

## Pries: M466-Groups, Rings, and Fields

### Homework 9: Finite Fields.

Due Wednesday 10/17

**Read:** Gallian 22, Reid 3.4, Wilkons 4.11

The field of size  $q = p^n$  is called  $\mathbb{F}_q$  by Reid and called  $\text{GF}(p^n)$  by Gallian. Also  $\mathbb{F}_p \simeq \mathbb{Z}/p$ .

### Problems:

- In the ring  $R = (\mathbb{Z}/5)[x]$ , let  $f(x) = x^2 + 2$  and let  $I = (f(x))$ .
  - Show that  $\mathbb{F} = R/I$  is a field.
  - If  $\beta \in \mathbb{F}^*$ , find a small list of possibilities for the order of  $\beta$ .
  - Let  $\alpha$  be the coset of  $x$  in  $R/I$ . Using (ii), show that  $\beta = \alpha + 1$  generates  $\mathbb{F}^*$ .
- Draw the lattice of subfields of  $\mathbb{F}_{p^{20}}$ .
- If  $m$  divides  $n$ , show that  $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$ .
- What is the smallest field  $\mathbb{F}$  that contains exactly 6 subfields (including itself)?
  - Count the number of monic degree two polynomials in  $(\mathbb{Z}/p)[x]$ .
  - Show there are  $p(p-1)/2$  irreducible monic degree two polynomials in  $(\mathbb{Z}/p)[x]$ .
- Let  $\tau : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$  be the map given by  $\tau(a) = a^p$  for all  $a \in \mathbb{F}_{p^n}$ .
  - Show that  $\tau$  is a ring homomorphism.
  - What is the order of  $\tau$ ?  
(in other words, what is the smallest positive integer  $e$  so that  $\tau^e = \text{id}$ )?
  - Find an inverse map for  $\tau$  (thus  $\tau$  is an automorphism).
  - Show that  $\tau(a) = a$  if and only if  $a \in \mathbb{F}_p$ .
- (harder) An element  $a \in \mathbb{F}_q$  is a *non-square* of  $\mathbb{F}_q$  if  $a \neq b^2$  for any  $b \in \mathbb{F}_q$ .
  - How many non-squares are there in  $\mathbb{F}_q$ ?
  - Suppose  $a$  is a non-square of  $\mathbb{F}_p$ . Show that  $a$  is a non-square of  $\mathbb{F}_{p^n}$  if and only if  $n$  is odd.