MATH 425 Hour Exam II Solution **Radford** **04/19/2009**

---

1. (**25 points**) Important fact about the minimal polynomial are found in Theorems 20.3, 21.2, and 21.3. These can be used without explicit reference.

(a) $\mathbf{Q}(\sqrt{5}+\imath\sqrt{3}) \subseteq \mathbf{Q}(\sqrt{5}, \imath\sqrt{3})$ (**2**). Since $(\sqrt{5}+\imath\sqrt{3})(\sqrt{5}-\imath\sqrt{3}) = 5+3 = 8$, $\alpha^{-1} = (1/8)(\sqrt{5}-\imath\sqrt{3})$, where $\alpha = \sqrt{5}+\imath\sqrt{3}$. Therefore $\sqrt{5} = \alpha/2 + 4\alpha^{-1}$ and $\imath\sqrt{3} = \alpha/2 - 4\alpha^{-1}$ belong to $\mathbf{Q}(\sqrt{5}+\imath\sqrt{3})$ which means $\mathbf{Q}(\sqrt{5}, \imath\sqrt{3}) \subseteq \mathbf{Q}(\sqrt{5}+\imath\sqrt{3})$ (**2**). Hence the two preceding field are the same (**2**).

Now $[\mathbf{Q}(\sqrt{5}) : \mathbf{Q}] = 2$ since $\sqrt{5}$ is a root of $x^2 - 5 \in \mathbf{Q}[x]$, which is irreducible by the Eisenstein Criterion with $p = 5$, and $[\mathbf{Q}(\sqrt{5})(\imath\sqrt{3}) : \mathbf{Q}(\sqrt{5}] \leq 2$ since $\imath\sqrt{3}$ is a root of $x^2 + 3 \in \mathbf{Q}(\sqrt{5})[x]$. As $\imath\sqrt{3} \notin \mathbf{Q}(\sqrt{5})$ the later index is 2. Therefore $[F : \mathbf{Q}] = [F : \mathbf{Q}(\sqrt{5})][\mathbf{Q}(\sqrt{5}) : \mathbf{Q}] = 2{\cdot}2 = 4$ (**3**).

(b) In light of part (a) we need only find a monic degree 4 polynomial $f(x) \in \mathbf{Q}[x]$ which has α as a root. $\alpha^2 = (\sqrt{5}+\imath\sqrt{3})^2 = 5 + 2\sqrt{5}\imath\sqrt{3} - 3 = 2 + 2\imath\sqrt{15}$ and therefore $-60 = (2\imath\sqrt{15})^2 = (\alpha^2-2)^2 = \alpha^4 - 4\alpha^2 + 4$ which means that $\alpha^4 - 4\alpha^2 + 64 = 0$. Take $f(x) = x^4 - 4x^2 + 64$.

(c) We use part (a). $[\mathbf{Q}(\sqrt{5}) : \mathbf{Q}] = 2$ as $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbf{Q}[x]$ which is irreducible by the Eisenstein Criterion with $p = 2$. Since $4 = [\mathbf{Q}(\alpha) : \mathbf{Q}] = [\mathbf{Q}(\alpha) : \mathbf{Q}(\sqrt{5})][\mathbf{Q}(\sqrt{5}) : \mathbf{Q}]$ we conclude that $[\mathbf{Q}(\alpha) : \mathbf{Q}(\sqrt{5})] = 2$. For the reasons cited in part (b) we need only find a monic degree 2 polynomial $g(x) \in \mathbf{Q}(\sqrt{5})[x]$ which has α as a root. Now $-3 = (\imath\sqrt{3})^2 = (\alpha-\sqrt{5})^2 = \alpha^2 - 2\sqrt{5}\alpha + 2$ means that $\alpha^2 - 2\sqrt{5}\alpha + 8 = 0$. Take $g(x) = x^2 - 2\sqrt{5}x + 8$.

---

2. (**25 points**) A rather detailed solution is provided. Important principles are involved. This problem is based on Theorem 21.2, Theorem 21.5 and its proof, and Example 2 on page 371.

(a) $3^{1/2}$, $7^{1/3}$ are roots of x^2-3, $x^3-7 \in \mathbf{Q}[x]$ and as such are irreducible by the Eisenstein Criterion with $p = 3, 7$ (**3**). Therefore $x^2 - 3$, $x^3 - 7$ are the minimal polynomials of $3^{1/2}$, $7^{1/3}$ over $\mathbf{Q}$ which means $[\mathbf{Q}(3^{1/2}) : \mathbf{Q}] = 2$ and $[\mathbf{Q}(7^{1/3}) : \mathbf{Q}] = 3$. Since $\mathbf{Q} \subseteq \mathbf{Q}(3^{1/2}), \mathbf{Q}(7^{1/3}) \subseteq F$ both 2 and 3 divide $[F : \mathbf{Q}]$ and therefore 6 divides $[F : \mathbf{Q}]$ (**2**).

Now $[F : \mathbf{Q}(2^{1/2})] \leq 3$, since $7^{1/3}$ is a root of $x^3-7 \in \mathbf{Q}(2^{1/2})[x]$, and from the degree calculation $[F : \mathbf{Q}] = [F : \mathbf{Q}(2^{1/2})][\mathbf{Q}(2^{1/2}) : \mathbf{Q}] \leq 3{\cdot}2 = 6$ the equation $[F : \mathbf{Q}] = 6$ follows (**2**).

(b) From part (a) $3 = [F : \mathbf{Q}(2^{1/2})] = [\mathbf{Q}(7^{1/3})(2^{1/2}) : \mathbf{Q}(3^{1/2})]$ and thus $x^3 - 7$ is the minimal polynomial of $7^{1/3}$ over $\mathbf{Q}(2^{1/2})$ (**3**). A basis for $\mathbf{Q}(2^{1/2})$ over $\mathbf{Q}$ is $\{1, 2^{1/2}\}$ and a basis for $F = \mathbf{Q}(2^{1/2})(7^{1/3})$ over $\mathbf{Q}(2^{1/2})$ is $\{1, 7^{1/3}, 7^{2/3}\}$. Thus a basis for F over $\mathbf{Q}$ is obtained by multiplying these two which yields $\{1,\ 7^{1/3},\ 7^{2/3},\ 2^{1/2}{\cdot}1,\ 2^{1/2}{\cdot}7^{1/3},\ 2^{1/2}{\cdot}7^{2/3}\}$ (**9**).

(c) $f(x)$ is an irreducible polynomial in $\mathbf{Q}[x]$ by the Eisenstein Criterion with $p = 2$ (**2**). Suppose that $a \in F$ is a root of $f(x)$. Since $f(x) \in \mathbf{Q}[x]$ is monic and irreducible it is the minimal polynomial of a over $\mathbf{Q}$. Therefore $4 = \operatorname{Deg} f(x) = [\mathbf{Q}(a) : \mathbf{Q}]$ divides $6 = [F : \mathbf{Q}]$, a contradiction (**2**). Thus $f(x)$ has no root in F (**2**).

---

3. (**25 points**) The bracketed comments are *explicit* justifications. These were not necessary to write down.

(a) $|G| = 3^3{\cdot}5$ so there is unique Sylow 5-subgroup of G since the number of them n_5 divides 3^3, and thus $n_5 = 1$, 3, 9, or 27 and $n_5 = 1 + 5\ell$ for some $\ell \geq 0$, and $2 = 3 - 1$, $8 = 9 - 1$ and $26 = 27 - 11$ are not divisible by 5 [Theorem 24.5, Sylow's Third Theorem] (**3**). N is a normal subgroup of G [Corollary to Theorem 24.5] (**3**).

Since 3^2 divides $|G|$ there is a subgroup H of G of order 3^2 [Theorem 24.3, Sylow's First Theorem] (**3**). Since N is a normal subgroup of G, HN is a subgroup of G (**3**) and $|HN| = |H||N|/|H{\cap}N| = |H||N| = 3^2{\cdot}5$; $|H{\cap}N| = 1$ as $|H{\cap}N|$ divides $|H| = 3^2$ and $|N| = 5$ (**3**)

(b) Since 3 divides $|G|$ there is a subgroup L of G of order 3 [Theorem 24.3] (**2**). Now LN is a subgroup of G of order $|LN| = 3{\cdot}5 = 15$ by the argument establishing $|HN|$ in part (a) (**2**).

(c) $|LN| = 3{\cdot}5$ and 3 does not divide $4 = 5 - 1$. Therefore LN is cyclic [Theorem 24.6] (**3**). Let a be a generator of LN. Then a has order 15 (**3**).

---

4. (**25 points**)

(a) Let $7^{1/4}$ be a real 4^{th} root of 7. Then

$$\begin{aligned} x^4 - 7 &= (x^2 - 7^{1/2})(x^2 + 7^{1/2}) \\ &= (x^2 - 7^{1/2})(x^2 - (-1)7^{1/2}) \\ &= (x - 7^{1/4})(x + 7^{1/4})(x - \imath 7^{1/4})(x + \imath 7^{1/4}) \ \ (\mathbf{6}) \end{aligned}$$

and thus $F = \mathbf{Q}(7^{1/4}, \imath)$ is a splitting field of $x^4 - 7$ over $\mathbf{Q}$ (**7**).

(b) $<a, b \,|\, a^2 = b^n = aba^{-1}b^{-1} = e>$. (**4**) for correct notation; (**2**), (**2**), (**4**) respectively for relations.

Comment: The last relation could be informally written as $ab = ba$. The presentation is based on the following calculations: $G = \{(a^i, b^j) \,|\, 0 \leq i < 1, 0 \leq j < n\}$, $(a^i, b^j) = (a^i, e)(e, b^j) = (a, e)^i(e, b)^j$, and $(a, e)(e, b) = (e, b)(a, e)$.