Modern Algebra II, Spring 2015

Homework 8, due Wednesday April 1

What to read: Rotman Appendix C pages 129-137; P.Gallagher §16
Finite fields.

1. Which of the following numbers are constructible using a ruler and compass?
\[
\frac{1}{3} \sqrt[3]{3} \quad \sqrt{5 + \sqrt{7}} \quad \sqrt[5]{5} - 1 \quad \sqrt{2} + 2.
\]

2. Suppose we have a ruler and compass, as before, but are given 3 points \(A, B, C\) on a line in the plane, with \(B\) between \(A\) and \(C\) and distances \(|AB| = 1\), \(|BC| = \sqrt{2}\). Explain how to modify the arguments in Monday’s lecture to show that \(\sqrt{2}\) is not constructible with these assumptions. (Hint: What are the properties of the tower of fields \(\mathbb{Q} \subset K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n\) where the field \(K_i\) is generated by the coordinates of \(A, B, C\) and of the next \(i\) points that we create? What can you say about the degree \([K_n : \mathbb{Q}]?\)

3. Write down a factorization of the polynomial \(f(x)\) into the product of irreducibles over the field \(\mathbb{F}_p\), where
   (a) \(f(x) = x^9 - x\) and \(p = 3\),
   (b) \(f(x) = x^p - 2\) and \(p\) is any prime number.
   (c) \(f(x) = x^{16} - x\) and \(p = 2\) (Hint: first solve problem 5(a)).

4. (a) List all elements of Galois groups \(\text{Gal}(\mathbb{F}_{64}/\mathbb{F}_8), \text{Gal}(\mathbb{F}_{27}/\mathbb{F}_3)\).
   (b) How many subfields (including itself) does the field \(\mathbb{F}_{4096}\) have?

5. (a) Find all irreducible polynomials of degree 4 over \(\mathbb{F}_2\).
   (b) Choose one of the polynomials \(f(x)\) from part (a) and consider a particular realization of \(\mathbb{F}_{16}\) as \(\mathbb{F}_2[\theta]/(f(\theta))\). Compute the orbit of \(\theta\) under the action of the Galois group \(G = \text{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)\).

6. (a) Explain why the field \(\overline{\mathbb{F}}_p\) that we defined on Wednesday, the algebraic closure of \(\mathbb{F}_p\), has countably many elements.
   (b) Show that the group \(\overline{\mathbb{F}}_p^\times\) of invertible elements is not cyclic.
   (c) Show that the Frobenius map \(a \mapsto a^p\) is an automorphism of \(\overline{\mathbb{F}}_p\) of infinite order.
Additional practice problems, won’t be graded.

7. Find all degree two monic irreducible polynomials over the field $\mathbb{F}_4$.

8. Determine the number of monic irreducible polynomials of (a) degree 4, (b) degree 6 over the field $\mathbb{F}_p$. 