

HOMEWORK 1-2. DUE FRIDAY APRIL 11

HAND IN: 7.2.5, 7.2.8, 7.3.3, 7.3.5, 7.3.6, 7.3.7.

AND

1. (i) Prove: If $p \neq 2$ is prime, then \mathbb{Z}_p has an element a satisfying $a^2 = -1$ if and only if $p \equiv 1 \pmod{4}$; in that case there are exactly two such elements a of \mathbb{Z}_p .
(ii) Prove: If p is prime, then \mathbb{Z}_p has an element $a \neq 1$ satisfying $a^3 = 1$ if and only if $p \equiv 1 \pmod{3}$; in that case, there are exactly two such elements. **Also** show in this case that there are two elements $b \in \mathbb{Z}_p$ such that $b^2 = -3$.
(iii) Prove: If p is prime, then \mathbb{Z}_p has an element a satisfying $a^9 = -1$. How many such elements a are there?
2. (i) Find all irreducible polynomials over \mathbb{Z}_2 of degree 4.
(ii) Find all monic irreducible polynomials over \mathbb{Z}_3 of degree 3.
3. (i) Let L be a finite field and K a subfield, with $|L| = p^n$ for a prime p . Prove: $|K| = p^m$ where $m|n$, and $\dim_K(L) = n/m$.
(ii) Conversely, if $m|n$ prove that L has one and only one subfield of size p^m .
(iii) If K_1 and K_2 are subfields of L , where $|K_1| = p^a$ and $|K_2| = p^b$, find $|K_1 \cap K_2|$.
4. Exactly how many subfields are there in a field of size 7^{60} ? Why?

DO NOT HAND IN: 7.2.1, 7.2.2, 7.2.4, 7.2.7, 7.3.1.

AND

5. (i) Let $g \in \mathbb{Z}_p[x]$ be irreducible of degree d . Prove: $g \mid x^{p^n} - x$ if and only if $d|n$. (ii) Prove: $x^{p^n} - x$ is the product of ALL irreducible polynomials in $\mathbb{Z}_p[x]$ of degree dividing n .