Mathematics GU4042 Modern Algebra II
Assignment # 6

Benjamin Church

December 21, 2017

Page 163.

Problem 3.

$\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ which is generated by a finite number of algebraic elements (since $\sqrt{2}$ and $\sqrt{3}$ solve X^2-2 and X^2-3 respectively) so it is an algebraic extension. Therefore, every element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is algebraic including $\sqrt{2}+\sqrt{3}$.

Consider the polynomial,

$$\begin{aligned}
&(X-(\sqrt{2}+\sqrt{3}))(X+(\sqrt{2}+\sqrt{3}))(X-(\sqrt{2}-\sqrt{3}))(X+(\sqrt{2}-\sqrt{3})) \\
&\qquad = (X^2-(5+2\sqrt{6}))(X^2-(5-2\sqrt{6})) = ([X^2-5]-2\sqrt{6})([X^2-5]+2\sqrt{6}) \\
&\qquad = [X^2-5]^2 - 4\cdot 6 = X^4 - 10X^2 + 1
\end{aligned}$$

Clearly, $\sqrt{2}+\sqrt{3}$ is a root of X^4-10X^2+1 and this must be the minimal polynomial because it has degree 4 which is the degree of $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2$

Problem 5.

Let $E = \mathbb{Q}(\sqrt[6]{2})$ then because $\sqrt{2} = (\sqrt[6]{2})^3 \in \mathbb{Q}(\sqrt[6]{2})$ we have $\mathbb{Q}(\sqrt{2}) \subset E$. However, $\sqrt{2} \notin \mathbb{Q}$ and $\sqrt[6]{2}$ is not of degree 2 so $\sqrt[6]{2} \notin \mathbb{Q}(\sqrt{2})$. Thus, $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq E$.

Page 165.

Problem 3.

Let $K \subset E \subset F$ be fields with F algebraic over E and E algebraic over K. Let $\alpha \in F$ then α satisfies some $f \in E[X]$ with $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ where $a_i \in E$. Thus, $f \in K(a_0, \dots, a_n)[X]$ so α is algebraic over $K(a_0, \dots, a_n)$ and therefore, $K(a_0, \dots, a_n)(\alpha)$ is a finite extension of $K(a_0, \dots, a_n)$. Finally,

$$[K(a_0, \dots, a_n)(\alpha) : K] = [K(a_0, \dots, a_n)(\alpha) : K(a_0, \dots, a_n)][K(a_0, \dots, a_n) : K]$$

and the two factors on the right hand side are finite. Therefore, $[K(a_0, \dots, a_n)(\alpha) : K]$ is finite so the fact that

$$[K(a_0, \dots, a_n)(\alpha) : K] = [K(a_0, \dots, a_n)(\alpha) : K(\alpha)][K(\alpha) : K]$$

gives that $[K(\alpha) : K]$ is finite so α is algebraic over K. Thus, F is an algebraic extension of K.

Additional Problem 1.

Let E/K be a field extension and $\alpha \in E$ be algebraic over K. Let $q \in K[X]$ be the minimal polynomial of α. Suppose that $f \in K[X]$ is a monic polynomial with degree equal to the degree of q such that $f(\alpha) = 0$. Now, let $ev_\alpha : K[X] \to K$ be the homomorphism given by $ev_\alpha(f) = f(\alpha)$. By definition, $\ker ev_\alpha = (q)$ and $f \in \ker ev_\alpha$. Therefore, $f = kq$ so $\deg f = \deg k + \deg q$ and thus, $\deg k = 0$ because $\deg f = \deg q$. Now, $k \in K$ but both polynomials are monic so $k = 1$. Thus, $f = q$.

Alternatively, $(f - q)(\alpha) = 0$ but f and q are monic of equal degree so $\deg (f - q) < \deg q$. However, q is the minimal polynomial so we must have $f - q = 0$ and thus $f = q$.

Additional Problem 2.

Let E/K be a field extension and $\alpha \in E$ be algebraic over K. Let $q \in K[X]$ be the minimal polynomial of α with $d = \deg q$. We introduce the homomorphism $ev_\alpha : K[X] \to K(\alpha)$ given by $ev_\alpha(f) = f(\alpha)$. Now, $\ker ev_\alpha = (q)$ and q is irreducible so (q) is a maximal ideal. Since (q) is maximal, $K[X]/(q)$ is a field. Also, $K[X]/(q) \cong \mathrm{Im}(ev_\alpha) \subset K(\alpha)$. However, by the isomorphism, $\mathrm{Im}(ev_\alpha)$ is a field containing α and K contained in $K(\alpha)$ so $\mathrm{Im}(ev_\alpha) = K(\alpha)$ by minimality. The map ev_α factors through $K[X]/(q)$ by $ev_\alpha = f \circ \pi$ with unique isomorphism f. Since f is a surjection, given any element $k \in K(\alpha)$ we can write $f(p + (q)) = k$ for some $p \in K[X]$. Now write $p = qs + r$ with $s, r \in K[X]$ and $r = 0$ or $\deg r < \deg q = d$. Therefore, we can write

$$r(X) = a_0 + a_1 X + \cdots + a_l X^l$$

with $a_i \in K$ and $l < d$. Now, $p + (q) = qs + r + (p) = r + (p) = \pi(r)$. Thus, we have,

$$k = f \circ \pi(r) = ev_\alpha(r) = a_0 + a_1\alpha + \cdots + a_l\alpha^l$$

thus $k \in \mathrm{span}\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ so the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ spans all of $K(\alpha)$. Also, suppose that for some constants $a_i \in K$ we have,

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{d-1}\alpha^{d-1} = 0$$

Then, the polynomial $p \in K[X]$ given by $p(X) = a_0 + a_1 X + \ldots a_{d-1}X^{d-1}$ has α as a root. However, $\deg p = d - 1 < d = \deg q$ contradicting the minimality of q unless $p = 0$. Therefore, each $a_i = 0$ so the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is linearly independent and thus a basis.