Exercise sheet 6

1. *(Irreducibility of the cyclotomic polynomial)* Let n be a positive integer, and $P \in \mathbb{Z}[X]$ a monic irreducible factor of $X^n - 1 \in \mathbb{Q}[X]$. Suppose that ξ is a root of P.

1. Show that for each $k \in \mathbb{Z}_{\geq 0}$ there exists a unique polynomial $R_k \in \mathbb{Z}[X]$ such that $\deg(R_k) < \deg(P)$ and $P(\xi^k) = R_k(\xi)$. Prove that $\{R_k | k \in \mathbb{Z}_{\geq 0}\}$ is a finite set. We define
$$a := \sup\{|u| : u \text{ is a coefficient of some } R_k\}$$
2. Show that for $k = p$ a prime, p divides all coefficients of R_p, and that when $p > a$ one has $R_p = 0$ [*Hint:* $P(\xi^p) = P(\xi^p) - P(\xi)^p$].
3. Deduce that if all primes dividing some positive integer m are strictly greater then a, then $P(\xi^m) = 0$.
4. Prove that if r and n are coprime, then $P(\xi^r) = 0$ [*Hint:* Consider the quantity $m = r + n\prod_{p \leq a, p \nmid r} p$].
5. Recall the definition of n-th cyclotomic polynomial Φ_n for $n \in \mathbb{Z}_{>0}$: we take $W_n \subseteq \mathbb{C}$ to be the set of primitive n-th roots of unity, and define
$$\Phi_n(X) := \prod_{x \in W_n} (X - x).$$
Prove the following equality for $n \in \mathbb{Z}_{>0}$:
$$\prod_{0<d|n} \Phi_d(X) = X^n - 1,$$
and deduce that $\Phi_n \in \mathbb{Z}[X]$ for every n.
6. Prove that the n-th cyclotomic polynomial is irreducible. [*Hint:* Take $\xi := \exp(2\pi i/n)$ and P its minimal polynomial over $\mathbb{Q}$. Check that P satisfies the required hypothesis to deduce that $\Phi_n(X)|P$ (using Points 1-4). Then irreducibility of P together with Point 5 allow you to conclude.]

2. Let $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$, and $\alpha \in \bar{\mathbb{Q}}$ be a root of f. Define $K = \mathbb{Q}(\alpha)$.

1. Check that f is irreducible in $\mathbb{Q}[X]$.
2. Prove that f splits over K, and deduce that $K/\mathbb{Q}$ is Galois with group $\mathbb{Z}/3\mathbb{Z}$. [*Hint:* Factor f over $\mathbb{Q}(\alpha)$ as $f = (x-\alpha)g$, and solve g, observing that $12 - 3\alpha^2 = (-4 + \alpha + 2\alpha^2)^2$]

Please turn over!

3. Deduce, without computation, that the discriminant of f is a square in $\mathbb{Q}^\times$. Then check this by using the formula of the discriminant $\Delta = -4a^3 - 27b^2$ for a cubic polynomial of the form $X^3 + aX + b$.

3. Let n be a positive integer. Prove that the symmetric group S_n is generated by the cycle $(1\ 2\ \cdots\ n)$ and τ, where τ is any transposition.

4. Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of prime degree p, and suppose that it has precisely 2 non-real roots. Let L_f be the splitting field of f, and $G := \mathrm{Gal}(L_f/\mathbb{Q})$. Recall that the action of G on the roots of f gives an injective group homomorphism $G \hookrightarrow S_p$, and call H the image of G via this injection.

1. Notice that the complex conjugation is a $\mathbb{Q}$-automorphism of L_f, and deduce that H contains a transposition.
2. Show that p divides the order of G, and that G contains an element of order p [*Hint:* Use First Sylow Theorem. See Exercise 7 from Exercise Sheet 5 of the HS14 course Algebra I].
3. Conclude that $H = S_p$ [*Hint:* Previous exercise].

Use this to show that the Galois group of the splitting field of $f(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$ is S_5. [You have to check that f is irreducible and has precisely 2 non-real roots.]