Section V.5. Finite Fields

Note. In this section, as Hungerford states (on page 278) "finite fields...are characterized in terms of splitting fields and their structure completely determined." We also present a result to give a clear classification of finite groups in terms of their order and characteristic.

Theorem V.5.1. Let F be a field and let P be the intersection of all subfields of F. Then P is a field with no proper subfields. If $\text{char}(F) = p$ (where p is prime), then $P \cong \mathbb{Z}_p$. If $\text{char}(F) = 0$ then $P \cong \mathbb{Q}$.

Note. The field P of Theorem V.5.1 is called the *prime subfield* of field F. Notice that it is the "smallest" subfield of F. So $\mathbb{Z}_p$ is a subfield of every field of characteristic p and $\mathbb{Q}$ is a subfield of every field of characteristic 0 (up to isomorphism). Notice that this implies that there is no proper subfield of $\mathbb{Q}$ (up to isomorphism...$2\mathbb{Q}$ is technically a subfield).

Corollary V.5.2. If F is a finite field, then $\text{char}(F) = p \neq 0$ for some prime p and $|F| = p^n$ for some $n \in \mathbb{N}$.

Theorem V.5.3. If F is a field and G is a finite subgroup of the multiplicative group of nonzero elements of F, then G is a cyclic group. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Corollary V.5.4. If F is a finite field, then F is a simple extension of its prime subfield $\mathbb{Z}_p$; that is, $F = \mathbb{Z}_p(u)$ for some $f \in F$. (Notice Hungerford's comment on page 279 that we do not distinguish between $P \cong \mathbb{Z}_p$ and $P = \mathbb{Z}_p$ in term of the prime subfield.)

Note. The next two results will allow us to clearly classify finite fields in Corollary V.5.7.

Lemma V.5.5. If F is a field of characteristic p and if $r \geq 1$ is an integer, then the map $\varphi : F \to F$ given by $u \mapsto u^{p^r}$ is a $\mathbb{Z}_p$-monomorphism of fields. If F is finite, then φ is a $\mathbb{Z}_p$-automorphism of F.

Note. The following is a classification of finite fields in terms of splitting fields.

Proposition V.5.6. Let p be a prime and $n \geq 1$ an integer. Then F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Corollary V.5.7. If p is a prime and $n \in \mathbb{N}$, then there exists a field with p^n elements. Any two finite fields with the same number of elements are isomorphic.

Proof. Given p and n, a splitting field F of $x^{p^n} - x$ over $\mathbb{Z}_p$ exists by Theorem V.3.2. By Proposition V.5.6, this splitting field has order p^n. Since every finite field of order p^n is a splitting field of $x^{p^n} = x$ over $\mathbb{Z}_p$ by Proposition V.5.6 (it is an if-and-only-if result), any two such fields are isomorphic by Corollary V.3.9. ∎

Corollary V.5.8. If K is a finite field and $n \in \mathbb{N}$, then there exists a simple extension field $F = K(U)$ of K such that F is finite and $[F : K] = n$. Any two n-dimensional extension fields of K are K-isomorphic.

Note. The following result implies that no finite field is algebraically closed. We leave the proof as an exercise.

Corollary V.5.9. If K is a finite field and $n \in \mathbb{N}$, then there exists an irreducible polynomial of degree n in $K[x]$.

Proposition V.5.10. If F is a finite dimensional extension field of a finite field K, then F is finite and is Galois over K. The Galois group $\mathrm{Aut}_K(F)$ is cyclic.

Note. By Corollary V.5.2, if F is a finite field then $|F| = p^n$ for some prime p and some $n \in \mathbb{N}$. In addition, as seen in the proof of Corollary V.5.2, $F \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$. By theorem V.5.3, the multiplicative group of all nonzero elements of a finite field is cyclic. I summarize this as (my choice of title):

> **Fundamental Theorem of Finite Fields.** A finite field of order m exists if and only if $m = p^n$ for some prime p and some $n \in \mathbb{N}$. All fields of order p^n are isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (that is, elements add as n-tuples of elements of $\mathbb{Z}_p$). As a group under multiplication, the set of nonzero elements forms a cyclic group of order $m - 1 = p^n - 1$ and so is isomorphic to the group $\mathbb{Z}_{p^n-1}$.

Note. For an example of a finite field of order $16 = 2^4$, see my class notes for Introduction to Modern Algebra 2 (MATH 4137/5137):

`http://faculty.etsu.edu/gardnerr/4127/notes/VI-33.pdf`

This example is based on results from Chapter 22, "Finite Fields," in Joseph Gallian's *Contemproary Abstract Algebra* 8th Edition, Brooks/Cole (2013).

Revised: 1/1/2016