Math 835 Homework 1

Theo Koss

September 2024

1 Chapter 13

1.1 Chapter 2

1. Prove that if $\operatorname{ch}\mathbb{F} = p$, then $|\mathbb{F}| = p^n$.

   Proof. Let $\mathbb{F}$ be a field with $\operatorname{ch}\mathbb{F} = p$. Consider the prime subfield $K < \mathbb{F}$, generated by 1_F. From the book, $F \supset \langle 1_F \rangle \cong \mathbb{Z}_p$ if $\operatorname{ch}\mathbb{F} = p$. Consider the vector space over K, and since K has p elements, we have finitely many choices for the basis. WLOG, choose a basis $b_1, b_2, \ldots, b_n$. Then $[K : F] = \dim_F K = n$ and so $|\mathbb{F}| = p^n$. $\square$

14. Prove that if $[F(\alpha) : F]$ is odd, then $F(\alpha) = F(\alpha^2)$

   Proof. Let $[F(\alpha) : F]$ be odd. Then the degree of the minimal polynomial of α is odd. By way of contradiction, assume $F(\alpha^2) \neq F(\alpha)$. In particular, $\alpha \notin F(\alpha^2)$ Then the extension of $F(\alpha)/F(\alpha^2)$ is quadratic, with minimal polynomial $x^2 - \alpha^2$. But this is a problem because by theorem 14,

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)] \cdot [F(\alpha^2) : F]$$

   But we assumed LHS is odd, and showed that $F(\alpha)/F(\alpha^2)$ is quadratic. Contradiction. Therefore, $\alpha \in F(\alpha^2)$. Which implies $F(\alpha) = F(\alpha^2)$ $\square$

18. Let k be a field and let $k(x)$ be the field of rational functions in x with coefficients from k. Let $t \in k(x)$ be the rational function $\frac{P(x)}{Q(x)}$ with relatively prime polynomials $P(x), Q(x) \in k[x]$, with $Q(x) \neq 0$. Then $k(x)$ is an extension of $k(t)$ and to compute its degree it is necessary to compute the minimal polynomial with coefficients in $k(t)$ satisfied by x.

(a). Show that the polynomial $P(X) - tQ(X)$ in the variable X and coefficients in $k(t)$ is irreducible over $k(t)$ and has x as a root.

$$P(X) - tQ(X) = 0 \text{ is linear in } (k[X])[t] \text{ so it is irreducible}$$

It also (trivially) has x as a root. We also have that $(k[X])[t] = (k[t])[X]$ so $P(X) - tQ(X)$ is irreducible in $(k(t))[X]$.

(b). Show that the degree of $P(X) - tQ(X)$ as a polynomial in X with coefficients in $k(t)$ is the maximum of the degrees of $P(x)$ and $Q(x)$.

Proof. Let $n \in \mathbb{N}$ be the maximum of the degrees of $P(x)$ and $Q(x)$. So we may now write them as:

$$P(x) = a_n x^n + \cdots + a_1 x + a_0$$
$$Q(x) = b_n x^n + \cdots + b_1 x + b_0$$

Where a_n and b_n are not *both* 0. Now we can analyse the leading term in $P(X) - tQ(x)$, which is $a_n - tb_n$. We must show $a_n \neq tb_n$. This is true because $t \in k(x)$ but $t \notin k$, so t is some rational polynomial in x, not a constant, and a_n is just a constant. So $a_n - tb_n \neq 0$ and therefore $deg(P(X) - tQ(X)) = n$ which we defined to be the maximum of the degrees. $\square$

(c). Show that

$$[k(x) : k(t)] = \left[k(x) : k\left(\frac{P(x)}{Q(x)}\right)\right] = \max(\deg P(x), \deg Q(x))$$

Proof. We have from part (a). that $P(X) - tQ(X)$ is irreducible in $(k(t))[X]$ and has x as a root, so we can mod out by the polynomial to get

$$k(x) \cong (k(t)[X]) / \langle P(X) - tQ(X) \rangle$$

By part (b), we have that the degree of this extension is the maximum of the degrees of the polynomials. So

$$[k(x) : k(t)] = \max(\deg P(x), \deg Q(x))$$

As required. $\square$