Mathematics 352 – Abstract Algebra II
Solutions for Problem Set 6
March 10, 2008

*Section 10.5*

13. The inclusion $\mathbb{Q}(\sqrt{p}+\sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p},\sqrt{q})$ is automatic. To show equality, we will use the multiplicativity of degrees in towers. From $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}+\sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p},\sqrt{q})$, we see $[\mathbb{Q}(\sqrt{p}+\sqrt{q}):\mathbb{Q}]$ is a divisor of $[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}]$. By the same reasoning used in the example on page 349 in the text (and Exercises 3,4,5,6 in Section 10.3), $[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}] = 4$. Hence $[\mathbb{Q}(\sqrt{p}+\sqrt{q}):\mathbb{Q}]$ is either 2 or 4. We claim that it cannot be 2, hence $\mathbb{Q}(\sqrt{p}+\sqrt{q}) = \mathbb{Q}(\sqrt{p},\sqrt{q})$. Suppose on the other hand that $[\mathbb{Q}(\sqrt{p}+\sqrt{q}):\mathbb{Q}] = 2$. Then $\sqrt{p}+\sqrt{q}$ has minimal polynomial of the form $x^2+bx+c \in \mathbb{Q}[x]$ by Theorem 10.7. But then

$$0 = 2\sqrt{pq} + b\sqrt{p} + b\sqrt{q} + c + p + q = 0.$$

However, we know from Theorem 10.4 that $\beta = \{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ is a basis of $\mathbb{Q}(\sqrt{p},\sqrt{q})$ over $\mathbb{Q}$, so we get a contradiction because the above equation would imply that $\beta$ was linearly dependent over $\mathbb{Q}$. Hence $\mathbb{Q}(\sqrt{p}+\sqrt{q}) = \mathbb{Q}(\sqrt{p},\sqrt{q})$.

*Note:* It is also possible to adapt the proof of Theorem 10.18 for this problem. You need to show that taking $c = 1$ in $u = \sqrt{p} + c\sqrt{q}$ satisfies the condition on $c$ needed for the portion of that proof showing $F(v,w) = F(u)$ for some $u = v + cw$.

14. (*Note:* The point of this exercise is to reexamine the proof of Theorem 10.18 to see that only the hypothesis that $w$ is the root of a separable polynomial is needed to show that $F(v,w)$ is a simple extension of $F$ when $F$ is infinite. )

We proceed as in the proof of Theorem 10.18. Let $p(x)$ be the minimal polynomial of $v$ over $F$ and let $q(x)$ be the minimal polynomial of $w$ over $F$. Let $L$ be a splitting field of $p(x)q(x)$ and let $v = v_1, \ldots, v_m$ be the roots of $p(x)$ in $L$, while $w = w_1, \ldots, w_n$ are the roots of $q(x)$ in $L$. Let $u = v + cw$, where

$$c \neq \frac{v_i - v}{w - w_j}, \tag{1}$$

for all $1 \leq i \leq m$ and $1 < j \leq n$. We claim that $F(v,w) = F(u)$. To see this, let $r(x) = p(u - cx) \in F(u)[x]$. Since $v = u - cw$, this polynomial has $w = w_1$ as a root. We claim that none of the other roots of $q(x) = 0$ is a root of $r(x)$. If this were true, then $u - cw_j = v_i$, so $v + cw = v_i + cw_j$, and $c = \frac{v_i - v}{w - w_j}$. But this contracdicts (1), so $w$ is the only root of $q(x)$ that is also a root of $r(x)$. Let $s(x)$ be the minimal polynomial of $w$ over $F(u)[x]$. Then $s(x)$ divides $q(x)$ and $r(x)$ in $F(u)[x]$. Since the roots of $q(x)$ are *distinct* by hypothesis, this implies that $s(x) = x - w$ must be the gcd of $q(x)$ and $r(x)$ in $F(u)[x]$. Hence $w \in F(u)$. From $u = v + cw$, it follows that $v \in F(u)$ as well. Therefore $F(v,w) = F(u)$.

*Section 10.6*

5. We have that $K$ is an extension field of $F$. Since $K$ is a finite set, the dimension of $K$ over $F$ must also be finite, say $[K : F] = n$. Then $|K| = |F|^n = q^n$.

10. By Lemma 10.24 (the "freshman's dream"), we have $f(a+b) = (a+b)^p = a^p + b^p = f(a) + f(b)$. Moreover, $f(ab) = (ab)^p = a^p b^p = f(a)f(b)$ since multiplication in a field is commutative. This shows that $f : K \to K$ is a ring homomorphism. The order of $K$ must be $p^n$ for some $n \geq 1$. By Theorem 10.25, $K$ is a splitting field of $x^{p^n} - x$. Hence if $a, b \in K$ and $f(a) = f(b)$, then $a^p = b^p$. But then

$$a = a^{p^n} = (a^p)^{p^{n-1}} = (b^p)^{p^{n-1}} = b^{p^n} = b,$$

which shows that $f$ is one-to-one. Theorem 10.25 also shows that every $a$ in $K$ satisfies $a = \left(a^{p^{n-1}}\right)^p = f(a^{p^{n-1}})$. Hence $f$ is onto.

12. By Fermat's "little theorem," every $a \in \mathbb{Z}_p$ satisfies $a^p = a$. If $c$ is a root of $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$, then Theorem 10.7 implies the simple extension $K = \mathbb{Z}_p(c)$ is a finite field also, of order $p^n$ for some $n \leq \deg(f)$. It follows from Exercise 10 that $F : K \to K$ defined by $F(x) = x^p$ is an isomorphism which satisfies $F(a) = a$ for all $a \in \mathbb{Z}_p$. Hence if we apply $F$ to both sides of the equation $0 = a_n c^n + \cdots + a_1 c + a_0$, then

$$\begin{aligned} 0 = F(0) &= F(a_n c^n + \cdots + a_1 c + a_0) \\ &= F(a_n)F(c)^n + \cdots + F(a_1)F(c) + F(a_0) \quad \text{since } F \text{ is an isomorphism} \\ &= a_n F(c)^n + \cdots a_1 F(c) + a_0 \quad \text{since } F(a) = a \text{ for all } a \in \mathbb{Z}_p. \end{aligned}$$

Therefore, $F(c) = c^p$ is also a root of $f(x)$.

15. (a) Since $x^3 + x + 1$ has degree three, but has no roots in $\mathbb{Z}_2$, it is irreducible in $\mathbb{Z}_2[x]$. By Theorem 5.10, $K = \mathbb{Z}_2[x]/(x^3 + x + 1)$ is a field, and since $\{1, x, x^2\}$ is a basis of $K$ over $\mathbb{Z}_2$, $K$ has order 8. The element $x$ generates the multiplicative group of nonzero elements since:

$$\begin{aligned} x^0 &= 1 \\ x^1 &= x \\ x^2 &= x^2 \\ x^3 &= x + 1 \\ x^4 &= x^2 + x \\ x^5 &= x^2 + x + 1 \\ x^6 &= x^2 + 1 \\ x^7 &= 1. \end{aligned}$$

If we write the elements of $K$ as $K = \{0, 1, x, x^2, \ldots, x^6\}$, then the addition and multiplication

tables for $K$ are as follows:

| $+$ | $0$ | $1$ | $x$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ |
|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $1$ | $x$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ |
| $1$ | $1$ | $0$ | $x^3$ | $x^6$ | $x$ | $x^5$ | $x^4$ | $x^2$ |
| $x$ | $x$ | $x^3$ | $0$ | $x^4$ | $1$ | $x^2$ | $x^6$ | $x^5$ |
| $x^2$ | $x^2$ | $x^6$ | $x^4$ | $0$ | $x^5$ | $x$ | $x^3$ | $1$ |
| $x^3$ | $x^3$ | $x$ | $1$ | $x^5$ | $0$ | $x^6$ | $x^2$ | $x^4$ |
| $x^4$ | $x^4$ | $x^5$ | $x^2$ | $x$ | $x^6$ | $0$ | $1$ | $x^3$ |
| $x^5$ | $x^5$ | $x^4$ | $x^6$ | $x^3$ | $x^2$ | $1$ | $0$ | $x$ |
| $x^6$ | $x^6$ | $x^2$ | $x^5$ | $1$ | $x^4$ | $x^3$ | $x$ | $0$ |

and

| $\cdot$ | $0$ | $1$ | $x$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ |
|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $x$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ |
| $x$ | $0$ | $x$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ | $1$ |
| $x^2$ | $0$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ | $1$ | $x$ |
| $x^3$ | $0$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ | $1$ | $x$ | $x^2$ |
| $x^4$ | $0$ | $x^4$ | $x^5$ | $x^6$ | $1$ | $x$ | $x^2$ | $x^3$ |
| $x^5$ | $0$ | $x^5$ | $x^6$ | $1$ | $x$ | $x^2$ | $x^3$ | $x^4$ |
| $x^6$ | $0$ | $x^6$ | $1$ | $x$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ |

(Note: The multiplicative group of nonzero elements is cyclic of order 7.)

18. (a) Following the hint, let $n = qk + r$ in $\mathbb{Z}$ where $0 \leq r < k$. Then we note that

$$x^n - 1 = (x^{n-k} + x^{n-2k} + \cdots + x^{n-qk})(x^k - 1) + (x^r - 1), \tag{2}$$

as can be seen by multiplying out the right hand side. Since $r < k$, this equation is also the result of dividing $x^k - 1$ into $x^n - 1$ using polynomial division in $K[x]$ (by the uniqueness of the quotient and remainder in polynomial division).
$\Rightarrow$: Suppose first that $x^k - 1$ divides $x^n - 1$ in $F[x]$. Then the remainder of the polynomial division must be zero. This is true only if $r = 0$, so $k$ divides $n$ in $\mathbb{Z}$.
$\Leftarrow$: Conversely, if $k|n$, then $r = 0$, so $x^k - 1$ divides $x^n - 1$ in $K[x]$.
(b) Consider equation (2) but replace $x$ by $p$ (a prime $\geq 2$ in $\mathbb{Z}$):

$$p^n - 1 = (p^{n-k} + p^{n-2k} + \cdots + p^{n-qk})(p^k - 1) + (p^r - 1),$$

This is also the result of dividing $p^r - 1$ into $p^n - 1$ in $\mathbb{Z}$ (since $0 \leq p^r - 1 < p^n - 1$, by the uniqueness of quotient and remainder in integer division).

$$(p^k - 1)|(p^n - 1) \Leftrightarrow p^r - 1 = 0 \Leftrightarrow r = 0 \Leftrightarrow k|n.$$

19. (a) Let $F$ be a subfield of the finite field $K$ of order $p^n$. Since $p \cdot x = 0$ for all $x \in K$, $F$ also has characteristic $p$, and hence $|F| = p^d$ for some $d \leq n$. However, not all such $d$ are possible orders of

$F$. The the multiplicative group of nonzero elements in $F$ is a subgroup of the multiplicative group of nonzero elements in $K$. As a result, by Lagrange's Theorem, $p^d - 1$ must divide $p^n - 1$. By part (b) of Exercise 18, this implies $d|n$.
(b) If $d|n$, consider the polynomial $x^{p^d} - x$. We know that the splitting field of this polynomial is a field of order $p^d$. If we factor out the common factor $x$, then the nonzero elements of the field are the roots of $x^{p^d-1} - 1$. By part (b) of Exercise 18, since $d|n$, $p^d - 1$ divides $p^n - 1$. But then part (a) of Exercise 18 shows that $x^{p^d-1} - 1$ divides $x^{p^n-1} - 1$, so $x^{p^d} - x$ divides $x^{p^n} - x$ as well. Hence if $K$ is a field of order $p^n$ and $d|n$, then by Theorem 10.25, $K$ contains a subfield of order $p^d$.

By Corollary 10.27, if there are two such subfields, then they are isomorphic as fields (in particular the multiplicative orders of all the corresponding nonzero elements must be the same). However, this implies that such a subfield is unique, since the subgroup the multiplicative group of nonzero elements in $K$ consisting of elements of orders dividing $p^d - 1$ is unique.

20. If $f(x)$ is not irreducible, then since it is a quadratic polynomial it must have a root $\alpha$ in $K$. It follows that $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = 2$ by Theorem 10.7, so $\mathbb{Z}_p(\alpha)$ has order $p^2$. This would contradict the result of Exercise 19, though: $\mathbb{Z}_p(\alpha)$ would be a field of order $p^2$ contained in $K$ which has order $p^3$. Since $2 \not| 3$, this is not possible. Therefore $f(x)$ must be irreducible in $K[x]$.