Problem Set # 9

Due Friday November 22th in recitation

Exercise 1(⋆): 30 points
Prove that if \([F(\alpha) : F]\) is odd then \(F(\alpha) = F(\alpha^2)\).

Solution :
If \(\alpha \notin F(\alpha^2)\) then \(F(\alpha^2)\) is a proper subfield of \(F(\alpha)\). moreover \(\alpha\) satisfies \(x^2 - \alpha^2 \in F(\alpha^2)\), so \([F(\alpha) : F(\alpha^2)] = 2\). However,

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

which contradicts the fact that \([F(\alpha) : F]\) is odd. thus \(\alpha \in F(\alpha^2)\), and therefore \(F(\alpha) = F(\alpha^2)\).

Exercise 2(⋆): 60 points
A field of prime characteristic \(p\) is perfect if the map \(F \to F\) given by \(\alpha \mapsto \alpha^p\) is surjective.

1. Show every finite field is perfect.

2. Let \(F\) be an arbitrary field of characteristic \(p \neq 0\). Show that the field of rational function

\[ F(x) = \{ \frac{f(x)}{g(x)} : \forall f \in K[x], g \in K[x^\times] \} \]

where \(K[x^\times] = K[x]\}\{\text{the null polynomial}\} is not perfect. (Hint: Consider the polynomial \(x \in F(x)\).)

Solution :

1. Recall that \((\alpha + \beta)^p = \alpha^p + \beta^p\) in a field of characteristic \(p\), so the map \(\phi(x)\) is a group homomorphism. Since \(F\) is a field, \(\phi(x) = 0\) if and only if \(x = 0\); in other words \(\phi\) is injective. Since a map of finite sets is injective if and only if it is surjective, this means that \(F\) is perfect.

2. It is enough to find one element of \(F(x)\) which is not a \(p^{th}\) power. We claim that \(x\) is not a \(p^{th}\) power. Say \(x = (a(x)/b(x))^p\). Then \(x \times b(x)^p = a(x)^p\). Since \(F\) is a field, the degree of the left hand side is \(p \times \deg(b) + 1\) and the degree of the right side is \(p \times \deg(a)\). Since one side is divisible by \(p\) and the other isn’t, they can’t be equal.
Exercise 3(*): 60 points

1. Suppose that \([L : K] = p\) is a prime number. Prove that \(L/K\) is a simple extension i.e. there is \(\alpha \in L\) such that \(L = K(\alpha)\) (Hint: You can choose any \(\alpha \in L \setminus F\)).

2. Let \(L/K\) be a finite extension, and let \(p(x)\) be an irreducible polynomial in \(K[x]\) with \(\text{deg}(p(x)) \geq 2\). Prove by contradiction that, if \(\text{deg}(p)\) and \([L : K]\) are coprime, then \(p(x)\) has no zeros in \(L\). (Hint: If \(\alpha \in L\) is a root of \(p(x)\), then consider the field \(K(\alpha)\).)

**Solution:**

1. Suppose that \([L : K] = p\) is prime and let \(\alpha \in L \setminus K\). Then \([K(\alpha) : K]\) divides \([L : K]\), so \([K(\alpha) : K] = 1\) or \(p\). Since \(K(\alpha) \neq K\), it follows that \([K(\alpha) : K] = p\) and so \([L : K(\alpha)] = 1\). Therefore \(L = K(\alpha)\) and \(L\) is a simple extension of \(K\).

2. Suppose that \(\alpha \in L\) is a root of \(p\). Then \([K(\alpha) : K] = p\) divides \([L : K(\alpha)]\). But \([K(\alpha) : K] = \text{deg}(p(x))\), so \(\text{deg}(p(x))\) divides \([L : K]\). Since these numbers are assumed to be coprime, it follows that \(\text{deg}(p(x)) = 1\), a contradiction.

Exercise 4(*): 30 points
Let \(K\) be a finite extension field of \(F\), then any endomorphism of \(K\) over \(F\) is an automorphism.

**Solution:**
For any endomorphism over \(F\) \(\sigma : K \rightarrow K\), since \(\sigma(1) = 1\), \(\sigma\) is not zero homomorphism, thus \(\sigma\) is injective. Since \([K : F] < \infty\), let \(a_1, \ldots, a_n\) be a basis of \(K\) over \(F\), we can easily check \(\sigma(a_1), \ldots, \sigma(a_n)\) is also a basis of \(K\) over \(F\). For any \(c \in K\), there exist \(b_1, \ldots, b_n \in F\) such that \(b_1\sigma(a_1) + \ldots + b_n\sigma(a_n) = c\). It follows \(\sigma(b_1a_1 + \ldots + b_na_n) = c\). Then \(\sigma\) is surjective, as required.

Exercise 5(*): 20 points Prove that the ring \(F_2[x]/(x^3 + x + 1)\) is a field, but that \(F_3[x]/(x^3 + x + 1)\) is not a field.

**Solution:**
It is easy to check that 0, 1 are both not a root \(x^3 + x + 1\) in \(F_2[x]/(x^3 + x + 1)\), hence \(x^3 + x + 1\) is irreducible. Since \(F_2[x]\) is a principal ideal integral domain, the irreducibility of \(x^3 + x + 1\) implies that \(x^3 + x + 1\) is maximal. Therefore, \(F_2[x]/(x^3 + x + 1)\) is a field.
For the second statement, one has \(x^3 + x + 1 = (x - 1)(x^2 - x + 1)\) (1 is a root. Hence the ideal \((x^3 + x + 1)\) is not maximal and \(F_3[x]/(x^3 + x + 1)\) is not a field.