Mathematics 352 – Abstract Algebra II
Solutions for Problem Set 5
February 18, 2008

Section 10.3

3. Following the example on page 349 of the text, consider the tower of field extensions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}).$$

We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ with basis $\{1, \sqrt{2}\}$ since the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$. At the next step, we claim that $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ also and a basis is $\{1, \sqrt{3}\}$. Clearly $x^2 - 3$ is a polynomial in $\mathbb{Q}(\sqrt{2})[x]$ with $\sqrt{3}$ as a root. Moreover, it is irreducible because no $a + b\sqrt{2}$ is a root of this polynomial. (If there were such a root, then $(a + b\sqrt{2})^2 = 3$ would imply $\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$, which we know is not the case.) Hence as in the proof of Theorem 10.4 (the multiplicativity of degree in towers), $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$. Now we argue the same way for the final extension above. $\sqrt{5}$ is a root of $x^2 - 5 \in \mathbb{Q}(\sqrt{2},\sqrt{3})[x]$, but no $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ is a root of this polynomial, so $[\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{2},\sqrt{3})] = 2$ and $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}, \sqrt{5}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$ is a basis of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ over $\mathbb{Q}$.

5. We follow the same procedure as in the previous problem. Consider

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, i).$$

We have $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ with basis $\{1, \sqrt{3}\}$ since the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}$ is $x^2 - 3$. Next, i is a root of $x^2 + 1 \in \mathbb{Q}(\sqrt{3})[x]$ and this is the minimal polynomial because no $a + b\sqrt{3}$ can be a root of $x^2 + 1$ (since $a + b\sqrt{3}$ are all real numbers). Hence $[Q(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] = 2$ and $\{1, i\}$ is a basis. As in the proof of Theorem 10.4, $\{1, \sqrt{3}, i, i\sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{3}, i)$ over $\mathbb{Q}$. Hence $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$.

7. Assume $[K : F]$ is finite and u is algebraic over K. By Theorem 10.7, $[K(u) : K]$ is finite (this equals the degree of the minimal polynomial of u over K, $p(x) \in K[x]$. Now, we have $F \subseteq K \subseteq K(u)$, so also $F \subseteq F(u) \subseteq K(u)$. From the first tower $[K(u) : F] = [K(u) : K][K : F]$ is finite. This implies $[F(u) : F]$ is also finite from the second tower. By Theorem 10.7 again, $[F(u) : F]$ equals the degree of the minimal polynomial $q(x) \in F[x]$ of u over F. Since this polynomial has u as a root and also lies in $K[x]$, it follows that $p(x)|q(x)$ in $K[x]$. Therefore $\deg q(x) = [F(u) : F] \geq [K(u) : K] = \deg p(x)$.

8. Let $[K : F]$ be finite and assume u is algebraic over K. By Theorem 10.7, every element v of $K(u)$ is of the form

$$v = a_0 + a_1 u + \cdots a_{n-1} u^{n-1}, \tag{1}$$

with $a \in K$ (where n is the degree of the minimal polynomial of u over K). Now let $\{b_1, \ldots, b_k\}$ be a basis of K over F. We can expand each coefficient

$$a_i = c_{i1} b_1 + \cdots + c_{ik} b_k,$$

where $c_{ij} \in F$. Substituting these into (1), and regrouping terms we see that

$$v = (c_{01} + c_{11}u + \cdots + c_{n-1,1}u^{n-1})b_1 + \cdots + (c_{0k} + c_{1k}u + \cdots + c_{n-1,k}u^{n-1})b_k.$$

This shows that $\{b_1, \ldots, b_k\}$ also spans $K(u)$ over $F(u)$. Hence $[K(u) : F(u)] \leq [K : F]$ (with equality if and only if $\{b_1, \ldots, b_k\}$ is linearly independent over $F(u)$, which is *not automatic*).

11. (a) Consider the towers of field extensions $F \subseteq F(u) \subseteq F(u)(v) = F(u, v)$ and $F \subseteq F(v) \subseteq F(v)(u) = F(u, v)$. By hypothesis and Theorem 10.7, $[F(u) : F] = \deg p(x) = m$. So then by Theorem 10.4, $m|[F(u, v) : F]$. Similarly, $[F(v) : F] = \deg q(x) = n$. So then by Theorem 10.4, $n|[F(u, v) : F]$. So this says $[F(u, v) : F]$ is a *common multiple* of m, n. Since $(m, n) = 1$, then least common multiple is of m, n is the product mn. However, from problem 7 above with $K = F(v)$, we also know $[F(u, v) : F(v)] \leq [F(u) : F] = m$. Therefore $[F(u, v) : F] = [F(u, v) : F(v)][F(v) : F] \leq mn$. Therefore $[F(u, v) : F] = mn$.

(b) For a simple example, consider $F = \mathbb{Q}$, $u = \sqrt{2}$ and $v = 1 + \sqrt{2}$. We have $[\mathbb{Q}(u) : \mathbb{Q}] = [\mathbb{Q}(v) : \mathbb{Q}] = 2$ (look at the minimal polynomials). So the degrees are not relatively prime. Moreover $v \in \mathbb{Q}(u)$, so in fact $\mathbb{Q}(u, v) = \mathbb{Q}(u)$ and $[\mathbb{Q}(u, v) : \mathbb{Q}] = 2$, not $2 \cdot 2 = 4$.

(c) $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$ by part (a) since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ are relatively prime.

12. Method 1: (A "brute force" method not following the Hint.) Since we are given that D is a ring, the only thing "missing" is that we must show that every $u \in D$ has an inverse in D. So let $u \in D$. Since K is algebraic over F, every element of K is algebraic over F, and it follows that u is a root of a nonzero polynomial $c_n x^n + \cdots + c_1 x + c_0 \in F[x]$, or

$$c_n u^n + \cdots + c_1 u + c_0 = 0.$$

We can assume that zero is not also a root of this polynomial (why?). Hence we may assume $c_0 \neq 0$. But then rearranging the last equation,

$$(-c_0^{-1}(c_n u^{n-1} + \cdots + c_1))u = 1.$$

This shows $u^{-1} = -c_0^{-1}(c_n u^{n-1} + \cdots + c_1)$, which is in D since D is closed under sums and products and $u \in D$. Hence D is a field.

Method 2: (Following the Hint.) Let $u \in D$. Since u is in K, which is a field, we have the tower $F \subseteq F(u) \subset K$. Since K is algebraic over F, by Theorem 10.7 we know $F(u)$ has a basis $\{1, u, \ldots, u^{n-1}\}$ if the minimal polynomial of u over F has degree n. Therefore all the elements of $F(u)$ look like $v = a_0 + a_1 u + \cdots + a_{n-1}u^{n-1}$ where $a_i \in F$. But $u \in D$ and D is a ring (hence closed under sums and products). It follows that $F(u) \subseteq D$. Therefore D contains u^{-1}, the multiplicative inverse of u in K. Hence D is a field.

Comment: I happen to prefer proofs like the first one, because they give a method for finding u^{-1} in addition to establishing the existence of u^{-1} in D.

Section 10.4

2. For $x^2 - 3$, we have the roots $x = \pm\sqrt{3}$. Hence the splitting field is $\mathbb{Q}(\sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{3})$. For $x^2 - 2x - 2$, the quadratic formula gives

$$x = \frac{2 \pm \sqrt{4+8}}{2} = \frac{2 \pm 2\sqrt{3}}{2} = 1 \pm \sqrt{3}.$$

Therefore the splitting field of this polynomial is $\mathbb{Q}(1+\sqrt{3}, 1-\sqrt{3}) = \mathbb{Q}(1+\sqrt{3})$. Since $1+\sqrt{3}$ is an element of $\mathbb{Q}(\sqrt{3})$ and conversely every element of $\mathbb{Q}(\sqrt{3})$ is contained in $\mathbb{Q}(1+\sqrt{3})$, it follows that the splitting fields of these two polynomials are equal.

6. We have $u \in K$, so $F(u) \subseteq K$. Since K is a splitting field of a polynomial in $F[x]$ it is a finite (algebraic) extension of F. By Theorem 10.4, $[K : F] = [K : F(u)][F(u) : F]$. Since $[K : F] = p$ is prime, but we are given $u \neq F$, it follows that $[F(u) : F] = p$ and $[K : F(u)] = 1$. Therefore $K = F(u)$.

7. Since $F(u)$ is normal over F, by definition, if $p(x)$ is any irreducible polynomial in $F[x]$ and $p(x)$ has one root in $F(u)$, then $p(x)$ splits completely over $F(u)$ (has all its roots in $F(u)$). Apply this to $p(x) =$ the minimal polynomial of u over F. It follows that all the roots $u = u_1, u_2, \ldots, u_n$ of $p(x)$ are contained in $F(u)$. Therefore $F(u, u_2, \ldots, u_n) \subseteq F(u)$. The other inclusion is automatic, so $F(u, u_2, \ldots, u_n) = F(u)$. This shows that $F(u)$ is the splitting field of $p(x)$, which is what we wanted to show.

8. We use Theorem 10.15 for all the parts here.

(a) $\mathbb{Q}(\sqrt{3})$ is normal over $\mathbb{Q}$ since this is the splitting field of the polynomial $x^2 - 3$ over $\mathbb{Q}$.

(b) $\mathbb{Q}(\sqrt[3]{3})$ is not a normal extension of $\mathbb{Q}$ since this number is a root of the irreducible polynomial $x^3 - 3 \in \mathbb{Q}[x]$, but the other two roots of this polynomial are not contained in $\mathbb{Q}(\sqrt[3]{3})$ (they are the nonreal numbers $\rho\sqrt[3]{3}, \rho^2\sqrt[3]{3}$ where $\rho = \frac{-1}{2} + \frac{i\sqrt{3}}{2}$).

(c) $\mathbb{Q}(\sqrt{5}, i)$ is a normal extension of $\mathbb{Q}$, since this is the splitting field of $p(x) = (x^2-5)(x^2+1)$. (Note that the polynomial need not be irreducible in $F[x]$ in the theorem.)

18. Let $u_1, \ldots, u_t$ be the roots of $f(x) \in F[x]$ adjoined to obtain E, and let $u_1, \ldots, u_n$, $n \geq t$ be all of the roots of $f(x)$. By the definition, K is a splitting field of $f(x)$ over f if and only if $K = F(u_1, \ldots, u_n)$. But this is true if and only if

$$\begin{aligned} K &= F(u_1, \ldots, u_n) \\ &= F(u_1, \ldots, u_t)(u_{t+1}, \ldots, u_n) \\ &= E(u_{t+1}, \ldots, u_n) \\ &= E(u_1, \ldots, u_n) \text{ since } u_1, \ldots, u_t \text{ are already in } E\ . \end{aligned}$$

Finally, $K = E(u_1, \ldots, u_n)$ if and only if K is a splitting field of $f(x)$ over E, again by the definition.