School of Mathematics and Statistics

MT5836 Galois Theory

Handout V: Finite Fields

5 Finite Fields

Construction of finite fields

Proposition 5.1 *A finite field F has order p^n where p is a prime number equal to the characteristic of F and where n is the degree of F over its prime subfield $\mathbb{F}_p$.*

Lemma 5.2 *Let F be a finite field of order $q = p^n$ and characteristic p. Then*

(i) $a^{q-1} = 1$ *for all* $a \in F \setminus \{0\}$*;*

(ii) ***("Freshman's Exponentiation")***

$$(a + b)^{p^k} = a^{p^k} + b^{p^k}$$

for all $a, b \in F$ and non-negative integers k.

Theorem 5.3 *Let p be a prime number and n be a positive integer. Then there is precisely one field of order p^n up to isomorphism.*

Definition 5.4 The (unique) field of order p^n is denoted $\mathbb{F}_{p^n}$ and is often called the *Galois field* of order p^n.

The multiplicative group of a finite field

Definition 5.6 The *exponent* of a finite group is the least common multiple of the orders of elements of G.

Lemma 5.7 *Let G be a finite abelian group with exponent ν. Then there exists some $g \in G$ of order ν.*

Theorem 5.8 *The multiplicative group of a finite field is cyclic.*

Corollary 5.9 *Let $F \subseteq K$ be an extension of finite fields. Then $K = F(\alpha)$ for some $\alpha \in K$.*