Modern Algebra II, spring 2022

Homework 8, due Wednesday March 30.

1. (30 points)
(a) Prove that any automorphism of a prime field ($\mathbb{Q}$ and $\mathbb{F}_p$) is trivial.
(b) Compute the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$, 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 Wednesday'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) Can you give an example of a degree two extension E/F with the trivial Galois group $\mathrm{Gal}(E/F)$? (Hint: use characteristic two.)

2. (30 points)
(a) Determine the automorphism group of the ring $\mathbb{Z} \times \mathbb{Z}$. (Hint: an automorphism takes idempotents to idempotents. What are the idempotent elements of $\mathbb{Z} \times \mathbb{Z}$?)
(b) Prove that the automorphism group of the ring $\mathbb{Z}/2 \times \mathbb{Z}/3$ is trivial.
(c) Explain why the automorphism group of the ring $R = \mathbb{Q}[x]/(x^3)$ is infinite. (A harder question is to determine the automorphism group of this ring; can you find all automorphisms of R? Do not write this up, it's just something to think about or discuss with the instructor or the TAs.)

3. (30 points) Polynomial $x^4 + x + 1$ is irreducible over $\mathbb{F}_2$, and the 16-element field $\mathbb{F}_{16}$ can be written as $\mathbb{F}_2[\alpha]/(\alpha^4 + \alpha + 1)$. (This polynomial is one of the three irreducible degree 4 polynomials over $\mathbb{F}_2$, necessarily monic, since $\mathbb{F}_2$ has only two elements). Recall the definition of the Frobenius automorphism $\sigma = \sigma_2$.

(a) What is the order of σ as an automorphism of $\mathbb{F}_{16}$? What is the orbit of σ that contains α? Using the results obtained in class, explain why there's factorization over $\mathbb{F}_{16}$

$$x^4 + x + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^4)(x + \alpha^8).$$

Simplify α^4 and α^8 in the basis $(1, \alpha, \alpha^2, \alpha^3)$ of $\mathbb{F}_{16}$ over $\mathbb{F}_2$.

(b) Let $\beta = \alpha^2 + \alpha + 1$. Write down powers of β in the basis of powers of α until you find a linear relation on them. What is the irreducible polynomial $p(x) = \mathrm{irr}(\beta, \mathbb{F}_2)$? What are other roots of $p(x)$ in $\mathbb{F}_{16}$? (Hint: use properties of the Galois symmetries and the Frobenius.) What subfield of $\mathbb{F}_{16}$ does β generate?

(c) Let $\gamma = \alpha^3$. Write down powers of γ in the basis of powers of α until you find a linear relation on them. What is the irreducible polynomial $q(x) = \mathrm{irr}(\gamma, \mathbb{F}_2)$? Find all roots of $q(x)$ in $\mathbb{F}_{16}$.

(d) (*optional; additional 10 points*) 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?

4. (20 points) (a) Why is polynomial $x^3 - 5$ irreducible over $\mathbb{Q}$? How many roots does $x^3 - 5$ have in the field $B = \mathbb{Q}(\sqrt[3]{5})$? Why is B not a splitting field of $x^3 - 5$? Factor $x^3 - 5$ into irreducible polynomials over B. Determine the Galois group $\mathrm{Gal}(B/\mathbb{Q})$. (Hint: we discussed the Galois group for a similar polynomial $x^3 - 2$ in class.)
(b) Let E be the splitting field of $x^3 - 5$ over $\mathbb{Q}$. What can you say about the Galois group $\mathrm{Gal}(E/\mathbb{Q})$? We can choose E to contain the subfield B above, so that $E \supset B \supset \mathbb{Q}$. What is the the degree $[E : B]$ and the Galois group $\mathrm{Gal}(E/B)$? What other subfields of E can you find?