HOMEWORK 5. DUE FRIDAY FEBRUARY 22

HAND IN: 6.6.3, 6.6.5, 6.7.2, 6.7.3, 6.8.2, 6.8.4 AND

1. Let $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$.

(i) Describe the quotient ring $A = \mathbb{Z}_2[x]/(f)$: write down its 4 elements, write down 4×4 tables describing its addition and multiplication.

(ii) Show that A is a field.

2. Let $K = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}_3 \right\}$ Prove:

(i) K is a field;

(ii) K has exactly 9 elements; and

(iii) $K^\times$ is a cyclic group of order 8.

3. Let $A = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}_5 \right\}$, a subset of the ring of all 2×2 matrices with entries in $\mathbb{Z}_5$.

(i) Prove: A is a ring having exactly 25 elements, but it is not an integral domain and is not a field.

(ii) What happens if 5 is replaced by 7? 11? 13? 17? 19? Compare with question #2. Do you see a similarity with $\mathbb{C}$?

DO NOT HAND IN: 6.6.1, 6.6.2, 6.6.4, 6.7.1, 6.7.5, 6.8.1, 6.8.6 AND

4. (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?