MATH 7230 Homework 8 - Fall 2018

Due Wednesday, Nov. 14 at 1:30

`https://www.math.lsu.edu/~mahlburg/teaching/2018F-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.

The notation "Ash A.B.C" means Problem C from Section A.B in the textbook.

Problems 1–4 explore the interesting invariants for the cyclotomic fields $\mathbb{Q}(\zeta_p)$. This covers most of the material in Ash 7.1.

1. The *cyclotomic polynomials* are defined by $\Phi_1(X) := X - 1$, and for $n \geq 2$,

$$\Phi_n(X) := \frac{X^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \Phi_d(X)}. \tag{1}$$

   (a) Prove that

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1; \\ p & \text{if } n = p^k \text{ is a prime power;} \\ 1 & \text{if } n \text{ is composite.} \end{cases}$$

   Hint: Use strong induction on n.

   (b) Prove that

$$\Phi_n(X) = \prod_{\substack{0 \leq m \leq n-1 \\ (m,n)=1}} (X - \zeta_n^m),$$

   where $\zeta_n := e^{\frac{2\pi i}{n}}$.

   (c) Conclude that $\Phi_n(X)$ is a polynomial with integer coefficients. What is its degree?

2. Now focus on the case that $n = p$ is prime. Let B be the ring of algebraic integers in $L = \mathbb{Q}(\zeta_p)$. It is immediate that $B \supseteq \mathbb{Z}[\zeta_p]$ (why?).

   (a) Use Eisenstein's criterion to prove that $\Phi_p(1 - X)$ is irreducible.
   Remark: This implies that $\Phi_p(X)$ is irreducible. It is also true that $\Phi_n(X)$ is irreducible, but this is nontrivial; see S. Weintraub's article for several proofs:
   `https://www.lehigh.edu/~shw2/c-poly/several_proofs.pdf`.

   (b) Conclude that the minimal polynomial of $1 - \zeta_p$ is $\Phi_p(1 - X)$. Actually, this should more properly be $(-1)^{\phi(p)}\Phi_p(1 - X)$, as we know that $1 - \zeta_p$ is an algebraic integer, and the sign ensures a **monic** polynomial. Calculate $\mathrm{Nm}_{L/\mathbb{Q}}(1 - \zeta_p)$ – note that the constant term of $\Phi_p(1 - X)$ is $\Phi_p(1)$.

   (c) Finally, use Proposition 4.2.6 and Corollary 4.2.8 to show that $(1 - \zeta_p)_B$ is a prime ideal.

3. (a) Calculate the discriminant of the power basis generated by ζ_p, namely $D_L\left(1, \zeta_p, \cdots, \zeta_p^{p-2}\right)$. The easiest approach is to use Corollary 2.3.6, as the derivative of $\Phi_p(X)$ is quite simple.

   (b) Show that the norm you calculated in Problem 2 2b can be written as

$$\begin{aligned}\mathrm{Nm}_{L/\mathbb{Z}}(1-\zeta_p) &= (1-\zeta_p)\left(1-\zeta_p^2\right)\cdots\left(1-\zeta_p^{p-1}\right)\\ &= (1-\zeta_p)\cdot u_2(1-\zeta_p)\cdots u_{p-1}(1-\zeta_p),\end{aligned}$$

   where $u_j := (1-\zeta_p^j)/(1-\zeta_p)$ is a unit in $\mathbb{Z}[\zeta_p]$.

   (c) Prove that p therefore ramifies completely in B, as $(p)_B = (1-\zeta_p)_B^{p-1}$.

4. Finally, in this problem you will complete the proof that $B = \mathbb{Z}[\zeta_p]$. The argument relies on the fact that the discriminant is a power of p, which is also the norm of $\pi := 1-\zeta_p$. This introduces a sort of "nilpotency" that is key for showing that $B \subseteq \mathbb{Z}[\zeta_p]$.

   (a) Much of the linear algebra in Ash 4.2.5 does not require I to be an ideal (though that is ultimately needed for the ideal norm to be multiplicative). Suppose that $J \subseteq B$ is a free $\mathbb{Z}$-module of rank n, with $B = \langle b_1, \cdots, b_n\rangle_{\mathbb{Z}}$ and $J = \langle z_1, \cdots, z_n\rangle_{\mathbb{Z}}$. If $(z_1, \cdots, z_n)^T = C(b_1, \cdots, b_n)^T$ for $C \in M_n(\mathbb{Z})$, use Lemma 2.3.2 to show that

$$|B/J| = \left|\frac{D_L(z_1, \cdots, z_n)}{d}\right|^{\frac{1}{2}},$$

   where $d = D_L(b_1, \cdots, b_n)$ is the field discriminant.

   (b) Use part (a) and Problem 3 to show that $|B/\mathbb{Z}[\zeta_p]| = p^m$ for some $m \leq \frac{p-1}{2}$.

   (c) Explain why $B/(\pi)_B \cong Z/pZ$, and why this further implies that $B = \mathbb{Z} + (\pi)_B$.

   (d) Finally, use part (c) to inductively conclude that for any $b \in B$, there is an expansion

$$b = k_0 + k_1\pi + \cdots + k_{\ell-1}\pi^{\ell-1} + b_\ell\pi^\ell,$$

   where each $k_j \in \mathbb{Z}$ and $b_\ell \in B$. Now use part (b) and pick an appropriate ℓ such that $b \in \mathbb{Z}[\zeta_p]$ (noting that $\mathbb{Z}[\zeta_p] = \mathbb{Z}[\pi]$.

5. (a) Ash 9.1.1. Use the fact that if F is a finite field, then $F^\times = F \setminus \{0\}$ is a finite multiplicative group.

   (b) Ash 9.1.2. Use Proposition 9.1.7 – this was skipped in lecture, so be sure to read the proof!

6. Ash 9.1.3. You can refer to Ash's solution for nearly all of the details for the forward direction: that if $|\bullet|_1, |\bullet|_2$ are equivalent, then $|\bullet|_1 = |\bullet|_2^a$ for some $a > 0$. Be sure that you also address the reverse direction!