Math 562 **Spring 2014**
Homework 5 **Drew Armstrong**

---

1. (Finite Implies Algebraic) Consider a field extension $L \supseteq K$. Recall that we say $\alpha \in L$ is algebraic over K if there exists nonzero $f(x) \in K[x]$ such that $f(\alpha) = 0$. We say that the field extension $K \subseteq L$ is algebraic if every element of L is algebraic over K. Prove that if $[L : K] < \infty$ (i.e. if L is finite dimensional as a vector space over K) then $L \supseteq K$ is algebraic. [Hint: Given any $\alpha \in L$ the set $1, \alpha, \alpha^2, \ldots$ is linearly **dependent** over K.]

2. (Algebraic Closure) Given a field extension $L \supseteq K$, define the set

$$\bar{K} := \{\alpha \in L : \alpha \text{ is algebraic over } K\} \subseteq L,$$

called the algebraic closure of K in L. Prove that $\bar{K}$ is a field. [Hint: Given $\alpha, \beta \in \bar{K}$ we want to show that $\alpha - \beta, \alpha\beta^{-1} \in \bar{K}$. Since $\alpha - \beta, \alpha\beta^{-1} \in K(\alpha, \beta)$ it suffices by Problem 1 to show that $K(\alpha, \beta) \supseteq K$ is a finite dimensional extension. Use the Tower Law.]

3. (Characteristic of a Domain) Let R be a domain.

(a) Show that there exists a unique ring homomorphism $\varphi : \mathbb{Z} \to R$. [Hint: $\varphi(2_\mathbb{Z}) = \varphi(1_\mathbb{Z} + 1_\mathbb{Z}) = \varphi(1_\mathbb{Z}) + \varphi(1_\mathbb{Z}) = 1_R + 1_R$.]

(b) Show that $\ker(\varphi) = (p) < \mathbb{Z}$, where $p = 0$ or p is prime. This p is called the characteristic of the domain R.

(c) If R is finite, show that its characteristic is not 0.

4. (The Size of a Finite Field). Suppose that the field K is finite. By Problem 3, the unique ring map $\varphi : \mathbb{Z} \to K$ has kernel (p) for some prime $0 \neq p \in \mathbb{Z}$.

(a) Prove that the image $\varphi(\mathbb{Z}) \subseteq K$ is a subfield of K (called the prime subfield).

(b) Prove that K is a finite dimensional vector space over $\varphi(\mathbb{Z})$, say $[K : \varphi(\mathbb{Z})] = n < \infty$.

(c) Conclude that $|K| = p^n$.

5. (Examples of Finite Fields) For all primes $p \in \mathbb{Z}$ we define

$$\mathbb{F}_p := \mathbb{Z}/(p).$$

This a field of size p. However, it is not obvious that fields of size p^n exist for any $n > 1$.

(a) Prove that the polynomial $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible.

(b) Prove that the ring $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a field of size 4. We will call it $\mathbb{F}_4$.

(c) Let $\alpha := x + (x^2 + x + 1) \in \mathbb{F}_4$. Explicitly write down the addition and multiplication tables of $\mathbb{F}_4$ in terms of the ("imaginary") element α.

6. (A Special Polynomial) Let $n, p \in \mathbb{N}$ with p prime and consider the special polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$. If $f(x) \in \mathbb{F}_p[x]$ is irreducible of degree d, prove that

$$f(x) \text{ divides } (x^{p^n} - x) \text{ in } \mathbb{F}_p[x] \quad \Longleftrightarrow \quad d \text{ divides } n \text{ in } \mathbb{Z}.$$

[Hint: The group of units of the field $\mathbb{F}_p[x]/(f(x))$ has size $p^d - 1$, hence Langrange's Theorem implies that $c^{p^d} = c$ for all $c \in \mathbb{F}_p/(f(x))$. If $n = dk$ then raising any $c \in \mathbb{F}_p[x]/(f(x))$ to the p^d-th power k successive times gives

$$c = c^{p^d} = c^{p^{2d}} = \cdots = c^{p^{kd}} = c^{p^n}.$$

Now let $c = x + (f(x))$. Conversely, assume $f(x)$ divides $x^{p^n} - x$ and divide n by d to get $n = qd + r$ with $0 \leq r < d$. From above we know that $x^{p^d} = x \bmod f(x)$, and hence

$$x = x^{p^n} = (x^{p^{qd}})^{p^r} = x^{p^r} \bmod f(x).$$

Now recall the Freshman's Binomial Theorem which says that $(a+b)^p = a^p + b^p \bmod p$ for a, b in any ring. It follows that $g(x)^{p^r} = g(x) \bmod f(x)$ for any polynomial $g(x) \in \mathbb{F}_p[x]$. Thus every element of the field $\mathbb{F}_p[x]/(f(x))$ is a root of the polynomial $T^{p^r} - T \in \mathbb{F}_p[x]/(f(x))[T]$. If $r \neq 0$, use HW4.4 and Problem 4(b) to show that $p^d \leq p^r$, and hence $d \leq r$. This contradiction implies that $r = 0$ as desired.]

7. (Gauss' Formula for Counting Irreducible Polynomials)

(a) Let K be a field. For all $f(x) = \sum_k a_k x^k \in K[x]$ we define the formal derivative:

$$f'(x) := \sum_k k a_k x^{k-1}.$$

Prove that if $f(x)$ has a repeated factor then $f(x)$ and $f'(x)$ are not coprime. [Hint: You can assume that the usual product rule holds.]

(b) Let $N_p(d)$ be the number of irreducible polynomials in $\mathbb{F}_p[x]$ of degree d and with leading coefficient 1. Use Problem 6 to prove Gauss' formula:

$$p^n = \sum_{d|n} d N_p(d).$$

[Hint: Show that the special polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$ and its derivative are coprime, so every irreducible factor of $x^{p^n} - x$ occurs with multiplicity 1.]