HOMEWORK #10 – MATH 435

SOLUTIONS

Chapter 5, Section 3: #12 If a is as in Problem 11, show that $F(a) \simeq F(x)$ where $F(x)$ is the field of rational functions in x over F.

Solution: Consider the function $\phi : F(x) \to F(a)$ defined by the rule $\phi(f(x)/g(x)) = f(a)/g(a)$. This is certainly well defined since first $g(a) \neq 0$ for any non-zero $g(x)$ (because a is transcendental). Also note $f(x)h(x)/(g(x)h(x))$ is sent to $f(a)h(a)/(g(a)h(a)) = f(a)/g(a)$ and so ϕ is well defined.

Of course,

$$\begin{array}{rl} & \phi(f(x)/g(x) + f'(x)/g'(x)) \\ = & \phi((f(x)g'(x) + f'(x)g(x))/(g(x)g'(x))) \\ = & (f(a)g'(a) + f'(a)g(a))/(g(a)g'(a)) \\ = & f(a)/g(a) + f'(a)/g'(a) \\ = & \phi(f(x)/g(x)) + \phi(f'(x)/g'(x)) \end{array}$$

and likewise

$$\begin{array}{rl} & \phi\big((f(x)/g(x))(f'(x)/g'(x))\big) \\ = & \phi\big((f(x)f'(x))/(g(x)g'(x))\big) \\ = & (f(a)f'(a))/(g(a)g'(a)) \\ = & (f(a)/g(a))(f'(a)/g'(a)) \\ = & \phi(f(x)/g(x))\phi(f'(x)/g'(x)) \end{array}$$

which proves that ϕ is a ring homomorphism. It remains to show that ϕ is bijective. Certainly it is surjective for any $f(a)/g(a) \in K(a)$ can be written as $\phi(f(x)/g(x))$. Finally, $f(x)/g(x) \in \ker\phi$ and so therefore that $\phi(f(x)/g(x)) = 0$. This implies that $f(a)/g(a) = 0$ and thus that $f(a) = 0$. But then $f(x)$ must be the zero polynomial since a is transcendental. Thus $f(x)/g(x) = 0$ as well. Thus $\ker\phi = \{0\}$ and so ϕ is injective. This completes the proof.

Chapter 5, Section 3: #14 Using the result of #13, show that a finite field k has p^n elements for some prime p and some positive integer n.

Solution: Let p denote the characteristic of the field k in question. Since k is finite, p is finite and as we've seen before, p must also be prime. Consider the set $F = \{\underbrace{1 + \cdots + 1}_{m} | 0 \leq m \leq p-1\}$. This set is certainly closed under addition and multiplication (since $\underbrace{1 + \cdots + 1}_{p} = 0$). It is therefore a subringof a field. Thus F is an integral domain. But F is also a finite integral domain so that F itself is a field.

Now, we can consider $[k : F]$. This number is finite since k is finite. Thus $|k| = |F|^n$ for some integer n. But $|F| = p$ and the problem is completed.

Chapter 5, Section 3: #15 Construct two fields K and F such that K is an algebraic extension of F but is not a finite extension of F.

Solution: There are many correct solutions, here's one that uses the notation of the next chapter. Choose $F = \mathbb{Q}$. Let $K = E_{\mathbb{R}}(F)$, the algebraic closure of F in $\mathbb{R}$. This is certainly algebraic (I just adjoined only algebraic elements). Suppose that $[K : F] = n < \infty$, and thus choose $a = 2^{\frac{1}{n+1}} \in \mathbb{R}$. We notice that $2^{\frac{1}{n}}$ is a root of the polynomial $f(x) = x^{n+1} + 2$, which is irreducible in $\mathbb{Q}[x]$ by Eisenstein. Thus a is algebraic and so $a \in K$. Therefore we have the chain

$$F \subseteq F[a] \subseteq K$$

of extension fields and so:

$$[K : F] = [K : F[a]] \cdot [F[a] : F].$$

But $[F[a] : F] = n + 1$ and so $n + 1$ divides $[K : F] = n$, a contradiction.

Chapter 5, Section 4: #2 If $a, b \in K$ are algebraic over F of degrees m and n respectively and suppose that m and n are relatively prime. Prove that $[F(a, b) : F] = mn$.

Solution: First we make some simple observations. $F(a)$ is the smallest field containing F and a, and also that $F[a] = F(a)$. Therefore $F(a, b) = F[a](b) = F[a][b]$ is the smallest field containing F and also both a and b. Thus $F[b][a] = F(b, a) = F(a, b) = F[a][b]$. Now, we have the chain of containments $F \subseteq F[a] \subseteq F[a][b] = F(a, b)$ and so we can write

$$[F(a, b) : F] = [F[a] : F] \cdot [F[a][b] : F[a]]$$

but therefore $m = [F[a] : F]$ divides $[F(a, b) : F]$. By symmetry, n also divides $[F(a, b) : F]$ and so $[F(a, b) : F] \geq mn$ since m and n are relatively prime.

On the other hand, $g(b) = 0$ for some $g(x) \in F[x]$ of degree n. Note $F[x] \subsetneq F[a][x]$ and so $g(x) \in F[a][x]$ as well. Thus $g(b) = 0$. Let's let $h(x) \in F[a][x]$ be the minimal polynomial for b, so that $h|g$. It follows that $\deg h \leq n$ and so $[F[a][b] : F[a]] = \deg h \leq n$. Thus

$$mn \leq [F(a, b) : F] = [F[a] : F] \cdot [F[a][b] : F[a]] = m \cdot [F[a][b] : F[a]] \leq mn$$

and so we have our desired equality.

Chapter 5, Section 4: #4 If $K \subseteq F$ is such that $[K : F] = p$ with p a prime, show that $K = F(a)$ for *every* $a \in K \setminus F$.

Solution: Choose $a \in K \setminus F$. Thus we have a chain of field extensions

$$F \subsetneq F(a) = F[a] \subseteq K.$$

Note the first inequality follows because $a \notin F$. Thus $[F(a) : F] > 1$ (it is the degree of the minimal polynomial for a over F, that polynomial is not linear since $a \notin F$).

Therefore

$$p = [K : F] = [K : F[a]] \cdot [F[a] : F]$$

and so since $[F[a] : F] > 1$ and divides p, $[F[a] : F] = p$. But we have just shown that the F-vector subspace $F[a] \subseteq K$ has the same dimension over F as does K. Thus from a previous homework $F[a] = K$. This completes the proof.