Solutions to Homework 9

Math 601, Spring 2008

38) (10 points). Let K be a field of characteristic $p > 0$, and $a \in K$. Prove that if $X^p - X - a$ has no root in K, it is irreducible in $K[X]$.

Let α be a root of an irreducible factor of $f(X) := X^p - X - a$. Then $K(\alpha)/K$ is already the splitting field of the separable polynomial $f(X)$ because $\{\alpha + i \,|\, 1 \le i \le p\}$ can be verified to be its roots. Thus $K(\alpha)/K$ is Galois with Galois group $\mathbb{Z}/p\mathbb{Z}$ generated by $\alpha \mapsto \alpha + 1$. Thus $[K(\alpha) : K] = p$ and hence $f(X)$ is irreducible.

39) [D-F] 14.3 #8 (10 points). Let $f(X) := X^p - X - a \in \mathbb{F}_p[X]$, where $a \ne 0$. Show $\mathrm{Gal}(f) = \mathbb{Z}/p\mathbb{Z}$.

By the previous problem, the splitting field of $f(X)$ is $\mathbb{F}_p[X]/(f(X))$ and $\mathrm{Gal}(f) = \mathbb{Z}/p\mathbb{Z}$ generated by $X + (f) \mapsto X + 1 + (f)$.

40) [D-F] 14.2 #3 (10 points). Let $f(X) := (X^2 - 2)(x^2 - 3)(X^2 - 5) \in \mathbb{Q}[X]$. Determine $\mathrm{Gal}(f)$ and all subfields of the splitting field K of $f(X)$.

$\mathrm{Gal}(f)$ is a subgroup of $G = (\mathbb{Z}/2\mathbb{Z})^3$ given by the permutations $(\sqrt{2}, \sqrt{3}, \sqrt{5}) \mapsto (\pm\sqrt{2}, \pm\sqrt{3}, \pm\sqrt{5})$. Since $3 \cdot 5$ is not a square in $\mathbb{Q}(\sqrt{2})$, by HW7 Problem 27), we get that $K/\mathbb{Q}(\sqrt{2})$ is biquadratic whence $K/\mathbb{Q}$ has degree 8. Since $K/\mathbb{Q}$ is Galois we have that $\mathrm{Gal}(f)$ has order 8 and hence equals G. The subfields of degree 4 correspond to the one dimensional subspaces of the $\mathbb{Z}/2\mathbb{Z}$- vector space $(\mathbb{Z}/2\mathbb{Z})^3$ which are $2^3 - 1 = 7$ in number. These subfields are $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{2}, \sqrt{15})$, $\mathbb{Q}(\sqrt{3}, \sqrt{10})$, $\mathbb{Q}(\sqrt{6}, \sqrt{10})$ and $\mathbb{Q}(\sqrt{6}, \sqrt{15})$. The subfields of degree 2 are in correspondence with the 2-dim'l subspaces of $(\mathbb{Z}/2\mathbb{Z})^3$, which by taking the orthogonal complement (w.r.t the inner product given by identity matrix), again corresponds to the 1-dim'l subspaces, 7 in number. These subfields are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{15})$ and $\mathbb{Q}(\sqrt{30})$. There is exactly one obvious subfield of degree 1 and 8.

41) [D-F] 14.2 #6 (10 points). Let $K = \mathbb{Q}(2^{1/8}, i)$ and $F_1 = \mathbb{Q}(i)$, $F_2 = \mathbb{Q}(\sqrt{2})$ and $F_3 = \mathbb{Q}(\sqrt{-2})$. Prove that $\mathrm{Gal}(K/F_1) = \mathbb{Z}/8\mathbb{Z}$, $\mathrm{Gal}(K/F_2) = D_8$ and $\mathrm{Gal}(K/F_3) = Q_8$.

We will use the information given on page 577 of [D-F] on the splitting field of $X^8 - 2$. $\mathrm{Gal}(K/\mathbb{Q})$ is the group $G = \langle s, t \,|\, s^8 = t^2 = 1, t^{-1}st = s^3 \rangle$. The fixed field of the subgroup $\mathbb{Z}/8\mathbb{Z}$ generated by s is F_1. Thus $\mathrm{Gal}(K/F_1) = \mathbb{Z}/8\mathbb{Z}$. The fixed field of the subgroup D_8 generated by s^2 and t is F_2. Thus $\mathrm{Gal}(K/F_2) = D_8$. The subgroup generated by s^2, st and ts is Q_8 and its fixed field is F_3, hence $\mathrm{Gal}(K/F_3) = Q_8$.

42) (10 points).

$K = \mathbb{Q}(\xi)$ is the splitting field of $f(X) = X^p - 1$. The discriminant of a polynomial g of degree n is $(-1)^{n(n-1)/2}$ times the product of the values of g' at the roots of g. Thus the discriminant of $f(X)$ is $(-1)^{p(p-1)/2}p^p \prod_{i=1}^{p} \xi^{(p-1)i} = (-1)^{p(p-1)/2}p^p$, which is thus not a square in $\mathbb{Q}$. Thus $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{\pm p})$ (according as $p \equiv \pm 1 \bmod 4$), is the unique degree 2 subfield $K/\mathbb{Q}$.