MATH 421 QUIZ 6 Solutions 4/26/2004

1. (6 pts) True or false:
Let K be a subfield of F, and let u, v be elements in F that are algebraic over K, with minimal polynomials $p(x)$ and $q(x)$, respectively.

T $\underline{x}$ F $\underline{\quad}$ If $K(u) \subseteq K(v)$, then $\deg(p(x)) \leq \deg(q(x))$.

T $\underline{x}$ F $\underline{\quad}$ If $K(u) \subseteq K(v)$, then $\deg(p(x)) \mid \deg(q(x))$.

This is true since $\deg(p(x)) = [K(u) : K]$, and $[K(u) : K]$ is a divisor of $[K(v) : K] = \deg(q(x))$. Since this implies that $\deg(p(x)) \leq \deg(q(x))$, the first statement is also true.

T $\underline{\quad}$ F $\underline{x}$ If $\deg(p(x)) \leq \deg(q(x))$, then $K(u) \subseteq K(v)$.

As a counterexample, let $K = \mathbf{Q}$, let $u = \sqrt{2}$, and let $v = \sqrt[3]{2}$. A homework problem shows that $\mathbf{Q}(\sqrt{2})$ is not contained in $\mathbf{Q}(\sqrt[3]{2})$, even though the degree of the minimal polynomial $x^2 - 2$ of $\sqrt{2}$ is less than the degree of the minimal polynomial $x^3 - 2$ of $\sqrt[3]{2}$.

2. (6 pts) Describe the elements of $\mathbf{Q}(\sqrt[5]{2})$. If you were asked to find the inverse of $2 + \sqrt[5]{2} + \sqrt[5]{4}$ in $\mathbf{Q}(\sqrt[5]{2})$, describe what you would do. (*But don't do it!*).

The minimal polynomial of $\sqrt[5]{2}$ over $\mathbf{Q}$ is $x^5 - 2$ ($\sqrt[5]{2}$ is a root of $x^5 - 2$, and it is irreducible over $\mathbf{Q}$ by Eisenstein's criterion with $p = 2$) and so $\mathbf{Q}(\sqrt[5]{2})$ has degree 5 over $\mathbf{Q}$. In general, if $u \in F$ has degree n over K, then $K(u)$ has basis $1, \ldots, u^{n-1}$ over K. Thus $\mathbf{Q}(\sqrt[5]{2}) = \{a + b\sqrt[5]{2} + c\sqrt[5]{4} + d\sqrt[5]{8} + e\sqrt[5]{16} \mid a, b, d, c, e \in \mathbf{Q}\}$.

To find the inverse of $2 + \sqrt[5]{2} + \sqrt[5]{4}$, we can work either in $\mathbf{Q}(\sqrt[5]{2})$ or in the isomorphic field $\mathbf{Q}[x]/\left\langle x^5 - 2 \right\rangle$. In the first case, we can set $(2 + \sqrt[5]{2} + \sqrt[5]{4})(a + b\sqrt[5]{2} + c\sqrt[5]{4} + d\sqrt[5]{8} + e\sqrt[5]{16}) = 1$ and solve the resulting system of equations. In the second case, we can use the Euclidean algorithm in $\mathbf{Q}[x]$ to find the gcd of $x^5 - 2$ and $x^2 + x + 2$. Writing $(x^2 + x + 2)f(x) + (x^5 - 2)g(x) = 1$ shows that the coset of $f(x)$ is the inverse of the coset of $x^2 + x + 2$, and then the corresponding element $f(\sqrt[5]{2})$ is the inverse of $2 + \sqrt[5]{2} + \sqrt[5]{4}$ in $\mathbf{Q}(\sqrt[5]{2})$.

3. (8 pts) Let K be a subfield of F, and let u be a nonzero element of F that is algebraic over K. Let $I = \{f(x) \in K[x] \mid f(u) = 0\}$, and let $p(x)$ be a nonzero polynomial of minimal degree in I. Prove that $p(x)$ is a factor of each polynomial in I, and that $p(x)$ is irreducible.

Hint: Do this from first principles, using the division algorithm for polynomials, OR quote results that we have already proved about the ideals in the polynomial ring $K[x]$.

See the last three paragraphs on page 235 of the text, and the proof of Proposition 6.1.3.

From first principles: for any $f(x) \in I$ use the division algorithm to write $f(x) = q(x)p(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < \deg(p(x))$. Then $r(u) = f(u) - q(u)p(u) = 0 - q(u) \cdot 0 = 0$, so $r(x) \in I$, which contradicts the choice of $p(x)$ unless $r(x) = 0$. Thus $p(x)$ is a factor of each polynomial in I. Now suppose that we could factor $p(x)$ as $p(x) = f(x)g(x)$, where $f(x)$ and $g(x)$ have lower degree. Then $f(u)g(u) = p(u) = 0$, so either $f(u) = 0$ or $g(u) = 0$ since $f(u), g(u)$ are elements in a field. This again contradicts the choice of $p(x)$ as an element of minimal degree in I, and so $p(x)$ must be irreducible.

Using ideals in $K[x]$: define a ring homomorphism $\phi_u : K[x] \to F$ by $\phi_u(f(x)) = f(u)$, for all $f(x) \in K[x]$. Then $I = \ker(\phi_u)$, so I is an ideal of $K[x]$ and therefore is generated by any nonzero polynomial of minimal degree. It follows that $p(x)$ is a factor of each polynomial in I. The image of ϕ_u is an integral domain, since it is a subring of F, and therefore I is a prime ideal, so its generator $p(x)$ must be an irreducible polynomial.