Exercise sheet #5

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

May 25, 2016

Exercise 1. Let $f \in \mathbb{Z}[X]$ be a non constant polynomial. Show that f has a root modulo p for infinitely many prime numbers p.
Hint: Reduce to the case where $f(0) \neq 0$, and then consider the polynomial $g(X) = f(f(0)X)/f(0)$ to reduce further to the cases where $f(0) = 1$.

Exercise 2. Let $f = X^4 + 1 \in \mathbb{Q}[X]$.

1. Show that f is irreducible.
2. Show that f is reducible modulo 2.
3. Show that f is reducible modulo every prime number p.

   Hint: Show that for any prime $p > 2$, $\mathbb{F}_{p^2}$ contains a primitive 8th root of unity.

Exercise 3. Let p be a prime number and let K be a field that contains a primitive p-th root of unity. Let $c \in K$.
Show that if the polynomial $X^p - c$ is not irreducible then it splits into linear factors.

Exercise 4. Let $f \in \mathbb{Q}[X]$ be a polynomial of degree $n > 2$, and let K be the splitting field of f over $\mathbb{Q}$. Suppose that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the symmetric group S_n. Let $\alpha \in K$ be a root of f.

1. Show that f is irreducible.
2. Show that the only automorphism of $\mathbb{Q}(\alpha)$ is the identity.

   Hint: If σ is a non-trivial isomorphism of $\mathbb{Q}(\alpha)$, study the tower of extensions $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \sigma\alpha) \subseteq K$.

3. If $n \geqslant 5$, show that $\alpha^n \notin \mathbb{Q}$.