MATH 7230 Homework 2 - Fall 2019

Due Tuesday, Sep. 17 at 10:30

`https://www.math.lsu.edu/~mahlburg/teaching/2019-MATH7230.html`

You are required to turn in at least **one** of the following problems, and must complete a total of **20** by semester's end. Group work is allowed, but your solutions must be written up individually.
Problems 1 – 2 are taken from Ash (where Ash A.B.C means Problem C from Section A.B), but with a bit of additional discussion.

1. Ash 8.1.1.

   (a) Verify the claim that $D(\sigma(Q)) = \sigma D(Q)\sigma^{-1}$ for all $\sigma \in G = \mathrm{Gal}(L/K)$. This means that all of the decomposition groups for primes above $P \subset A$ are conjugate, and therefore isomorphic.

   (b) Prove the following characterization of the inertia group:
   $$\tau \in I(Q) \iff \tau(b) - b \in Q \; \forall b \in B.$$

   (c) Show that $I(\sigma(Q)) = \sigma I(Q)\sigma^{-1}$. The direct approach is to use part (b).

2. Ash 8.1.2.

In Problems 3 – 6 you will prove a number of consequences of Galois Theory for cyclotomic fields.

3. The Hasse-Minkowski Theorem gives a "Local-Global" principle for quadratic polynomials: a homogeneous quadratic polynomial $f(x_1, \ldots, x_n)$ is irreducible in $\mathbb{Z}[x_1, \ldots, x_n]$ if and only if it is irreducible modulo p for all $p \leq \infty$.

   In this problem you will prove a famous example of a quartic polynomial for which the Local-Global principle fails quite dramatically. Let $f(x) := x^4 + 1$. You will show that although this is irreducible over $\mathbb{Q}$, it is reducible modulo p for **every** prime $p \leq \infty$. (Recall that the "prime at infinity" refers to the completion of the archimedean valuation on $\mathbb{Q}$; in this case $\mathbb{Q}_\infty = \mathbb{R}$).

   (a) Show that $f(x) = \Phi_8(x)$.

   (b) Apply Eisenstein's criterion to $f(x+1)$ in order to prove that f is irreducible in $\mathbb{Q}[x]$.

   (c) Find the factorization of $f(x)$ in $\mathbb{R}[x]$.

   Remark: It is a general fact that polynomials in $\mathbb{R}[x]$ factor into linear or quadratic terms, although this relies on the deeper result that $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

4. This is a continuation of Problem 3 to the finite primes.

   (a) Show that $f(x)$ is reducible modulo 2, and find its factorization.

   (b) Now let p be odd, and show that $f(x)$ divides $x^{p^2} - x$ (and recall that this is the largest "splitting polynomial" for $\mathbb{F}_{p^2}$; i.e., this is precisely the product of **all** degree 1 and 2 irreducible polynomials modulo p).

(c) Let $E/\mathbb{F}_p$ be the (minimal) splitting field of $f(x)$ over $\mathbb{F}_p$. If $u \in E$ is a root of f, let $m_u(x) \in \mathbb{F}_p[x]$ be its minimal polynomial. Using part (d), explain why $E = \mathbb{F}_{p^2}$ or $\mathbb{F}_p$. Conclude that $m_u(x)$ is a nontrivial divisor of $x^4 + 1$.

Remark: In fact, you can further show that $E = \mathbb{F}_p$ if and only if $p \equiv 1 \pmod 8$.

5. In this problem you will use the Galois Correspondence to prove that there are no inert primes in $\mathbb{Q}(\zeta_8)$. In other words, for all $p \in \mathbb{N}$, $(p) = (Q_1 \cdots Q_g)^e$ for some $g \geq 2$.

   (a) Find the intermediate quadratic subfields of $\mathbb{Q}(\zeta_8)$ – there are three! Draw the corresponding subgroup diagram for $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$.

   (b) Using the Legendre symbol, determine which primes split in each of the quadratic subfields.

   (c) Combine all of the cases from part (b), and conclude that all p split in $\mathbb{Q}(\zeta_8)$.

6. Now you will give an alternative proof of the result in Problem 5 that only relies on properties of the Frobenius automorphism, rather than explicit descriptions of intermediate subfields.

   (a) Ash 8.3.1 states that if $p \nmid m$, then the prime factorization in $\mathbb{Z}[\zeta_m]$ is of the form

   $$(p) = Q_1 \cdots Q_g,$$

   where each Q_j has relative degree $f := \mathrm{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times}(f) = \min_k p^k \equiv 1 \pmod m$, and $fg = \phi(m)$. What can you conclude if p is an odd prime and $m = 8$?

   (b) Generalize the argument, and determine which cyclotomic fields have no inert primes.

In the remaining problems you will calculate the Decomposition and Inertia groups (and all other parts of the Galois Tower) for a few interesting examples of number fields.

7. Let $L = \mathbb{Q}(\zeta_5)$, and $p = (11)$.

   (a) Determine the prime factorization of p in $B = \mathcal{O}_L$.

   (b) We discussed in lecture that the Galois group is $\mathrm{Gal}(L/Q) = \{\sigma_1 = \mathrm{id}, \sigma_2, \sigma_3, \sigma_4\}$, where $\sigma_a : \zeta_5 \mapsto \zeta_5^a$. Find the Decomposition Group D (for some prime Q above p), and verify that it satisfies the required properties. For example, you should find that $\sigma_2 \notin D$, which can be verified by showing that $\sigma_2(\zeta_5 + 2) = \zeta_5^2 + 2 \notin Q$ (show that this element reduces to a nonzero residue in $B/Q \cong \mathbb{Z}/11\mathbb{Z}$!).

   (c) Finally, consider the Frobenius element of Q, $\sigma_Q = \sigma_{11}$. How does this automorphism relate to D?

8. Let $L = \mathbb{Q}(\zeta_{12})$.

   (a) Calculate the minimal polynomial for ζ_{12} (i.e., $\Phi_{12}(X)$).

   (b) Determine the Galois group $\mathrm{Gal}(L/\mathbb{Q})$, and describe it explicitly.

   (c) Now fill in all subfields and subgroups in the Galois Tower. You should find three intermediate quadratic fields – describe them explicitly!

9. It will be helpful if you do Problem 8 before this one. Let $L = \mathbb{Q}(\zeta_{12})$.

(a) Use the Dedekind-Kummer Theorem (or any other method) to determine the prime factorization of $p = (2)$ in $\mathcal{O}_L = \mathbb{Z}[\zeta_{12}]$.

(b) Determine the decomposition group D of Q, where Q is any prime above p in $\mathcal{O}_L$. Although it is possible to easily find D using the degrees of the extensions, you are required to also verify that $\sigma(Q) = Q$ for each $\sigma \in D$.

(c) Finally, calculate the inertia group I.