Solutions to Homework 7

Math 601, Spring 2008

32) (10 points). Let L/K be an extension field, and $a \in L$ an algebraic element over K whose minimal polynomial has odd degree. Show that $K(a) = K(a^2)$. Can you generalize this?

From the equation $[K(a) : K] = [K(a) : K(a^2)][K(a^2) : K]$ and the fact that the lhs is an odd number, we know $[K(a) : K(a^2)] = 1$ since it is either 1 or 2. But this means $K(a) = K(a^2)$. We now generalize this.

Claim : Let p be a prime number and let K be any field such that the polynomial $X^p - 1$ completely splits over K. Let L/K be an extension field, and $a \in L$ an algebraic element over K with $p \not| [K(a) : K]$, then $K(a) = K(a^p)$

To prove the claim we need a proposition.

Proposition : Let F be any field, and p a prime number. The polynomial $X^p - b \in F[X]$ is reducible iff b is a p-th power in F.

Proof : We only need to show that if $X^p - b$ is reducible then b is a p-th power. Let α be a root of $X^p - b$ in some extension field of $F(\alpha)$ of F. Since $\alpha^p - b = 0$, and since $X^p - b$ is reducible, we know $d := [F(\alpha) : F] \leq p - 1$. Multiplication by α is a vector space isomorphism of $F(\alpha)/F$ and has a well defined determinant $D \in F$. The p-th power of this linear transformation is scalar multiplication by $b \in F$, and hence has determinant b^d (since any basis gets scaled by b). Thus we get $D^p = b^d$. Now the set $\{i \in \mathbb{Z} \,|\, b^i \text{ is a } p \text{ -th power in } F\}$ is an additive group containing d as we just showed. It also contains p since b^p is trivially a p-th power. Since $0 < d < p$ is relatively prime to p, this additive group is $\mathbb{Z}$ and hence b is a p-th power in F.

In order to prove the claim , we use the proposition with $F = K(a^p)$ and $b = a^p$. From the equation $[K(a) : K] = [K(a) : K(a^p)][K(a^p) : K]$ and the hypothesis that the lhs is relatively prime to p, we get that $[K(a) : K(a^p)] < p$. Thus, $X^p - a^p \in K(a^p)[X]$ is reducible, and hence by the proposition we get that $X^p - a^p$ has a root $\alpha \in K(a^p)$. Since, by assumption $X^p - 1 = (X - \xi_1)(X - \xi_2) \cdots (X - \xi_p)$ in $K[X]$ we see that $X^p - a^p = \prod_{i=1}^{p} (X - \alpha\xi_i)$. In particular all the p-th roots of a^p in L including a itself are in $K(a^p)$, whence $K(a) = K(a^p)$.

31) (10 points). Let K be a field. Show that 0 is the intersection of the maximal ideals in $K[X_1, \cdots, X_n]$.

If $f(X_1, \cdots X_n)$ is in this intersection then $1 + f$ is a unit and hence a nonzero constant. Thus f itself is a constant. Since $(X_1, \cdots X_n)$ is a maximal ideal, the constant must be zero.

30) (10 points). Let K denote a splitting field for $X^8 - 2$ over $\mathbb{Q}$. Find $[K : \mathbb{Q}]$.

By Eisenstein's criterion $X^8 - 2$ is irreducible over $\mathbb{Q}$. If we adjoin the positive root $2^{1/8}$ to $\mathbb{Q}$, then we get an extension $F/\mathbb{Q}$ of degree 8 with $F \subset \mathbb{R} \subset \mathbb{C}$. Next we need to adjoin a primitive 8-th rooot of unity say $(1 + \sqrt{-1})/\sqrt{2}$ to F. Since $\sqrt{2} \in F$ we just need to adjoin $\sqrt{-1}$ which is a quadratic extension of F (since $\sqrt{-1}$ cannot already be in $F \subset \mathbb{R}$). Thus the degree of the required splitting field over $\mathbb{Q}$ is 16.

28 [D-F], 13.4 #5 (5 points). Let K/F be a finite extension. Show that K is a splitting field over $F \Leftrightarrow$ every irred. polynomial in $F[X]$ that has a root in K splits completely in K.

Proof of $\Leftarrow$: Let K/F be generated by $a_1, a_2, \cdots, a_m \in K$ and let $f_1, f_2, \cdots, f_m \in F[X]$ be the corresponding irreducible minimal polynomials. Then since each f_i has a root in K, it splits completely in K. Thus the product of the f_i splits completely in K and its roots generate K/F, so that K is a splitting field over F.

Proof of $\Rightarrow$: Let K be the splitting firld of $f(X) \in F[X]$ and let $g(X) \in F[X]$ be an irreducible polynomial which has a root $\alpha \in K$. We must show that $g(X)$ splits completely in K. Suppose not, then adjoin a root β of $g(X) \in K[X]$ to K and obtain a field $K(\beta)$. We have an isomorphism $\phi : F(\alpha) \to F(\beta)$ that sends $\alpha \mapsto \beta$. The splitting field of $(x - \alpha)f \in F(\alpha)[X]$ is K, whereas the splitting field of $\phi((x - \alpha)f) = (x - \beta)f \in F(\beta)[X]$ is $K(\beta)$. By Theorem 13.4.27 of the text, the isomorphsim ϕ extends to an isomorphism between K and $K(\beta)$. This isomorphism fixes F so that it is a vector space isomorphism of K/F with $K(\beta)/F$, whence $[K(\beta) : K][K : F] = [K : F]$ which is the same as $K(\beta) = K$. Thus $\beta \in K$ contradicting our assumption that $g(X)$ does not split completely in K. Thus $g(X)$ splits completely in K.

28 [D-F], 13.4 #6 (10 points) Suppose K_1 and K_2 are finite extensions of F contained in the field K, and assume both K_1 and K_2 are splitting fields over F, show that K_1K_2 and $K_1 \cap K_2$ are splitting fields over F.

If K_1 is the splitting field of $f_1(X) \in F(X)$ and K_2 the splitting field of $f_2(X)$ then by definition K_1K_2 is the smallest subfield of K generated by the roots of f_1 and f_2 and hence is the splitting field of $f_1f_2 \in F[X]$. As for $K_1 \cap K_2$, we use the previous problem: $K_1 \cap K_2$ is a splitting field over F if every irreducible polynomial $g(X) \in F[X]$ that has a root in $K_1 \cap K_2$ splits completely in $K_1 \cap K_2$. Indeed, if $g(X)$ has a root in $K_1 \cap K_2$ then it has a root in K_i (where $i = 1, 2$) , hence it splits completely in K_i (because K_i is a splitting field). Thus $g(X)$ splits completely in K and by the uniqueness of the factorization in $K[X]$ of g into $\deg(g)$ linear factors, we see that the roots of g in K_1 are the same as the roots of g in K_2. Thus $g[X]$ splits completely in $K_1 \cap K_2$.

27 [D-F], 13.2 #8 (10 points). Let F be a field with $\mathrm{char}(F) \neq 2$. Let D_1, D_2 be elements of F neither of which is a square in F. Prove that $[F(\sqrt{D_1}, \sqrt{D_2}) : F]$ is 2 or 4 according as D_1D_2 is or is-not a square in F.

Suppose D_1D_2 is a square in F, then $F(\sqrt{D_1}, \sqrt{D_2}) = F(\sqrt{D_1D_2}, \sqrt{D_2}) = F(\sqrt{D_2})$ and hence $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 2$. If D_1D_2 is not a square in F, Let $K = F(\sqrt{D_1D_2})$, and consider the automorphism $\sigma : K \to K$ which fixes F and sends $\sqrt{D_1D_2} \mapsto -\sqrt{D_1D_2}$. We note that $\mathrm{char}(F) \neq 2$ implies that $\sigma(x) = x \Leftrightarrow x \in F$. Suppose further that $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = [F(\sqrt{D_1D_2}, \sqrt{D_2}) : F] = 2$. This means $\sqrt{D_2}$ (and hence $\sqrt{D_1}$) exist in K. Since $\sigma(D_i) = D_i$, it follows that $\sigma(\sqrt{D_i}) = \pm\sqrt{D_i}$. Moreover $\sigma(\sqrt{D_1D_2}) = -\sqrt{D_1D_2}$, therefore exactly one of the $\sqrt{D_i}$'s gets sent to itself under sigma (and the other to its negative). But $\sigma(\sqrt{D_i}) = \sqrt{D_i}$ implies $\sqrt{D_i} \in F$, a contradiction. Therefore $[F(\sqrt{D_1}, \sqrt{D_2}) : F]$ cannot be 2 and must be 4.