Exercise sheet 1
Date: 20 September 2013

Exercise 1  Prime field examples
(a) Compute the multiplication table for \( \mathbb{F}_5 \). Show that \( \mathbb{F}_5^* \) is cyclic and give a generator.
(b) In \( \mathbb{F}_{79} \), compute \( 33 + 57 + 68, 5 \cdot 50, 41 \cdot 27, \frac{1}{20}, \) and \( \frac{3}{27} \).
(c) In \( \mathbb{F}_{1291} \), find the multiplicative inverses of 2, 6, and 538.

Exercise 2  Non-prime field examples
(a) Show that \( x^3 + x + 1 \) is irreducible over \( \mathbb{F}_2 \).
(b) List all elements of \( \mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1) \).
(c) Compute \((x + x^2) + (1 + x^2)\) and \((x + x^2) \cdot (1 + x^2)\) in \( \mathbb{F}_8 \).
(d) Show that \( \mathbb{F}_8^* \) is cyclic and find a generator.

Exercise 3  Square roots of unity in \( \mathbb{F}_q \)
Find all \( a \in \mathbb{F}_q \) such that \( a^2 = 1 \).

Exercise 4  Fermat’s Little Theorem
Let \( p \) be a prime and \( a \) an integer not divisible by \( p \). Show that \( a^{p-1} \equiv 1 \mod p \).

Exercise 5  Equation of \( \mathbb{F}_q \)
(a) Let \( \mathbb{F}_q \) be any finite field. Show that \( a^q = a \) for all \( a \in \mathbb{F}_q \).
(b) Now write \( q = p^n \) for \( p \) a prime. Deduce from (a) that \( \mathbb{F}_q \) is the splitting field of \( t^q - t \) over \( \mathbb{F}_p \).

Exercise 6  Subfields, intersection, and compositum
(a) Show that \( \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \) if and only if \( m \mid n \).
(b) Characterize the intersection \( \mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} \) and the compositum \( \mathbb{F}_{p^m} \mathbb{F}_{p^n} \).

Exercise 7  Every finite integral domain is a field
(a) Recall the definition of an integral domain. How is it different from a field?
(b) Show that every finite integral domain is a field.

Exercise 8  Wilson’s Theorem
Let \( p \) be prime. Show that \( p \) divides \((p - 1)! + 1 \).