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.]

Proof. Suppose that $[L : K] < \infty$. Then for any $\alpha \in L$ the set $\{1, \alpha, \alpha^2, \ldots\}$ is linearly dependent over K. That is, there exist some elements $a_0, \ldots, a_n \in K$ not all zero such that

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

Define the polynomial $f(x) := a_0 + a_1x + \cdots + a_nx^n \in K[x]$. Since $f \neq 0$ and $f(\alpha) = 0$ we conclude that α is algebraic over K. Since this is true for all $\alpha \in L$ we conclude that L is algebraic over K. $\square$

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.]

Proof. Consider a field extension $L \supseteq K$ and let $\alpha, \beta \in L$ be algebraic over K. We want to show that both $\alpha - \beta$ and $\alpha\beta^{-1}$ are algebraic over K. So consider $K(\alpha, \beta) \subseteq L$ which is the smallest subfield of L containing $K \cup \{\alpha, \beta\}$. Because α is algebraic over K we know that $K(\alpha) = K[\alpha]$ has finite dimension over K. Then since β is algebraic over K (hence also over $K(\alpha)$) we know that $K(\alpha)(\beta) = K(\alpha)[\beta]$ has finite dimension over $K(\alpha)$. It is straightforward to check that $K(\alpha, \beta)$ and $K(\alpha)(\beta)$ are the same thing, so by the Tower Law for field extensions we have

$$[K(\alpha, \beta) : K] = [K(\alpha)(\beta) : K] = [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K] < \infty.$$

Since $\alpha - \beta$ and $\alpha\beta^{-1}$ are in $K(\alpha, \beta)$, we conclude from Problem 1 that they are both algebraic over K. $\square$

[Remark: Given $\alpha, \beta \in L$ satisfying $f(\alpha) = g(\beta) = 0$ for some $f, g \in K[x]$, it is possible to prove that $\alpha - \beta$ and $\alpha\beta^{-1}$ are algebraic by using f, g to explicitly construct polynomials that they must satisfy. However this method of proof is much more difficult than the nonconstructive method given above.]

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.

Proof. For part (a), let $\varphi : \mathbb{Z} \to R$ be any ring homomorphism, so that we have $\varphi(0_{\mathbb{Z}}) = 0_R$ and $\varphi(1_{\mathbb{Z}}) = 1_R$. For any integer $n > 1$ we have

$$\varphi(n) = \varphi(1_{\mathbb{Z}} + \cdots + 1_{\mathbb{Z}}) = \varphi(1_{\mathbb{Z}}) + \cdots + \varphi(1_{\mathbb{Z}}) = 1_R + \cdots + 1_R = \text{“}n \cdot 1_R\text{”},$$

and for any integer $n < 0$ we have

$$\varphi(n) = -\varphi(-n) = -\text{“}(-n) \cdot 1_R\text{”}.$$

Now the map is determined.

For part (b), note that $\operatorname{im}\varphi \subseteq R$ is a subring of a domain, hence is itself a domain. By the First Isomorphism Theorem we have $\mathbb{Z}/\ker\varphi \approx \operatorname{im}\varphi$ and then HW3.1 implies that $\ker\varphi$ is a prime ideal of $\mathbb{Z}$. Recall that the prime ideals of $\mathbb{Z}$ are (0) and (p) for $p \in \mathbb{N}$ prime.

For part (c), let R be finite and assume for contradiction that $\ker\varphi = (0)$. Then since $\mathbb{Z} \approx \mathbb{Z}/(0) \approx \operatorname{im}\varphi$ we have

$$\infty = |\mathbb{Z}| = |\operatorname{im}\varphi| \leq |R| < \infty.$$

Contradiction. □

[Remark: We just proved that the characteristic of a finite domain is a prime $p > 0$. It is a bit silly to say it this way because any finite domain is actually a field. Indeed, let R be a finite domain. Then given any nonzero element $x \in R$ we consider the map $R \to R$ defined by $y \mapsto xy$. Since R is a domain this map is injective. Then since R is finite the map is also surjective, i.e., there exists $y \in R$ such that $xy = 1$.]

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 $|K| = p^n$.

Proof. Let K be a finite field of characteristic $p > 0$. By Problem 3 this means that $\mathbb{Z}/(p) \approx \varphi(\mathbb{Z}) \subseteq K$. But since $\mathbb{Z}$ is a PID we know that the prime ideal $(p) < \mathbb{Z}$ is also maximal, hence $\mathbb{Z}/(p)$ is a field. This proves part (a).

For part (b) we consider K as a vector space over $\varphi(\mathbb{Z})$. Since K is finite it has a finite spanning set (K itself). Since any spanning set contains a basis we conclude that K has a finite basis over $\varphi(\mathbb{Z})$, say $[K : \varphi(\mathbb{Z})] = n$.

For part (c) note that every element of K can be written uniquely as an ordered n-tuple of elements of $\varphi(\mathbb{Z})$ (the coefficients when expanded in some basis). Thus we have

$$|K| = |\varphi(\mathbb{Z})|^n = |\mathbb{Z}/(p)|^n = p^n.$$

□

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.

Proof. For part (a) suppose for contradiction that we can write

$$x^2 + x + 1 = f(x)g(x)$$

where $f, g \in \mathbb{F}_2[x]$ have degree strictly between 0 and 2. Then we have $f(x) = \alpha + \beta x$ for some $\alpha, \beta \in \mathbb{F}_2$ with $\beta \neq 0$ and hence $-\alpha/\beta \in \mathbb{F}_2$ is a root of x^2+x+1. But this polynomial has no roots in $\mathbb{F}_2$ because $1^2+1+1 = 3 = 1 \neq 0$ and $0^2+0+1 = 1 \neq 0$. We conclude that x^2+x+1 is irreducible over $\mathbb{F}_2$. [Remark: It is relatively easy to determine if a polynomial of degree ≤ 3 is irreducible. It is relatively hard to determine if a polynomial of degree ≥ 4 is irreducible.]

For part (b) note that the ideal $(x^2 + x + 1) < \mathbb{F}_2[x]$ is maximal among principal ideals because x^2+x+1 is irreducible. Since $\mathbb{F}_2[x]$ is a PID this implies that (x^2+x+1) is maximal among **all** ideals and hence $K := \mathbb{F}_2[x]/(x^2 + x + 1)$ is a field. In fact we saw in class that K can be thought of as a field extension of $\mathbb{F}_2$ that contains an element $\alpha \in K$ such that $\alpha^2 + \alpha + 1 = 0$. (To see this we show that the map $\mathbb{F}_2 \to K$ defined by $a \mapsto a + (x^2 + x + 1)$ is injective and note that $\alpha := x + (x^2 + x + 1) \in K$ satisfies $\alpha^2 + \alpha + 1 = 0$ in the field K.)

For part (c) we note that x^2+x+1 is the minimal polynomial of $\alpha \in K$ over $\mathbb{F}_2$. Indeed, if $m_\alpha(x) \in \mathbb{F}_2[x]$ is the minimal polynomial then $m_\alpha(x)$ divides $x^2 + x + 1$ over $\mathbb{F}_2$. But we saw in part (a) that $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, hence $m_\alpha(x) = x^2 + x + 1$. By a result from class this implies that $K \approx \mathbb{F}_2[\alpha] = \{a + b\alpha : a, b \in \mathbb{F}_2\}$. Note that this field has 4 elements:

$$\mathbb{F}_2[\alpha] = \{0, 1, \alpha, 1 + \alpha\}.$$

Finally, using the fact that $\alpha^2 + \alpha + 1 = 0$, we can explicitly write down the addition and multiplication tables:

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

□

[Remark: It's just like working with complex numbers.]

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 $c \in \mathbb{F}_p[x]/(f(x))$. 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.]

Proof. Let $f(x) \in \mathbb{F}_p[x]$ be irreducible of degree d.

Using the same argument as Problem 5 we can show that $\mathbb{F}_p[x]/(f(x))$ is a field of size p^d. This field has group of units of size $p^d - 1$ and hence for all nonzero $c \in \mathbb{F}_p[x]/(f(x))$ Lagrange's Theorem implies that $c^{p^d-1} = 1$. Then multiplying by c gives $c^{p^d} = c$ for any element c (even zero). Now suppose that $n = dk$ for some $k \in \mathbb{N}$. Raising any $c \in \mathbb{F}_p[x]/(f(x))$ to the p^d-th power k successive times gives

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

Finally, taking $c = x + (f(x))$ gives $x + (f(x)) = (x + (f(x)))^{p^n} = x^{p^n} + (f(x))$, hence $x^{p^n} - x = 0 + (f(x))$. We conclude that $f(x)$ divides $x^{p^n} - x$ over $\mathbb{F}_p$.

Conversely, suppose that $f(x)$ divides $x^{p^n} - x$ over $\mathbb{F}_p$, i.e., suppose that $x = x^{p^n}$ in $\mathbb{F}_p[x]/(f(x))$. Divide n by d to get $n = qd + r$ with $0 \leq r < d$. Using Lagrange's Theorem again shows that $x^{p^d} = x$ in $\mathbb{F}_p[x]/(f(x))$ and taking the p^d-th power k successive times gives $x^{p^{kd}} = x$ for any $k \in \mathbb{N}$. This implies that

$$x = x^{p^n} = x^{p^{qd+r}} = x^{p^{qd}p^r} = (x^{p^{qd}})^{p^r} = x^{p^r} \quad \text{in } \mathbb{F}_p[x]/(f(x)).$$

Now recall that $(a+b)^p = a^p + b^p \bmod p$ for a, b in any ring because the binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is divisible by p when $0 < k < p$ (in this case p divides the numerator and not the denominator). Let $g(x) = \sum_k a_k x^k \in \mathbb{F}_p[x]$ be any polynomial. If we raise $g(x)$ to the p-th power r successive times and use the Freshman's Binomial Theorem each time we get

$$(\sum_k a_k x^k)^{p^r} = \sum_k (a_k)^{p^r} (x^k)^{p^r} = \sum_k (a_k)^{p^r} (x^{p^r})^k = \sum_k (a_k)^{p^r} x^k.$$

But note that for all $a \in \mathbb{F}_p$ we have $a^p = a$ (again by Lagrange's Theorem) and so $a = a^p = (a^p)^p = a^{p^2} = \cdots = a^{p^r}$. We conclude that $g(x)^{p^r} = g(x)$ in $\mathbb{F}_p[x]/(f(x))$ for any polynomial $g(x) \in \mathbb{F}_p[x]$, hence **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 $r \neq 0$ then $T^{p^r} - T$ has degree p^r, so it can have at most p^r distinct roots in any field extension. Since the field $\mathbb{F}_p[x]/(f(x))$ has p^d elements we conclude that $p^d \leq p^r$, and since $p \geq 1$ (in fact $p \geq 2$) this implies that $d \leq r$. This contradicts the fact that $r < d$. Hence $r = 0$ as desired. □

[Remark: That polynomial is pretty special, right?]

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.]

Proof. For part (a), suppose that $f(x) \in K[x]$ has a nontrivial repeated factor, say $f(x) = g(x)^r h(x)$ with $\deg(g) \geq 1$ and $r \geq 2$. Taking the derivative and using the product rule gives

$$f'(x) = rg(x)^{r-1}h(x) + g(x)^r h'(x) = g(x)(g(x)^{r-2}h(x) + g(x)^{r-1}h'(x)).$$

We conclude that $f(x)$ and $f'(x)$ share the nontrivial factor $g(x)$.

For part (b), let $N_p(d)$ be the number of irreducible polynomials in $\mathbb{F}_p[x]$ of degree d and with leading coefficient 1. (The total number of irreducible polynomials in $\mathbb{F}_p[x]$ of degree d equals $(p-1)N_p(d)$ because we can multiply by any nonzero constant.) Now suppose we have factored the special polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$ into irreducibles. We may assume all the factors have leading coefficient 1 by collecing units. By Problem 6, each irreducible factor has degree d dividing n, and every irreducible polynomial with degree dividing n occurs in the factorization at least once. Note that the derivative $(x^{p^n} - x)' = p^n x^{p^n - 1} - 1 = 0 - 1 = -1$ has no nontrivial factor and so $x^{p^n} - x$ has no repeated factor by part (a). We conclude that $x^{p^n} - x$ can be expressed as the product of all irreducible polynomials in $\mathbb{F}_p[x]$ with leading coefficient 1 and degree d dividing n, each appearing once. Comparing degrees on both sides of the factorization gives Gauss' formula:

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

$\square$

[Remark: Gauss' formula is more often written as

$$N_p(n) = \frac{1}{n}\sum_{d|n} \mu(n/d)p^d,$$

but to make sense of this we would need to discuss the number-theoretic möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$, and we don't have time for that. If you will allow me to suppose that the coefficients are indeed in $\{-1, 0, 1\}$ then we can use Gauss' formula to prove that $N_p(n) > 0$ (see course notes). Thus there exist finite fields of all sizes p^n.]