

22 Chapter: Finite Fields

For every prime p and every positive integer n there is one and only one field (up to isomorphism) of order p^n . [Gallian, Theorem 22.1] This field is denoted in GAP by $\text{GF}(p^n)$. The set of nonzero elements in $\text{GF}(p^n)$ form a cyclic group under multiplication of order $p^n - 1$. [Gallian, Theorem 22.2] GAP denotes a generator of this cyclic group by $Z(p^n)$ and the remaining elements of $\text{GF}(p^n)$ are expressed in terms of $Z(p^m)$ for m a divisor of n . For example, the following defines F to be the field $\text{GF}(16)$ and then lists the elements in F :

```
gap> F:=GF(2^4);
GF(2^4)
gap> Elements(F);
[ 0*Z(2), Z(2)^0, Z(2^2), Z(2^2)^2, Z(2^4), Z(2^4)^2, Z(2^4)^3, Z(2^4)^4,
Z(2^4)^6, Z(2^4)^7, Z(2^4)^8, Z(2^4)^9, Z(2^4)^11, Z(2^4)^12, Z(2^4)^13,
Z(2^4)^14 ]
```

Careful: $Z(p^n)^m$ is not the same as $Z(p^{mn})$. The element $Z(p^n)$ is an element in $\text{GF}(p^n)$ of multiplicative order $p^n - 1$ and $Z(p^n)^m$ is the m th power of this element. The element $Z(p^{mn})$ is an element in $\text{GF}(p^{mn})$ of multiplicative order $p^{mn} - 1$.

```
gap> Order(Z(2^6));
63
gap> Order(Z(2^2)^3);
1
```

To understand the GAP notation think of the multiplicative group of nonzero elements in $\text{GF}(16)$ as generated by a . That is, $\text{GF}(16) = \{0, 1, a, a^2, \dots, a^{14}\}$. The field $\text{GF}(p^n)$ has one and only one subfield of order p^m for every integer m that divides n . [Gallian, Theorem 22.3] Thus $\text{GF}(16)$ has a unique subfield of order 2 and a unique subfield of order 4. The subfield of order 2 is $\{0, 1\}$ and the subfield of order 4 is $\{0, 1, a^5, a^{10}\}$. In the GAP notation $Z(2^4) = a$, $Z(2^2) = Z(2^4)^5 = a^5$, and $Z(2^2)^2 = a^{10}$. We can use GAP to test this as follows:

```
gap> Z(2^2) = Z(2^4)^5;
true
gap> Z(2^2)^2 = Z(2^4)^10;
true
```

The command $\text{DegreeFFE}(Z(p^n)^m)$, for p a prime and m and n positive integers, returns the degree of the smallest field containing $Z(p^n)^m$ over $\text{GF}(p)$. For example:

```
gap> DegreeFFE(Z(2^4));
4
gap> DegreeFFE(Z(2^4)^3);
4
gap> DegreeFFE(Z(2^4)^5);
2
```

The GAP commands, discussed in Chapter 21 of this manual, for defining fields by adjoining zeros of irreducible polynomials also work over finite fields. For example, we can create a field of order 16 in GAP [See Gallian, Chapter 22, Example 1]:

```
gap> x:= X(GF(2), "x");;
gap> f:= x^4+x+1;
x^4+x+Z(2)^0
gap> IsIrreducible(f);
true
gap> F:= AlgebraicExtension(GF(2),f);
<field of size 16>
```

Exercises

22.1 Using GAP, find the degree of the smallest field containing $Z(2^4)^m$ over $GF(2)$ for $m = 1, 2, 3, \dots, 10$. For which values of m is this degree strictly less than 4?

22.2 Find the multiplicative orders of $Z(2^4)^m$ for $m = 1, 2, 3, \dots, 10$.

22.3 Using GAP, find the degree of the smallest field containing $Z(3^3)^m$ over $GF(3)$ for $m = 1, 2, 3, \dots, 15$. For which values of m is this degree strictly less than 3?

22.4 Find the multiplicative orders of $Z(3^3)^m$ for $m = 1, 2, 3, \dots, 15$.

22.5 Under what condition will the degree of the smallest field containing $Z(p^n)^m$ over $GF(p)$ equal n ? Under what condition will this degree be less than n ?

22.6 Using GAP factor the polynomial $x^{3^n} - x$ over $GF(3)$ for $n = 2, 3$ and 4. For each n , what was the largest degree of an irreducible factor?

22.7 Using GAP factor the polynomial $x^{5^n} - x$ over $GF(5)$ for $n = 2$ and 3. For each n , what was the largest degree of an irreducible factor?

22.8 Make a conjecture concerning the largest degree of any irreducible factor of $x^{p^n} - x$ over $GF(p)$.

22.9 Prove your conjecture in Exercise 22.8. [Gallian, Chapter 22, Exercise 24]

22.10 a) Construct a field of order 32 using GAP by adjoining a zero of an appropriate irreducible polynomial over $GF(p)$ to $GF(p)$ for some prime p .

b) Construct a field of order 81 using GAP by adjoining a zero of an appropriate irreducible polynomial over $GF(p)$ to $GF(p)$ for some prime p .