**Math 430 Homework 6** **Sample solution based on that of Liam Bench**

**Chapter 22**

**2.** First we note that $[GF(p^n) : GF(p^m)] = ([GF(p^n) : GF(p)])/([GF(p^m) : GF(p)])$. Using Corollary 1 of Theorem 22.2 this is $n/m$.

**6.** We will show the other two distinct zeros are $\alpha^2$ and $\alpha^4$. Let $\mathbb{F} = \mathbb{Z}_2(\alpha)$. So $|\mathbb{F}^*| = 7$, $\mathbb{F}^* = \langle\alpha\rangle$, and $|\alpha| = 7$. First $f(\alpha^2) = \alpha^6+\alpha^2+1 = (\alpha^2+1)+\alpha^2+1 = 0$. Second $f(\alpha^4) = \alpha^{12}+\alpha^4+1 = (\alpha^2+\alpha+1)+(\alpha^2+\alpha)+1 = 0$.

**10.** First note that $x^2 + x + 2$ and $x^2 + 2x + 2$ are irreducible because they are degree 3 and have no zeros. So the two rings are Galois fields. They both have order $3^2$ because the two polynomials to create the factor ring are degree 2. So they are isomorphic since Galois fields are unique up to isomorphism.

**14.** First we show 12 is the smallest number with 6 divisors. Prime numbers only have 2 divisors so this eliminates 2,3,5,7, and 11. The number 4 has 3, 6 has 4, 8 has 4, 9 has 4, and 10 has 4 factors, where as 12 has 1,2,3,6, and 12 as divisors. So for each divisor, $m$, of 12, $GF(2^{12})$ has a unique subfield of order $p^m$ and these are the only subfields. So $GF(2^{12})$ has 6 subfields.

**20.** First note that $\mathbb{Z}_3[x]/\langle f(x)\rangle \approx GF(3^3)$. So as a group under multiplication $GF(27)^* \approx \mathbb{Z}_{26}$. Suppose $x$ and $2x$ are not generators of $GF(27)^*$. So the orders of $x$ and $2x$ are either 2 or 13. The order of $x$ and $2x$ are not 2 because $x^2 = (2x)^2 \neq 1$. Suppose $|x| = 13$. Then $(2x)^{13} = 2^{13}x^{13} = 2x^{13} = -1$ and so the order of $2x$ must be 13.

**32.** Let $\alpha$ be a zero of $f(x)$. In $\mathbb{Z}_p(\alpha)$, $f(x)$ can factor in one of two ways. Case 1 is $f(x) = (x-\alpha)h(x)$ where $\deg h(x) = 2$ and does not have zeros in the field. Case 2 is $f(x) = a(x-\alpha)(x-\alpha_1)(x-\alpha_2)$ where $\alpha_1, \alpha_2 \in \mathbb{Z}_p(\alpha)$.

Case 1: Let $\beta$ be an element such that $h(\beta) = 0$. So $[\mathbb{Z}_p(\alpha,\beta) : \mathbb{Z}_p] = [\mathbb{Z}_p(\alpha,\beta) : \mathbb{Z}_p(\alpha)][\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = 2\cdot 3 = 6$. So $\mathbb{Z}_p(\alpha,\beta)$ is a vector space over $\mathbb{Z}_p$ with a basis of 6 vectors. To express an element, there are 6 vectors each with a choice of $p$ scalar coefficients. So there are a total of $p^6$ elements in the splitting field.

Case 2: $\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = 3$ and so there are 3 vectors each with a choice of $p$ scalar coefficients. So there are $p^3$ elements in $\mathbb{Z}_p(\alpha)$.

**36.** Let $\mathbb{F}$ be a finite field with $n$ elements where the elements are $a_1, a_2, ..., a_n$. Suppose $\mathbb{F}$ is algebraically closed. Consider $f(x) = (x-a_1)(x-a_2)\cdots(x-a_n)+1$. So none of $a_1, a_2, ..., a_n$ are zeros of $f(x)$. So there must be a proper algebraic extension of $\mathbb{F}$. This contradicts the fact that $\mathbb{F}$ is algebraically closed.

**Chapter 23**

**4.** Looking at the figure in the book, let $Z$ be the point where 0 is, $B$ be the point length $b$ from $Z$, $A$ be the point length $a$ from $Z$, $C$ be the point length 1 from $Z$, and $D$ be the point at the intersection of $\overline{ZA}$ and the line segment going from $C$ to the middle of $\overline{ZA}$. I show that the length of $\overline{ZD}$ is $a/b$. First note that after constructing the line $\overline{BA}$ we can construct a line parallel which is $\overline{CD}$. So triangle $ZBA$ is similar to $ZCD$. Since $\frac{ZB}{ZC} = b$ we must have $\frac{ZA}{ZD} = b$. So $\frac{a}{ZD} = b$ and the length of $\overline{ZD}$ is $a/b$.

**6.** Suppose angle $\theta$ is constructible. Consider two rays that have an angle of $\theta$ intersecting at the origin with the bottom line on the positive x-axis. Call the bottom ray $\overrightarrow{ZA}$ and the top ray $\overrightarrow{ZB}$. Drawing a perpendicular line from $\overrightarrow{ZA}$ through $\overrightarrow{ZB}$ we create a right triangle. So $m(\angle BZA) = \theta$. So $\frac{AB}{ZB} = \sin(\theta)$ which is constructible by problem 4.

**10.** If a 40° angle is constructible then a 20° angle is constructible. But in the book it is shown that trisecting a 60° angle is impossible and therefore a 20° angle is not constructible.

**Optional problems**

**22.26** Suppose $g(x)$ is an irreducible polynomial of degree $m$ over $F = GF(p)$ and $g(x)$ is a factor of $x^{p^n} - x$. Then $F[x]/\langle g(x)\rangle$ is isomorphic to $F(\alpha)$, which is a subfield of $E = GF(p^n)$ and

$$n = [E, F] = [E : F(\alpha)][F(\alpha) : F] = m[F(\alpha) : F].$$

**22.40** Note that $GF(p^n)$ is the splitting field of $x^{p^n} - x \in GF(P)$, and $GF(p^n)^* = \langle\alpha\rangle$ is a cyclic group under multiplication. If $d$ is a factor of $n$, then $GP(p^d)$ can be viewed as a subfield of $GF(p^n)$ and $GP(p^d)^* = \langle\alpha^r\rangle$ with $r = (p^n-1)/(p^d-1)$. Suppose $f(x) \in GF(p)[x]$ is a monic (irreducible) minimal polynomial of $\beta = \alpha^r$ of degree $k$. Then $GF(p)(\beta)$ contains $\beta, \dots, \beta^r$ is the splitting field of $f(x)$ in $GF(p^n)$, so that $[GF(p)(\beta) : GF(p)] = k$ has $p^d$ elements. So, $k = d$.