HOMEWORK 11, DUE THU APR 22ND

All solutions should be with proofs, you may quote from the book or from previous home works

(1) Find the degrees of the splitting fields over $\mathbb{Q}$ for the following polynomials.

(a) $X^4 + 1$.

Solution. Let $u = e^{\pi/4}$. Then, the 4 roots of the polynomial are u, u^3, u^5, u^7 and so the splitting field is just $\mathbb{Q}(u)$ and the degree is 4. $\square$

(b) $X^6 + X^3 + 1$.

Solution. Let $u = e^{2\pi/9}$. Then, one easily checks that $u, u^2, u^4, u^5, u^7, u^8$ are the six roots of our polynomial. Thus, the splitting field is $\mathbb{Q}(u)$ and its degree is six. $\square$

(2) If p is a prime number, show that the splitting field of $X^p - 1$ over $\mathbb{Q}$ has degree $p - 1$.

Solution. We have seen (in a homework, using Eisenstein criterion) that $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$ and the second polynomial is irreducible. If $u = e^{2\pi/p}$, then all the roots of $X^p - 1$ are just $1, u, u^2, \ldots, u^{p-1}$ and then the splitting field is just $\mathbb{Q}(u)$ which has degree $p - 1$. $\square$

(3) Let $P(X) = X^3 + aX + b$, $a, b \in \mathbb{Q}$ and let K its splitting field over $\mathbb{Q}$. Find all possible degrees of K over the rationals.

Solution. If $P(X)$ is a product of linear polynomials, then all the roots are rational and so splitting field is just $\mathbb{Q}$ and so degree is 1.

If not, next possibility is that $P = QL$ where Q is a degree 2 irreducible polynomial and L is linear. If $Q(X) = X^2 + rX + s$ and u is a root of Q, then the other root is $-r - u$ and so the splitting field is just $\mathbb{Q}(u)$ and has degree 2.

Next case is P irreducible. Let u be a root. Then, $\mathbb{Q}(u)$ has degree 3. If this is the splitting field, then we have the degree.

If not, $P(X) = (X - u)Q(X)$ with Q an irreducible polynomial of degree 2 over $\mathbb{Q}(u)$ and then as before, the splitting field is got by attaching a root v of Q to $\mathbb{Q}(u)$ and it has degree 2 over $\mathbb{Q}(u)$. So, the splitting field has degree 6 over $\mathbb{Q}$. $\square$

(4) Let $\phi : \mathbb{Q}(2^{1/3}) \to \mathbb{Q}(2^{1/3})$ be an automorphism. Show that ϕ is the identity.

Solution. $2^{1/3}$ is a root of the irreducible polynomial $X^3 - 2$. It is easy to check that $\phi(q) = q$ for all $q \in \mathbb{Q}$, using the fact $\phi(1) = 1$. Thus, $\phi(2^{1/3})$ must be a root of $X^3 - 2$. But, the 3 roots are $2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}$, where $\omega = e^{2\pi/3}$. The last two are complex numbers, not real and so not contained in $\mathbb{Q}(2^{1/3})$. So, $\phi(2^{1/3}) = 2^{1/3}$. Since any element in $\mathbb{Q}(2^{1/3})$ can be written as $a + b2^{1/3} + c2^{2/3}$ with a, b, c rational, we see that ϕ must be identity. $\square$

(5) Let $\phi : \mathbb{R} \to \mathbb{R}$ be a field automorphism. Show that ϕ is the identity. (Hint: Show that if $a < b$, $\phi(a) < \phi(b)$.)

Solution. Let $a \in \mathbb{R}$ with $a \geq 0$. Then, we can write $a = b^2$ for some real number b and then $\phi(a) = \phi(b^2) = \phi(b)^2 \geq 0$. It is also clear that if $a > 0$, so is $\phi(a)$. If a, b are real numbers with $a < b$, then $b - a > 0$ and so $\phi(b) - \phi(a) = \phi(b - a) > 0$ and so $\phi(b) > \phi(a)$.

Now, as we observed in the previous problem, $\phi(q) = q$ for all $q \in \mathbb{Q}$. Now, let $r \in \mathbb{R}$. Then, for any $q \leq r$, q rational, we get, $\phi(q) = q \leq \phi(r)$. This says, $\phi(r)$ can not be less than r, since if so, pick a rational number q with $\phi(r) < q < r$ (Hope you know this), to get a contradiction. Identical argument will show that $\phi(r) \leq r$ and thus $\phi(r) = r$. Since r was arbitrary, ϕ must be identity. $\square$