Modern Algebra II, fall 2020, Instructor M.Khovanov

Homework 11, due Wednesday November 25.

1. (15 points) 1. Which of the following numbers are constructible using a ruler and compass? Briefly justify your answer.

$$\frac{1}{2}\sqrt[3]{3}, \qquad \sqrt{6+\sqrt{7}}, \qquad \sqrt[4]{5}-1, \qquad \sqrt[6]{2}+1.$$

2. (10 points) Briefly sketch the steps involved into constructing numbers $\sqrt{\sqrt{2}+1}$ and $\sqrt{\sqrt{\sqrt{2}+\sqrt{3}}+1}$ using a ruler and compass.

3. (20 points) 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 $|AB| = 1$, $|BC| = \sqrt[3]{2}$. Explain how to modify the arguments in Monday's lecture to show that $\sqrt[5]{2}$ 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 $[K_n : \mathbb{Q}]$?)

4. (20 points) We mentioned in class that $x^4 + 1$ is irreducible over $\mathbb{Q}$. Prove this using the substitution $x = y + 1$. Check that the same argument shows irreducibility of $x^{2^n} + 1$ over $\mathbb{Q}$ for any any n. (Hint: reduce coefficients modulo two to prove that they are even and use the Eisenstein criterion.) Explain how to use this result to check that the splitting field E of $x^{2^{n+1}} - 1$ over $\mathbb{Q}$ has degree 2^n. How many primitive 2^{n+1}-th roots of unity are there in E? What is the size of the Galois group $G = \mathrm{Gal}(E/\mathbb{Q})$? Explain why the Galois group is abelian.

5. (15 points) Recall the arguments from the lecture that $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to $C_2 \times C_2$, where E is the splitting field of $x^4 + 1$, and write a proof of this result in your own words. Explain how the Galois correspondence between intermediate fields and Galois groups works in this example.

6. (20 points) (a) Recall the properties of Euler's phi function $\phi(n)$. Prove that $\phi(p^n) = p^n - p^{n-1}$ for a prime p. Write down explicitly groups of invertible elements $\mathbb{Z}_5^*$, $\mathbb{Z}_7^*$, $\mathbb{Z}_8^*$. What result do we use to conclude that the first two groups are cyclic? Alternatively, you can find explicit generators for these groups.
(b) Check that the group $\mathbb{Z}_8^*$ is not cyclic. Can you use this result to show that $\mathbb{Z}_{2^n}^*$ is not cyclic for any $n \geq 3$? (Hint: set up a surjective ring homomorphism $\mathbb{Z}_{2^n} \longrightarrow \mathbb{Z}_8$ and investigate the effect of this homomorphism on the groups of invertible elements of these two rings.)

7. (20 points) (a) Explain why the field $\overline{\mathbb{F}}_p$ that we defined in the last lecture, the algebraic closure of $\mathbb{F}_p$, has countably many elements.
(b) Show that the group $\overline{\mathbb{F}}_p^*$ 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.
(d) Show that the group $\overline{\mathbb{F}}_p^*$ of invertible elements does not contain a cyclic group of order p. Hint: such a cyclic group would consists of p-th roots of unity. What can we say about p-th roots of unity in a finite field $\mathbb{F}_q$, $q = p^n$?

8. [This is a review exercise to recall finite fields and factorizations of polynomials over $\mathbb{F}_p$, do not write down a solution.]
(a) What do we know about factorization of the polynomial $x^{p^n} - x$ over the prime field $\mathbb{F}_p$? How does it factor in the special case $x^p - x$?
(b) Write down a factorization of the polynomial $f(x)$ into the product of irreducibles over the field $\mathbb{F}_p$, where
(1) $f(x) = x^9 - x$ and $p = 3$,
(2) Recall that any element a of $\mathbb{F}_p$ has a p-th root in $\mathbb{F}_p$. Why? How can we factor the polynomial $f(x) = x^p - 2$ over $\mathbb{F}_p$ if we are given $b \in \mathbb{F}_p$ such that $b^p = a$?

9. [another review exercise, do not submit] Find all monic irreducible polynomials of degree two over the field $\mathbb{F}_4$. For this exercise, first choose an explicit model of $\mathbb{F}_4$ as $\mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$. How can one list all monic degree two polynomials over $\mathbb{F}_4$? You'd then need to exclude reducible polynomials.

The midterm will also cover field extensions (degree of the extension, algebraic versus transcendental extensions), isomorphisms of fields and how they extend to larger fields, finite fields, Gauss lemma, Eisenstein criterion, and the technique from homework to check for roots in $\mathbb{Q}$ of a polynomial in $\mathbb{Z}[x]$. Separable and normal extensions and splitting fields. Examples of field extensions, their degrees and Galois groups. Galois main theorem and Galois correspondence between intermediate fields and subgroups of the Galois group. Euler's phi function and cyclotomic extensions. Algebraic closure of $\mathbb{F}_p$.
Please use Friedman notes "Galois theory I" and his earlier notes, posted on our website, for a review. Rotman's book is another resource.
If you'd like to see a more involved example of Galois groups and Galois correspondence, take a look at Friedman's notes "Galois theory III" (link on the website). In the middle of these notes he works out the correspondence for the splitting field of $x^4 - 2$ over $\mathbb{Q}$, with the dihedral group D_4 as the Galois group. There are more choices there for subgroups and subfields than in the examples worked out in class. It's an excellent practice to go through his arguments and fill in the details.