Math 4108 HW6

Pengfei Zhu

February 15, 2024

Exercise 6.6. Let K be a field of non-zero characteristic p.

1. Show that the mapping $\varphi : K \to K$ given by $\varphi(a) = a^p$ $(a \in K)$ is a monomorphism (called the Frobenius monomorphism). Show (a) that this is an automorphism if the field is finite; (b) that φ is the identity map if $K = \mathbb{Z}_p$.

   1) The mapping $\varphi(a) = a^p$ $(a \in K)$ is a monomorphism.

   The map φ is a homomorphism by definition:

   $$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$$

   $$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$$

   The map φ is also injective by definition:

   $$\varphi(a) = \varphi(b) \Rightarrow 0 = \varphi(a) - \varphi(b) = a^p - b^p = (a-b)^p \Rightarrow a - b = 0$$

   Thus φ is a monomorphism.

   a) φ is an automorphism.

   If F is finite, $|\varphi(F)| = |F| \Rightarrow \varphi(F) = F$. Thus φ is an automorphism.

   b) φ is the identity map if $K = \mathbb{Z}_p$.

   The elements of $\mathbb{Z}_p$ are $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. which can then written as $\{0, 1, 1+1, 1+1+1, \ldots, 1+1+\ldots+1_{p-1}\}$.

   We show that $\varphi(0) = 0$ and $\varphi(1) = 1$, and $\varphi(1+1+\ldots+1) = \varphi(1) + \varphi(1) + \ldots + \varphi(1)_{p-1} = 1+1+\ldots+1_{p-1}$. So φ is the identity map.

2. Give an example of an infinite K where ϕ does not map onto K.

   From previous HW1, we found an example of an infinite field with prime characteristic, which is $F_p(X) = \left\{ \frac{f}{g} \mid f, g \in F_p[x], g \neq 0 \right\}$. We let k to be this field, and x be a non-constant monic polynomial. Then $\varphi(x) = x^p$ is of degree $p\deg(x)$, but no polynomial of degree 1 to $p-1$ is in the image of φ.

Exercise 7.2. Determine $\mathrm{Aut}(\mathbb{Q})$ and $\mathrm{Aut}(\mathbb{Z}_p)$.

As a first step, we observe that any automorphism of K must fix 0 and 1 (i.e., map 0 and 1 to themselves), and hence by a trivial induction must fix the prime subfield of K.

Suppose, let $\varphi \in \mathrm{Aut}(\mathbb{Q})$. Then, $\varphi(1) = 1$ and $\varphi(-1) = -1$. This is because any automorphism must preserve the identity element and the inverse element. For all $n \in \mathbb{N}$, $\varphi(n) = n$ and similarly, $\varphi(-n) = -n$. This follows from the fact that any rational number can be expressed as a sum of 1's or -1's. For $m, n \in \mathbb{Z}$ and $n \neq 0$, $\varphi(\frac{m}{n}) = \frac{m}{n}$. This is shown by breaking down $\frac{m}{n}$ into $\varphi(m) \cdot \varphi(n)^{-1}$, and since $\varphi(m) = m$ and $\varphi(n) = n$, it simplifies to $\frac{m}{n}$.As a result, $\mathrm{Aut}(\mathbb{Q})$ is the trivial group.

Suppose, let $\varphi \in \mathrm{Aut}(\mathbb{Z}_p)$. For any automorphism φ in $\mathrm{Aut}(\mathbb{Z}_p)$, it must preserve the identity element, which is 1 in $\mathbb{Z}_p$. Therefore, $\varphi(1) = 1$. Similarly, $\varphi(-1) = -1$, as φ must also preserve the inverse element of 1. For any nonzero element $a \in \mathbb{Z}_p$, it generates the entire group $\mathbb{Z}_p$. Thus, any automorphism must preserve the generators. So, $\varphi(a)$ must also be a generator of $\mathbb{Z}_p$. Since every element in $\mathbb{Z}_p$ except for 0 is a generator, $\varphi(a)$ can be any nonzero element in $\mathbb{Z}_p$ for any nonzero generator a. Hence, φ is completely determined by its action on the nonzero elements of $\mathbb{Z}_p$. Given the nature of $\mathbb{Z}_p$, where every nonzero element is a generator, the number of possible automorphisms is $\varphi(p-1)$, where φ is Euler's totient function. $\varphi(p-1)$ counts the number of elements relatively prime to $p-1$ in the range $[1, p-1]$. Thus, $\mathrm{Aut}(\mathbb{Z}_p)$ has $\varphi(p-1)$ automorphisms. So, the automorphism group of $\mathbb{Z}_p$, $\mathrm{Aut}(\mathbb{Z}_p)$, has $\varphi(p-1)$ automorphisms, where φ is Euler's totient function.

Exercise 7.6. Describe the Galois group $\mathrm{Gal}(GF(8) : \mathbb{Z}_2)$.

The Galois group of the field extension GF(8), and Z2 is the group of automorphisms of the field extension. So, GF(8) is the finite field with 8 elements and Z2 is the field with 2 elements.

The field GF(8) can be represented as the splitting field of the polynomial x^3+x+1 over Z2. $GF(8)$ is $\mathbb{Z}_2[X]/(X^3+X+1)$. The Galois group of x^3+x+1 over Z2 has order 3, as the polynomial is irreducible over Z2 and hence has 3 distinct roots in its splitting field. Since the Galois group has order 3, it must be isomorphic to Z_3, the cyclic group of order 3.

If $\alpha = X + (X^3 + X + 1)$, then we may write $GF(8)$ as $\mathbb{Z}_2(\alpha)$, and the elements of $GF(8)$ are $0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2$. The powers of α are given by:

n	1	2	3	4	5	6	7
α^n	α	α^2	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$1+\alpha^2$	1

Since $\alpha^3+\alpha+1 = 0$, it follows, by squaring, that $\alpha^6+\alpha^2+1 = 0$, and so α^2 is also a root of $X^3 + X + 1$. Squaring again, we see that $\alpha^4 = \alpha + \alpha^2$ is again a root of $X^3 + X + 1$. Any $\mathbb{Z}_2$-automorphism must map a root of $X^3 + X + 1$ to another root. Accordingly, there are three elements in $\mathrm{Gal}(GF(8), \mathbb{Z}_2)$:

$\iota : \alpha \mapsto \alpha$, $\phi : \alpha \mapsto \alpha^2$, $\psi : \alpha \mapsto \alpha + \alpha^2$,

and the multiplication table is:

$\cdot$	ι	ϕ	ψ
ι	ι	ϕ	ψ
ϕ	ϕ	ψ	ι
ψ	ψ	ι	ϕ

Exercise 7.7. Let L be a normal extension of a field K, and let E be a subfield of L containing K. Show that L is a normal extension of E.

By **Theorem 7.13**, A finite extension L of a field K is normal if and only if it is a splitting field for some polynomial in $K[X]$. Therefore, since L is a normal extension of K, it is a splitting field for some polynomial f in $K[X]$. Since $f \in E[X]$, we conclude that L is a normal extension of E.

5. Prove that if p is prime, then the Galois group of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ is cyclic of order $p-1$, where $\omega = e^{\frac{2\pi i}{p}}$. (Optional: Generalize to the case when p is not prime.)

The complex number $\omega = e^{\frac{2\pi i}{p}}$ is a root of the polynomial $f(x) = x^p - 1$. This can be seen by noticing that $\omega^p = \left(e^{\frac{2\pi i}{p}}\right)^p = e^{2\pi i} = 1$.

We show that all the roots of $f(x) = x^p - 1$ are different, we can look at the derivative $f'(x)$:

$$f'(x) = p \cdot x^{p-1}$$

Since p is prime, $f'(x)$ has no common factors with $f(x)$. Therefore, $f(x)$ has no repeated roots, and all its roots are distinct.

Let's observe $(\omega^k)^p$:

$$(\omega)^p = e^{2\pi i \cdot \frac{kp}{p}} = e^{2\pi i k}$$

Since $e^{2\pi i k}$ represents the rotations on the complex plane, $(\omega^k)^p = 1$ for all integers k.Now, since all the roots of $f(x)$ are distinct and ω^k for $k = 1, 2, ..., p-1$ are $p-1$ distinct roots of $f(x)$, the degree of the extension $\mathbb{Q}(\omega) : \mathbb{Q}$ is $p-1$. Also, since ω generates all the roots of $f(x)$, $\mathbb{Q}(\omega)$ is the splitting field of $f(x)$ over $\mathbb{Q}$. Since ω satisfies $x^p - 1 = 0$ and generates the extension, $\mathbb{Q}(\omega)$ is cyclic.Therefore, $[\mathbb{Q}(\omega) : \mathbb{Q}] = p-1$, $\mathbb{Q}(\omega)$ is the splitting field of $f(x)$ over the rationals, and the extension is cyclic.

6.

(a) Let K be a finite field. Show that K is a simple extension of $\mathbb{Z}_p$.

The following requires two properties:

1. A finite field of order q exists if and only if q is a prime power p^k, where p is prime and k is a positive integer.

2. Finite fields of the same order are isomorphic to each other.

Since K is a finite field, it has order p^n for some positive integer n.

Let α be an element in K that is not in $\mathbb{Z}_p$. Such an element exists because if K were the same as $\mathbb{Z}_p$, then K wouldn't be a field (as the characteristic of K would be zero, not p). Consider the subfield of K generated by α and $\mathbb{Z}_p$, denoted $\mathbb{Z}_p(\alpha)$. Since K is finite, $\mathbb{Z}_p(\alpha)$ must also be finite. Now, $\mathbb{Z}_p(\alpha)$ is a field containing α and $\mathbb{Z}_p$, so it contains all polynomials in α with coefficients in $\mathbb{Z}_p$. Thus, $\mathbb{Z}_p(\alpha)$ contains at least p^n distinct elements (since each polynomial of degree less than n generates a distinct element in K). But since $\mathbb{Z}_p(\alpha)$ is a field of order p^m for some $m \leq n$ (the degree of the minimal polynomial of α over $\mathbb{Z}_p$ divides n), it must contain exactly p^m elements. Hence, $m = n$ and $\mathbb{Z}_p(\alpha)$ is actually all of K. Therefore, K is a simple extension of $\mathbb{Z}_p$ generated by α.

(b) Prove that there exists a prime number p and an irreducible polynomial $f \in \mathbb{Z}_p[x]$ such that $K \cong \mathbb{Z}_p[x]/(f)$.

In $\mathbb{Z}_p[x]$, which is a Euclidean domain, we can perform polynomial division. So, for any polynomial $q(x)$, there exist polynomials $a(x)$ and $r(x)$ such that $q(x) = a(x)f(x) + r(x)$, where $f(x)$ is a fixed polynomial (let's say irreducible) and $r(x)$ has degree less than n, the degree of $f(x)$. This means that when we divide $q(x)$ by $f(x)$, we obtain a quotient $a(x)$ and a remainder $r(x)$, with $r(x)$ being unique.

Now, in the quotient ring $\mathbb{Z}_p[x]/(f(x))$, we're essentially considering all polynomials in $\mathbb{Z}_p[x]$ modulo the ideal generated by $f(x)$. The elements of this quotient ring are equivalence classes of polynomials, where two polynomials are considered equivalent if their difference is divisible by $f(x)$.

The number of elements in $\mathbb{Z}_p[x]/(f(x))$ corresponds to the number of polynomials in $\mathbb{Z}_p[x]$ whose degree is strictly less than n, because every polynomial can be written uniquely as $a(x)f(x) + r(x)$ where $r(x)$ has degree less than n.

Now, each of these polynomials in $\mathbb{Z}_p[x]$ with degree less than n is uniquely determined by its coefficients. Since there are n coefficients, each taking one of the p values in $\mathbb{F}_p$, there are p^n possible combinations of coefficients. Thus, there are p^n distinct polynomials of degree less than n in $\mathbb{Z}_p[x]$, and therefore, $\mathbb{Z}_p[x]/(f(x))$ contains p^n elements.

(c) Prove that there exists an irreducible polynomial of every positive degree over $\mathbb{Z}_p$.

The multiplicative group of nonzero elements of any finite field is cyclic; so if K is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p[x]$, letting α be a generator of the multiplicative group of K, we have that $K = \mathbb{Z}_p(\alpha)$. In particular, the minimal polynomial of α over $\mathbb{Z}_p$, which is irreducible, must have the same degree as $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = [K : \mathbb{Z}_p] = n$, so there must exist an irreducible polynomial over $\mathbb{Z}_p$ of degree n.

7.

(a) Let $L : K$ be an extension of finite fields. Use the degree of the extension to show that if $|L| = p^n$ and $|K| = p^m$, then $m \mid n$.

Since L is a finite field extension of K, L is a finite-dimensional vector space over K. Let $[L : K] = n$, so L has dimension n over K. Thus, L has p^n elements. Similarly, K has dimension m over $\mathbb{F}_p$, so it has p^m elements.

Now, L is also an extension of $\mathbb{F}_p$ because K is. Thus, by the **Theorem 3.3** from Howie,

$$[L : \mathbb{F}_p] = [L : K] \cdot [K : \mathbb{F}_p] = n \cdot m.$$

But we know that the cardinality of L is p^n and the cardinality of $\mathbb{F}_p$ is p, so $|L| = p^n$.

Therefore, $n \cdot m = [L : \mathbb{F}_p] = \log_p |L| = \log_p p^n = n$, implying $m = 1$, which proves $m \mid n$.

(b) Prove that if $m \mid n$, then $(p^m - 1) \mid (p^n - 1)$.

Given $m|n$, there exists some $k \in \mathbb{Z}^+$ such that $n = mk$.

Since $p^m \equiv 1 \pmod{p^m - 1}$, we have

$$p^n = p^{mk} = (p^m)^k \equiv 1^k = 1 \pmod{p^m - 1}$$

This precisely means that $p^n - 1 \equiv 0 \pmod{p^m - 1}$, establishing the divisibility relationship $(p^m - 1)|(p^n - 1)$.

(c) Prove that if $m \mid n$, then $\mathrm{GF}(p^n)$ has a subfield with p^m elements.

With the zeros of $x^{p^n} - x$ are exactly the elements of a finite field with p^m elements. Since splitting fields are uniquely determined up to isomorphism, written as $\mathrm{GF}(p^n)$.

First, if m divides n, then $p^m - 1$ divides $p^n - 1$, and moreover $x^{p^n-1} - 1$ divides $x^{p^n} - 1$. Thus $x^{p^m} - x$ divides $x^{p^n} - x$. Hence, $\mathrm{GF}(p^m)$ is a subfield of $\mathrm{GF}(p^n)$.

** Conversely, if $\mathrm{GF}(p^m)$ is a subfield of $\mathrm{GF}(p^n)$, then $\mathrm{GF}(p^n)$ is a vector space over $\mathrm{GF}(p^m)$. Thus $p^n = (p^m)^k$ for some $k \geq 1$. Hence, m is a divisor of n.

8.

(a) In $\mathrm{GF}(p^n)$, show that the Frobenius automorphism $\phi : a \mapsto a^p$ has order n.

we can start by fixing every element of $\mathbb{F}_p$ by any automorphism because they are just sums of 1's. Then, for any nonzero element α in $\mathrm{GF}(p^n)$, $\alpha^{(p^n-1)} = 1$ due to Lagrange's theorem applied to the multiplicative group

of nonzero elements in $\mathrm{GF}(p^n)$. Hence, $\alpha^{p^n} = \alpha$ for all nonzero α in $\mathrm{GF}(p^n)$.

Suppose there exists some $m < n$ such that $\alpha^m = \alpha$ for all nonzero α in $\mathrm{GF}(p^n)$. Then, the field $\mathrm{GF}(p^n)$ would have only p^m elements, which contradicts the fact that it has p^n elements.

Since there is no smaller exponent $m < n$ for which $\alpha^m = \alpha$ holds for all nonzero α in $\mathrm{GF}(p^n)$, the order of the Frobenius automorphism must be n.

(b) Prove that the group of automorphisms of $\mathrm{GF}(p^n)$ is cyclic with order n.

Let's denote this automorphism group K. Firstly, K has $\mathbb{Z}_p$ as a subfield. Notice that if $f : K \to K$ is an automorphism, then it must be that f is the identity on $\mathbb{Z}_p$. This is because $f(1) = 1$ and $f(0) = 0$, and the elements of $\mathbb{Z}_p$ are obtained by adding 1's together: $0, 1, 1+1, 1+1+1, ..., p-1$. Thus, any automorphism of K is a $\mathbb{Z}_p$-automorphism. It follows that the automorphism group of K is the same as $\mathrm{Gal}(K/\mathbb{Z}_p)$.

Such K is a Galois extension of $\mathbb{Z}_p$ because all finite fields are isomorphic to $\mathrm{GF}(p^n)$ that it is a splitting field of the polynomial $h(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Thus, we can apply Galois theory. It follows that $\mathrm{Gal}(K/\mathbb{Z}_p)$ has order n since this is the dimension of K as a vector space over $\mathbb{Z}_p$.

Since every element of K is a zero of $h(x)$, it follows that $p^n = 1$. Suppose that p has an order strictly smaller than this d, say. Then $a^{p^d} = a$ for each a in K. But this means that the elements of K are all zeroes of a polynomial with degree p^d. In particular, K can have at most p^d elements, a contradiction. Thus, the Frobenius has the correct n order and the group is cyclic as required.