Exercise sheet #4

Prof. Peter Bürgisser, Dr. Pierre Lairez, Paul Breiding and Jesko Hüttenhain

May 18, 2016

Exercise 1. Describe all the subfields of $\mathbb{Q}(\zeta_8)$, where ζ_8 is a primitive 8th root of unity.

Exercise 2. Let $n > 0$ be an integer and let $\zeta \in \mathbb{C}$ be a primitive nth root of unity. Show that $\mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1})$ and that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$.

Exercise 3. Let K be a field and n a positive integer.

1. Show that if d divides n then $X^d - 1$ divides $X^n - 1$ in $K[X]$.

We define the nth cyclotomic polynomial over K by

$$\Phi_n^K(X) = \frac{X^n - 1}{\text{least common multiple of all } X^d - 1 \text{ with } 0 < d < n \text{ and } d \mid n},$$

where the least common multiple is chosen to be monic, so that Φ_n^K is a monic polynomial.

2. Show that $\Phi_n^{\mathbb{Q}}(X)$ has integer coefficients.

   Hint: Show that the lcm of two monic polynomials in $\mathbb{Z}[X]$ is monic.

3. Show that for any prime number p and any integer $r > 0$,

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}).$$

4. Let $i : \mathbb{Z}[X] \to K[X]$ be the morphism induced coefficient-wise by the unique ring morphism $\mathbb{Z} \to K$. Show that $\Phi_n^K = i(\Phi_n^{\mathbb{Q}})$.

5. If the characteristic of K does not divide n, show that

$$\Phi_n^K(X) = \prod_{\zeta \in P_n} (X - \zeta),$$

   where P_n is the set of all primitive nth roots of unity in the algebraic closure of K.

Exercise 4. Let $n > 0$ be an integer. The goal is to prove that there exist infinitely many prime numbers p such that $p = 1 \pmod{n}$.
Let $p_1, \ldots, p_r$ be a sequence of prime numbers congruent to 1 modulo n. Let $k > 0$ be an integer such that $\Phi_n^{\mathbb{Q}}(knp_1 \cdots p_r) > 1$. Let $N = \Phi_n^{\mathbb{Q}}(knp_1 \cdots p_r)$, it is an integer.

1. Show that $N = \pm 1 \pmod{p_i}$, for $1 \leqslant i \leqslant r$.

   Hint: Show that $\Phi_n^{\mathbb{Q}}(0) = \pm 1$.

Let q be a prime divisor of N.

2. Show that q does not divide n.
3. Show that the order of the class of N in $\mathbb{F}_q^\times$ is exactly n.

   Hint: Use the previous exercise, question 5.
4. Show that $q = 1 \pmod{n}$.
5. Conclude.