = 1 + 2a$. Since $s^2 \neq r^2$, we must have $s^2 = 1 - 2a$. Thus, $(r + s)^2 = 2 + 2rs$. Since $(rs)^2 = 9$ (by considering the constant term of f), $rs = 3$ or $rs = -3$. Interchanging the roles of s and $-s$ if necessary, say $rs = -3$, so $v = (r + s)/2$ satisfies $v^2 = -1$. Then $u = a/v$ satisfies $u^2 = 2$, and one now checks that not only does K contain $\mathbf{Q}(u, v)$, but the roots of f can be expressed in terms of u and v as asserted above, so $K = \mathbf{Q}(u, v)$.

Now check that no product of any two of the linear factors of f over K lie in $\mathbf{Q}[X]$. This proves irreducibility. The other part is checked by considering cases (and a bit of brute force).

5. Let $A = \mathbf{Z}[\sqrt{5}]$ and let $K = \mathbf{Q}(\sqrt{5})$ be the fraction field of A. Show that $X^2 - X - 1$ is irreducible in $A[X]$ but is reducible in $K[X]$. Why doesn't the proof of Gauss' Lemma apply here?

Gauss' Lemma applies to UFDs. It turns out that A is not a UFD (as the above example shows must be the case!). Any non-trivial factorization over $A[X]$, which involves monics without loss of generality (check!), would give rise to a monic factorization in $K[X]$. Thus, it is necessary and sufficient to check that $X^2 - X - 1$ factors into a product of linear monics in $K[X]$ which do not lie in $A[X]$. Use the quadratic formula.

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

Have fun. Cubics are irreducible iff they have no root.

7. 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, what can you say about $r_1 - r_2$?
(*iii*) Suppose $a \neq 0$. Show that f_a is irreducible in $\mathbf{F}_p[t]$.
(*iv*) Show that $t^p - t - 4 \in \mathbf{Q}[X]$ is irreducible for all primes p.

(*i*) Since $f(r) = 0$ for all $r \in \mathbf{F}_p$, certainly $\prod(t - r)$ divides f_0. Comparing degrees and leading coefficients, they are equal.

(*ii*) Let $d = r_1 - r_2$. Then $d^p - d = f_a(r_1) - f_a(r_2) = 0$ (since $(-1)^p = -1$ in characteristic p, including $p = 2$). By (*i*), we see that $d \in \mathbf{F}_p$. Thus, if r is a single root of f_a in k, then $\{r + d \,|\, d \in \mathbf{F}_p\}$ is a full set of p roots of f_a, all in k.

(*iii*) Suppose $f_a = gh$ with $g, h \in \mathbf{F}_p[t]$ monic, and g has degree δ with $0 \leq \delta \leq p$. The roots of g (in a splitting field of f_a) have the form $r + d$ for various $d \in \mathbf{F}_p$, with r a root of f_a in some splitting field. Note that $r \notin \mathbf{F}_p$, by (*i*). Thus, the second-highest term in g has coefficient of the form $\delta r + x$ with $x \in \mathbf{F}_p$. But this coefficient lives in $\mathbf{F}_p$, so $\delta r \in k$ actually lives in $\mathbf{F}_p$. Since $r \notin \mathbf{F}_p$, we must have $\delta = 0$ in k, so $\delta = p$ or $\delta = 0$. This proves the factorization of f_a had to be trivial.

(*iv*) Check $p = 2$ by the quadratic formula. Otherwise note this is irreducible mod p by (*iii*), so is irreducible in $\mathbf{Z}[X]$. By Gauss' Lemma, we have irreducibility in $\mathbf{Q}[X]$.

8. Clearly $a = e^{2\pi i/7}$ is a root of $X^7 - 1 = (X - 1)f$, where

$$f = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

was shown to be irreducible over $\mathbf{Q}$ in the previous exercise. Since $a \neq 1$, f is the minimal polynomial of a over $\mathbf{Q}$. Since $b = 2\cos(2\pi/7) = a + a^{-1}$, we see that $b^2 = a^2 + 2 + a^{-2}$ and $b^3 = a^3 + 3(a + a^{-1}) + a^{-3}$. Using $a^7 = 1$, we see that $b^3 - 3b + b^2 - 1 + b = f(a) = 0$, so b is a root of $g = X^3 + X^2 - 2X - 1$. We need to show g is irreducible over $\mathbf{Q}$. Use the rational root theorem.