Modern Algebra II, fall 2020, Instructor M.Khovanov

Homework 8, due Wednesday November 4.

1. (30 points) In class we wrote down the finite field $\mathbb{F}_{16}$ as $\mathbb{F}_2[\alpha]/(\alpha^4+\alpha+1)$, using one of the three irreducible degree 4 polynomials over $\mathbb{F}_2$ (necessarily monic, since $\mathbb{F}_2$ has only two elements). We found the subfield isomorphic to $\mathbb{F}_4$ and discussed the orbit of the Galois group $G = \mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)$ action that contains the element α (Frobenius automorphism σ generates this group). Elements in the orbit give all roots of x^4+x+1 in $\mathbb{F}_{16}$ and allow us to factor this polynomial into linear terms in $\mathbb{F}_{16}$. See our class notes posted online (lecture 14) for details.

(a) Pick one of the elements in $\mathbb{F}_{16}$ we have not considered. Write down powers of this element in the basis $(1, \alpha, \alpha^2, \alpha^3)$ until you find a linear relation on the powers. You should get one of the other two irreducible degree four polynomials over $\mathbb{F}_2$. Using the Frobenius automorphism, find all roots of this polynomial and write down its factorization in $\mathbb{F}_{16}$. This allows you to collect four more elements of $\mathbb{F}_{16}$ into an orbit of the Galois group action.

(b) Check that the remaining four elements of $\mathbb{F}_{16}$ are roots of the third irreducible polynomial on our list and that they constitute the remaining orbit of the Galois group action. Extend the diagram we drew in the notes of elements of $\mathbb{F}_{16}$ and the action of the Frobenius on them to all elements of $\mathbb{F}_{16}$ (our diagram contained only 8 elements).

(c) Consider the field $\mathbb{F}_4 \cong \mathbb{F}_2[\beta]/(\beta^2+\beta+1)$. Check that the polynomial $g(x) = x^2 + x + \beta \in \mathbb{F}_4[x]$ is irreducible. Recall the embedding $\mathbb{F}_4 \subset \mathbb{F}_{16}$ that takes β to $\alpha+\alpha^2$. Can you find the roots of $g(x)$ in $\mathbb{F}_{16}$ and factor it in $\mathbb{F}_{16}$?

(d) (optional) Using the theory developed in class, explain why any irreducible degree two polynomial $h(x) \in \mathbb{F}_4[x]$ has roots in $\mathbb{F}_{16}$. Can you count the number of monic irreducible degree two polynomials in $\mathbb{F}_4[x]$ without having to write them down explicitly?

6. (30 points) Review the material of Monday's lecture.

(a) Explain why any automorphism of a prime field ($\mathbb{Q}$ and $\mathbb{F}_p$) is trivial.

Compute the Galois groups

(b) $\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$, where p is a prime. What, in general, can we say about the Galois group $\mathrm{Gal}(E/F)$ of a degree two extension ($[E:F]=2$) when F has characteristic 0? Consult the notes of Monday's lecture, where we reduced any such extension (even in the more general situation when $\mathrm{char}(F) \neq 2$) to an extension $F[y]/(y^2-D)$, where D does not have a square root in F.

(c) $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$.

(d) How many roots does x^3-2 have in the field $F = \mathbb{Q}(\sqrt[3]{2})$? Factor the polynomial x^3-2 into irreducibles over this field. Use this factorization (or the results from Monday's lecture) to determine the Galois group $\mathrm{Gal}(E/F)$, where E is the splitting field of x^3-2. What is the degree of this extension E/F?