MATH 7230 Homework 3 - Fall 2019

Due Tuesday, Oct. 1 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 – 4 give further examples and general properties of the real subfields of cyclotomic fields.

1. Let $K = \mathbb{Q}(\alpha_7)$, with $\alpha_7 := \zeta_7 + \zeta_7^{-1}$. This is the *real subfield* of the cyclotomic field $\mathbb{Q}(\zeta_7)$. It is a fact that the ring of integers has a power basis, namely $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

   (a) Show that the minimal polynomial of α_7 is $X^3 + X^2 - 2X - 1$.

   (b) We discussed in lecture that by embedding $K \subset \mathbb{Q}(\zeta_7)$ one can conclude (see Childress Theorem 1.8) that p splits completely in K if and only if $p \equiv \pm 1 \pmod 7$. Verify this by finding the prime factorization of (13) in $\mathcal{O}_K$.

2. Let $K = \mathbb{Q}(\alpha_9)$, with $\alpha_9 := \zeta_9 + \zeta_9^{-1}$, and $\mathcal{O}_K = \mathbb{Z}[\alpha_9]$.

   (a) Show that the minimal polynomial of α_9 is $f(X) = X^3 - 3X + 1$.

   (b) Show that the roots of $f(X)$ are $\alpha, \alpha^2 - 2$, and $-\alpha^2 - \alpha + 2$.

   (c) Show explicitly that the Galois automorphism $\sigma : \alpha_7 \mapsto \alpha_7^2 - 2$ generates $\mathrm{Gal}(K/\mathbb{Q})$.

   Remark: This example is sometimes presented as $\mathbb{Q}(X)/(f(X))$, without any further context, which makes it seem much more mysterious!

3. This is a continuation of Problem 2.

   (a) Now consider the prime $p = (5)$ and calculate the decomposition group $D(Q, K/\mathbb{Q})$, where Q is some prime above p.

   (b) Verify that the Frobenius automorphism generates the decomposition group. In particular, how does $\sigma_5 = \left(\frac{p}{K/\mathbb{Q}}\right)$ relate to σ from Problem 2(c)?

4. In this problem you will fill explore a few further details related to Example 9 on p. 23 of Childress.

   (a) Childress Exercise 2.3.

   (b) Recall that if χ is a character for the group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, then the *field associated to* χ is the fixed field for $\ker(\chi)$. Let $n = 9$, with $(\mathbb{Z}/9\mathbb{Z})^\times = \langle 2 \rangle$, and consider the character defined by $\chi(2) := -1$. Find the field associated to χ.

   Hint: The field will be a quadratic extension of $\mathbb{Q}$.

   (c) Now let $n = 16$, with $(\mathbb{Z}/16\mathbb{Z})^\times = \langle -1 \rangle \times \langle 5 \rangle$, and define the character defined by $\chi(-1) = 1$ and $\chi(5) = -1$. Find the field associated to χ.

   Hint: The field will be real.

5. In this problem you will prove that primitive Dirichlet characters exist for all moduli $n \not\equiv 2 \pmod 4$. Denote the group of Dirichlet characters modulo n by $\widehat{G}_n := \widehat{(\mathbb{Z}/n\mathbb{Z})}^\times$. Let $\pi(n)$ be the number of primitive characters modulo n.

   (a) Prove that π is multiplicative: if $(n_1, n_2) = 1$, then $\pi(n_1 n_2) = \pi(n_1)\pi(n_2)$.

   (b) Show that for prime powers,
$$\pi(p^a) = \begin{cases} p-2 & \text{if } a = 1, \\ (p-1)^2 p^{a-2} & \text{if } a \geq 2. \end{cases}$$

   (c) Write down the general formula for $\pi(n)$ if $n = p_1^{a_1} \cdots p_m^{a_m}$.
   Remark: In practice, this means that primitive Dirichlet characters **always** *exist, recalling that $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$ for odd m.*

Problems 6 – 9 are an expanded version of Childress Exercise 2.9, and also give an in-depth example of Childress Theorem 2.2 and Corollary 2.3. As a final check of your work, you should find that $K/\mathbb{Q}$ and $K'/\mathbb{Q}$ are field extensions in which 3 and 5 are ramified, but K/K' is an extension in which **all** primes are unramified!

6. Let $K := \mathbb{Q}(\alpha, \zeta_3)$, where $\alpha := \zeta_{15} + \zeta_{15}^4$.

   (a) Determine the degrees of each field extension in the tower
$$\mathbb{Q} \subset \mathbb{Q}(\zeta_3) \subset K \subset \mathbb{Q}(\zeta_{15}).$$
   One approach to understanding K is to search for a relation between α, ζ_3 and the cyclotomic polynomial $\Phi_{15}(X)$ (or the somewhat simpler, if lengthier, relation $1 + \zeta_{15} + \zeta_{15}^2 + \cdots + \zeta_{15}^{14} = 0$).

   (b) Now determine the corresponding Galois subgroups for the field tower. For $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/K)$ it will be useful to note that $\sigma_4^2 = \sigma_1$ (using the usual notation $\sigma_b : \zeta_{15} \mapsto \zeta_{15}^b$).

   (c) Define the subgroup $X := \langle \chi^2, \psi \rangle$, where $\widehat{G}_5 = \langle \chi \rangle$, and $\widehat{G}_3 = \langle \psi \rangle$. Note that $\chi^2 = \left(\frac{\bullet}{5}\right)$.
   Calculate $\ker X$. How does this compare to $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/K)$ (which you calculated in Problem 6 (b))?

7. In this problem and the next you will fill in all parts of the field diagram on Childress p. 26. First let $p^a = 3$ (so $m = 5$), and denote the corresponding fields as E_3 and L_3.

   (a) Calculate $E_3 = \mathbb{Q}(\zeta_3)^{\ker X_3}$, with X as in Problem 6 (c).

   (b) Calculate $L_3 = \mathbb{Q}(\zeta_{15})^{\ker(X_3 \times \widehat{G}_5)}$. Verify that this equals $K(\zeta_5)$.

   (c) What is the ramification degree e of (3) in K? How does this compare to $|X_3|$?

8. Let $p^a = 5$ (so $m = 3$), and denote the corresponding fields as E_5 and L_5.

   (a) Calculate $E_5 = \mathbb{Q}(\zeta_5)^{\ker X_5}$, with X as in Problem 6 (c).

   (b) Calculate $L_3 = \mathbb{Q}(\zeta_{15})^{\ker(X_5 \times \widehat{G}_3)}$. Verify that this equals $K(\zeta_3)$.

   (c) What is the ramification degree e of (5) in K? How does this compare to $|X_5|$?

9. Define the subgroup $X' := \langle \chi_5^2 \chi_3 \rangle < \widehat{G}_{15}$.

(a) Calculate $\ker(X')$ (you should obtain a cyclic subgroup with 4 elements).

(b) Let $K' := \mathbb{Q}(\zeta_{15})^{\ker(X')}$. This is a quadratic extension of $\mathbb{Q}$ (why?) – identity which one. A very explicit approach is to show that $\alpha' \in K'$, where $\alpha' := \zeta_{15} + \zeta_{15}^2 + \zeta_{15}^4 + \zeta_{15}^8$. Then show that the minimal polynomial of α' is quadratic!

(c) Finally, show that 3 and 5 both ramify in K', and use the various degrees that you calculated in Problems 7 and 8 to conclude that there is no ramification in K/K'.