MATH 7230 Homework 1 - Fall 2019

Due Tuesday, Sep. 3 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.

1. **Postage Stamp Problem.** Suppose that postage stamps are available in denominations of a and b cents, where a and b are relatively prime. A postage amount n is *achievable* if it can be obtained as the total of some finite combination of stamps; in other words, n is contained in the semigroup

$$\langle a, b\rangle_{\mathbb{N}} := \{am + bn \mid m, n \in \mathbb{N}\}.$$

   (a) Determine which values are achievable if $a = 5, b = 8$.

   (b) Prove that all amounts that are at least $(a-1)(b-1)$ are achievable.

   (c) Prove that the number of amounts that are not achievable is exactly $\frac{(a-1)(b-1)}{2}$.

2. Suppose that p and q are odd primes, and for an odd integer n, let $n^* := (-1)^{\frac{n-1}{2}} n$. In this problem you will show that in $\mathbb{Q}(\sqrt{q^*})$ we have the factorization

$$(p) = \begin{cases} P_1 P_2 & (\textit{split}) \qquad \text{if } \left(\frac{q^*}{p}\right) = 1, \\ (p) & (\textit{inert}) \qquad \text{if } \left(\frac{q^*}{p}\right) = -1. \end{cases} \tag{1}$$

   (a) Show that the ring of algebraic integers is $\mathbb{Z}[\theta]$, where $\theta := \frac{1+\sqrt{q^*}}{2}$.

   (b) Show that the minimal polynomial is $m_\theta(X) = X^2 - X + \frac{1-q^*}{4}$, and that the discriminant is $d = q^*$.

   (c) Recall Dedekind-Kummer's theorem (Childress Theorem 1.1): if the ring of integers in $L/\mathbb{Q}$ has a *power basis* $\mathbb{Z}[\theta]$, then the factorization of (p) in L is dictated by the factorization of the minimal polynomial $m_\theta(X)$ mod p. Use this to conclude the main problem statement in (1).

   (d) Find the factorization of (3) in $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{13})$.

3. Problem 2 made use of Dedekind-Kummer's result for prime ideal factorization, but not every number field has a power basis!

   (a) Let $L := \mathbb{Q}\left(\sqrt[3]{5^2 \cdot 7}\right)$, and denote its ring of integers by O_L. Show that $\sqrt[3]{5 \cdot 7^2} \in O_L$.

   (b) Show that O_L does not have a power basis.

   Remark: See HW 5 from MATH 7230 Fall 2018 for examples in biquadratic number fields.

In Problems 4 – 5 you will prove several additional consequences of applying Galois Theory to quadratic and cyclotomic number fields. This is meant to give a further taste of what can be achieved with Class Field Theory!

4. Suppose that p and q are odd primes. In this problem you will prove that (p) is the product of an even number of prime factors in $Q(\zeta_q)$ if and only if it splits in $L = \mathbb{Q}(\sqrt{q^*})$.

   (a) For the reverse direction, suppose that $(p)_{\mathbb{Q}(\sqrt{q^*})} = P_1 P_2$. Use the conjugation map in $\mathrm{Gal}(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q})$ to explain why P_1 and P_2 must have the same number of prime factors in L.

   (b) Now consider the forward direction by supposing that $(p)_L = P_1 P_2 \cdots P_{2g}$. Show that these ideals are all distinct, and are partitioned into two orbits by the index 2 subgroup generated by σ^2, say $\langle \sigma^2 \rangle P_1 = \{P_{i_1}, \ldots, P_{i_g}\}$ and $\langle \sigma^2 \rangle \circ \sigma P_1 = \{P_{j_1}, \ldots, P_{j_g}\}$.

   Hint: Recall/show that $\Phi_q(X)$ has no repeated roots, and that Gal$(L/\mathbb{Q}) \cong C_{q-1} = \langle \sigma \rangle$ acts transitively on the P_j (see Ash 8.1).

   (c) Let
   $$P_e := P_{i_1} \cdots P_{i_g}, \quad P_o := P_{j_1} \cdots P_{j_g},$$
   and denote their intersections with $\mathbb{Q}(\sqrt{q^*})$ by P_e^*, P_o^*. Explain why $P_e^* P_o^* = (p)_{\mathbb{Q}(\sqrt{q^*})}$. Furthermore, explain why P_e^* and P_o^* must be distinct prime ideals.

   Hint: Recall the "efg"-relation for prime factorizations in field extensions, and the fact that the only primes with ramification are those that divide the discriminant.

5. In this problem you will prove the Kronecker-Weber Theorem: any quadratic number field $\mathbb{Q}(\sqrt{D})$ is a subfield of some cyclotomic extension of $\mathbb{Q}$.

   (a) First, explain why it is sufficient to restrict to squarefree D.

   (b) Next, use the fact from lecture that $\mathbb{Q}(\sqrt{q^*}) \subset \mathbb{Q}(\zeta_q)$ to conclude the statement for the case that $D = q$ is prime. You will need to take care with primes that are 3 modulo 4. For example, given that $7^* = -7$, and thus $\mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$, which cyclotomic field contains $\mathbb{Q}(\sqrt{7})$? You also need to treat the case $D = 2$ separately!

   (c) Finally, explain how to piece together your solution for part (b) in order to address the general case of any squarefree D.