Fields

Patrick Dugan

1 Introduction

These are some results I found while trying to prove that $(Z/nZ)^*$ always has a generator for prime n. Also some assorted results that I bumped into while just exploring.

2 Notation

Kernel

$$\text{Where f is an automorphism : } H \rightarrow H$$

$$Ker(f) = \{x : x \in H, f(x) = e_H\}$$

Polynomial

$$deg(f) = \text{ the degree of polynomial f}$$

$$sol(f) = \text{ number of solutions of polynomial f}$$

3 Generator for field

F is a field with commutative multiplication
Let $F_\times$ denote the multiplicative group
Let $n = |F_\times|$ and $n = p_1^{m_1} p_2^{m_2} \ ... \ p_i^{m_i}$

3.1 Product

Since $F_\times$ is abelian we can break it up into kernels (Check my previous write up "kernels")

$$F_\times \cong Ker(x^{p_1^{m_1}}) \times Ker(x^{p_2^{m_2}}) \times ... \times Ker(x^{p_i^{m_i}})$$

3.2 $Ker(x^{p_i^{m_i}}) \cong C_{p_i^{m_i}}$

Let $A = Ker(x^{p_i^{m_i}})$
Assume that $A \ncong C_{p_i^{m_i}}$

$$\nexists g \in A \text{ such that } |g| = p_i^{m_i}$$

So

$$\text{For all x } \in A, \ |x| < p_i^{m_i}$$

Also

$$\text{For all x } \in A,\ |x| \text{ divides } |A| \ (|A| = p_i^{m_i})$$

Putting these to together

$$\text{For all x } \in A,\ |x| \text{ divides } p_i^{m_i - 1}$$

This means that

$$\text{For all x } \in A,\ x^{p_i^{m_i-1}} = 1$$

$f(x) = x^{p_i^{m_i-1}} - 1$

$$f(x) \text{ has a solution for every element in A}$$

This means

$$sol(f) \geq |A|$$
$$sol(f) \geq p_i^{m_i}$$

And also

$$deg(f) = p_i^{m_i-1}$$

So

$$deg(f) < sol(f)$$

Contradiction as

For all polynomials g with coefficients in a field $sol(g) \leq deg(g)$ (Check previous write up "Polynomials")

This means that

$$Ker(x^{p_i^{m_i}}) \cong C_{p_i^{m_i}}$$

3.3 $F_\times$ has a generator

$$F_\times \cong Ker(x^{p_1^{m_1}}) \times Ker(x^{p_2^{m_2}}) \times ... \times Ker(x^{p_i^{m_i}})$$

With 3.1

$$F_\times \cong C_{p_1^{m_1}} \times C_{p_2^{m_2}} \times ... \times C_{p_i^{m_i}}$$

products of coprime cyclic groups are cyclic

$$F_\times \cong C_n$$

So

$$\text{For any field with commutative multiplication } F,\ F_\times \text{ is cyclic}$$

4 Additive groups

F is a field with not necessarily commutative multiplication (I think there is a term for this)
F_+ denotes the additive group
1 is multiplicative identity

4.1 $< 1 >_+ \cong C_p$

Assume $|1|$ is composite

$$|1| = ab$$

let

$$x = \sum_{i=0}^{a} 1 \text{ and } y = \sum_{i=0}^{b} 1$$

Then

$$xy = \sum_{i=0}^{ab} 1 = 0$$

Since $x, y \in F_\times$ and $0 \notin F_\times$ this is a contradiction

$$|1| = p \text{ (prime)}$$

$$< 1 >_+ \cong C_p$$

4.2 For all x $|1|$ divides $|x|$

For all non zero $x \in F$

$$\sum_{i=0}^{|x|} x = 0$$

$$x \sum_{i=0}^{|x|} 1 = 0$$

$$\sum_{i=0}^{|x|} 1 = 0$$

$$|1| \text{ divides } |x|$$

4.3 For all x $|x| = p$

$$\sum_{i=0}^{|1|} 1 = 0$$

For all nonzero $x \in F$

$$\sum_{i=0}^{|1|} x = 0$$

$$|x| \text{ divides } |1|$$

In conjunction with 4.2 ad 4.1

$$|x| = |1| = p$$

4.4 $F_+ \cong {C_p}^m$

Since for all $x \in F_+$, $|x| = p$

$$< x >_+ \cong C_p$$

So F_+ can be split into disjoint subgroups of C_p

$$F_+ \cong C_p \times C_p \times \ \ldots \ \times C_p$$

5 Recap

For any field F with commutative multiplication

$$F_+ \cong {C_p}^m \text{ and } F_\times \cong C_{p^m - 1}$$

This is kinda cool because any field's addition can be represented as a vector space over C_p. Also the multiplication on a field is a set of liner transformations over that vector space (aka a matrix). So it seems that any field can be written as a field of matrices over C_p.