Solutions of 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.]

Solution: Recall that for a monic polynomial $f \in \mathbb{Z}[X]$ we know that f is irreducible in $\mathbb{Z}[X]$ if and only if it is irreducible in $\mathbb{Q}[X]$ (see the Gauss's Lemma, in the solution of Exercise Sheet 11 of Algebra I, HS 2014).

1. Since P is monic and irreducible in $\mathbb{Z}[X]$, it is also irreducible in $\mathbb{Q}[X]$, so that $\mathbb{Q}(\xi) \cong \mathbb{Q}[X]/(P(X))$ is an algebraic extension of $\mathbb{Q}$ of degree $\deg(P)$, and the elements $1, \xi, \ldots, \xi^{\deg(P)}$ are linearly independent. Then $P(\xi^k) \in \mathbb{Q}(\xi)$ cannot be expressed in more then one way as $P(\xi^k) = R_k(\xi)$ with $R_k \in \mathbb{Z}[X]$ of degree

$< \deg(P)$, and we only have to check existence. This is a special case of proving that for each $f \in \mathbb{Z}[X]$ we have $f(\xi) = b_0 + b_1\xi + \cdots + b_{\deg(P)-1}\xi^{\deg(P)-1}$ for some $b_i \in \mathbb{Z}$, which is easily proven by induction on $\deg(f)$: the statement is trivial for all $\deg(f) < \deg(P)$; for bigger degree, we see that the degree of f can be lowered (up to equivalence modulo P) by substituting the maximal power $X^{\deg(P)+a}$ of X in f with $X^a(X^{\deg(P)} - P(X))$, which has degree strictly smaller then $\deg(P)+a$ as P is monic, so that the inductive hypothesis can be applied. [More simply, one can notice that $\mathbb{Z}[X]$ is a unique factorization domain, and that Euclidean division of f by P can be performed (as in $\mathbb{Q}[X]$), so that $R_k(X)$ is nothing but the residue of the division of $R(X^k)$ by $P(X)$.]

Since $\xi^k = \xi^h$ for $n|k-h$, the set $\{\xi^k : k \in \mathbb{Z}_{\geq 0}\}$ is finite, and so is the set of the R_k's.

2. Notice that for $f \in \mathbb{Z}[X]$ one has that $f(X^p) - f(X)^p$ is divisible by p. Indeed, we write $f = \sum_{j=0}^{s} \lambda_j X^j$ and consider the multinomial coefficient for a partition into positive integers $t = \sum_i t_i$:

$$(*)\ \binom{t}{t_1,\ldots,t_s} = \frac{t!}{t_1!\cdots t_s!} = \binom{t}{t_1}\binom{t-t_1}{t_2}\binom{t-t_1-t_2}{t_3}\cdots\binom{t_{s-1}+t_s}{t_{s-1}} \in \mathbb{Z},$$

which counts the number of partitions of a set of t elements into subsets of $t_1, t_2, \ldots, t_s$ elements, and we have

$$\begin{aligned} f(X^p) - f(X)^p &= \sum_{j=0}^{s} \lambda_j X^{jp} - \sum_{\substack{e_0+\cdots+e_j=p \\ 0\leq e_j\leq p}} \binom{p}{e_0,\ldots,e_s} \prod_{j}^{s} (\lambda_j)^{e_j} X^{je_j} \\ &= \sum_{j=0}^{s} (\lambda_j - \lambda_j^p) X^{jp} - \sum_{\substack{e_0+\cdots+e_j=p \\ 0\leq e_j< p}} \binom{p}{e_0,\ldots,e_s} \prod_{j=0}^{s} (\lambda_j)^{e_j} X^{je_j}. \end{aligned}$$

By Fermat's little theorem we have $p|\lambda_j - \lambda_j^p$ for each j. Moreover, each multinomial coefficient appearing in the second sum is divisible by p, because the definition in terms of factorials in $(*)$ makes it clear that none of the e_j has p as a factor, so that p does not cancel out while simplifying the fraction, which belongs to $\mathbb{Z}$. Hence $p|f(X^p) - f(X)^p$.

We can then write $P(\xi^p) = P(\xi^p) - P(\xi)^p = pQ(\xi)$ for some $Q(X) \in \mathbb{Z}[X]$, and by what we proved in the previous point we can write $Q(\xi) = R_Q(\xi)$ for some polynomial $R_Q \in \mathbb{Z}[X]$ of degree strictly smaller than $\deg(P)$. This gives $R_p(\xi) = P(\xi^p) = pR_Q(\xi)$, and by uniqueness of R_p we can conclude that $R_p = pR_Q \in p\mathbb{Z}[X]$.

If $p > a$, then the absolute values of the coefficients of R_p are non-negative multiples of p, and by definition of a they need to be zero, so that $R_p = 0$ in this case.

3. This is an easy induction on the number s of primes (counted with multiplicity) dividing m. One can indeed write $m = \prod_{i=1}^{s} p_i$ for some primes $p_i > a$. For $s = 1$ this is just the previous point, because $R_{p_1} = 0$ means $P(\xi^{p_1}) = 0$. More

See next page!

in general, by inductive hypothesis we can assume that $P(\xi^{p_1 \cdots p_{s-1}}) = 0$, and apply the previous point with $\xi^{p_1 \cdots p_{s-1}}$ (which is a root of P) instead of ξ to get $P((\xi^{p_1 \cdots p_{s-1}})^{p_s}) = 0$.

4. Let $m = r + n \prod_{p \le a, p \nmid r} p$. For $q \le a$ a prime, we see that q either divides r or $n \prod_{p \le a, p \nmid r} p$, so that q does not divide m and by previous point we get $P(\xi^m) = 0$. But $\xi^n = 1$ by hypothesis (because $P | X^n - 1$), so that $\xi^m = \xi^r$ and we get $P(\xi^r) = 0$.

5. Let $\gamma_n = \prod_{0<d|n} \Phi_d$. Since a complex number belongs to W_k if and only if it has multiplicative order k, all the W_k's are disjoint. Then γ_n has distinct roots, and its set of roots is $\cup_{0<d|n} W_d$. On the other hand, the roots of $X^n - 1$ are also all distinct: they are indeed the n distinct complex numbers $\exp(2\pi i k/n)$ for $a = 0, \ldots, n-1$. It is then easy to see that the two polynomials have indeed the same roots, since a n-th root of unity has order d dividing n, and primitive d-th roots of unity are n-th roots of unity for $d|n$. As both γ_n and Φ_n are monic, unique factorization in $\mathbb{Q}[X]$ gives $\gamma_n = \Phi_n$ as desired.

   We then prove that the coefficients of the Φ_n are integer by induction on n. For $n = 1$ we have $\Phi_n = X - 1 \in \mathbb{Z}[X]$. For $n > 1$, suppose that $\Phi_k \in \mathbb{Z}[X]$ for all $k < n$. Then
   $$\Phi_n = \frac{X^n - 1}{\prod_{\substack{0<d|n \\ d \neq n}} \Phi_d(X)},$$
   and since the denominator lies in $\mathbb{Z}[X]$ by inductive hypothesis, we can conclude that $\Phi_n \in \mathbb{Z}[X]$. Indeed, Φ_n needs necessarily to lie in $\mathbb{Q}[X]$ (else, for l the minimal degree of a coefficient of Φ_n not lying in $\mathbb{Q}$ and m the minimal degree of a non-zero coefficients of the denominator, one would get that the coefficient of degree $l + m$ in $X^n - 1$ would not lie in $\mathbb{Q}$, contradiction). We can then write the monic polynomial Φ_n as $\frac{1}{\mu}\Theta_n$ for some primitive polynomial $\Theta_n \in \mathbb{Z}[X]$, but then Gauss's Lemma (see the solution of Exercise Sheet 11 of Algebra I, HS 2014) tells us that $X^n - 1$ equals $\frac{1}{d}$ times a primitive polynomial, and the only possibility is $d = \pm 1$, which implies that $\Phi_n \in \mathbb{Z}[X]$.

6. $\xi = \exp(2\pi i/n)$ satisfies both its minimal polynomial P and $X^n - 1$, so that $P | X^n - 1$. Being $X^n - 1$ and P monic we necessarily have $P \in \mathbb{Z}[X]$ by Gauss's lemma. Then $W_n = \{\xi^r : 0 < r < n, (r, n) = 1\}$, so that by point 4 we get $P(x) = 0$ for each $x \in W_n$ and by definition of Φ_n we obtain $\Phi_n | P$. This is a divisibility relation between two polynomials in $\mathbb{Q}[X]$, hence an equality as P is irreducible in $\mathbb{Q}[X]$. In particular, the cyclotomic polynomial Φ_n is itself irreducible.

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 $X^3 + aX + b$.

Solution:

1. f is irreducible in $\mathbb{Q}[X]$ if and only if it has no root in $\mathbb{Q}$. By Gauss's lemma, such a root would actually lie in $\mathbb{Z}$ as f is monic, so that it would divide the constant term 1. But $f(1) = 1 - 3 + 1 = -1$, while $f(-1) = -1 + 3 + 1 = 3$, so that f has no integer root and is irreducible.
2. Let $g(X) = X^2 + aX + b \in K(\alpha)$ be such that $f = (X - \alpha)g(X)$. Then equalizing the coefficients in degree 2 and 1 we get $a = \alpha$ and $b = \alpha^2 - 3$, so that $g(X) = X^2 + \alpha X + (\alpha^2 - 3)$. Then

$$g(X) = \left(X + \frac{\alpha}{2}\right)^2 - \frac{1}{4}(12 - 3\alpha^2) = \left(X + \frac{\alpha}{2}\right)^2 - \left(\frac{1}{2}(-4 + \alpha + 2\alpha^2)\right)^2$$
$$= \left(X + \frac{\alpha}{2} + \frac{1}{2}(-4 + \alpha + 2\alpha^2)\right) \cdot \left(X + \frac{\alpha}{2} - \frac{1}{2}(-4 + \alpha + 2\alpha^2)\right),$$

   Then f splits in K which is its splitting field over $\mathbb{Q}$ and as such is Galois (the polynomial f is separable because the roots of g are distinct and they are different from α) of degree 3, so that its Galois group is $\mathbb{Z}/3\mathbb{Z}$ (which is the only group with 3 elements up to isomorphism).
3. Via the action on the roots of f, the Galois group is embedded in S_3. Since the only subgroup of S_3 containing 3 elements is A_3, the image of $\mathrm{Gal}(K/\mathbb{Q})$ in S_3 via this embedding is A_3, and the discriminant of f is a square in $\mathbb{Q}^\times$ as seen in class.

   Using the given formula we see indeed that $\Delta = +4 \cdot 27 - 27 = 3 \cdot 27 = 9^2 \in \mathbb{Q}^\times$.

3. Let n be a positive integer. Prove that the symmetric group S_n is generated by the cycle $(1\ 2\ \cdots\ n)$ and $\tau = (a\ b)$, if $b - a$ is coprime with n.

Solution: Without loss of generality, assume that $b > a$. Then $\langle \sigma^{b-a} \rangle = \langle \sigma \rangle$ by hypothesis, so that $\langle \sigma, (a\ b) \rangle = \langle \sigma^{b-a}, (a\ b) \rangle$ and since $\sigma^{b-a}(a) = b$, up to renaming the elements permuted by S_n we can assume without loss of generality that $(a\ b) = (1\ 2)$.

It is easily seen that for each transposition $(\alpha\ \beta)$ and permutation γ one has $\gamma(\alpha\ \beta)\gamma^{-1} = (\gamma(\alpha)\ \gamma(\beta))$. Then $\sigma^k(1\ 2)\sigma^{-k} = (k+1\ k+2)$ for each $0 \leq k \leq n-2$, so that $\langle \sigma, (1\ 2) \rangle$ contains all the transpositions $(k\ k+1)$ for $1 \leq k \leq n-1$.

We now prove that $\langle \sigma, (1\ 2) \rangle = \langle \sigma, (1\ 2), (2\ 3), \ldots, (n-1\ n) \rangle$ contains all transpositions. Each permutation can be written as $(\alpha\ \beta)$ with $\beta > \alpha$, and we work by induction on $\beta - \alpha$, the case $\beta - \alpha = 1$ being trivial. Suppose that we have proven that all permutations between two elements whose difference is strictly smaller then $\beta - \alpha$ do lie in $\langle \sigma, (1\ 2) \rangle$. Then applying $\gamma(\alpha\ \beta)\gamma^{-1} = (\gamma(\alpha)\ \gamma(\beta))$ for $\gamma = (\beta - 1\ \beta)$ we get $(\beta - 1\ \beta)(\alpha \beta - 1)(\beta - 1\ \beta) = (\alpha\ \beta) \in \langle \sigma, (1\ 2) \rangle$ by inductive hypothesis.

See next page!

To conclude, we just have to notice that the set of all transpositions generates S_n, since every permutation can be written as a product of disjoint cycles, and a cycle $(a_1\ a_2\ \dots a_t)$ can be written as $(a_1\ a_t)(a_1\ a_{t-1})\cdots(a_1\ a_2)$

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.]

Solution:

1. Decomposing a complex number into real and imaginary part $z = x + iy$ one easily checks that $z \mapsto \bar{z}$ respects sum and multiplication, and fixes 0 and 1, so that it is a field automorphism of $\mathbb{C}$ (bijectivity is immediate from the fact that it is its own inverse). Moreover, conjugates of roots of $f \in \mathbb{Q}$ are still roots of f (since $f(\overline{x}) = \overline{f(x)}$), so that complex conjugation restricts to an automorphism of L_f. Since it only interchanges the 2 non-real roots, its image in H is a transposition.
2. For x any root of f, we have that $p = \deg(f) = [\mathbb{Q}(x) : \mathbb{Q}] | [L_f : \mathbb{Q}] = |G|$ by multiplicativity of the degree in towers of extensions, so that p divides the order of G. Then by the First Sylow Theorem G has a p-subgroup, and given a non-trivial element g of this subgroup has order p^a for some positive a. Then $g^{p^{a-1}} \in G$ has order p.
3. The image of the element of order p via the embedding in S_p is a p-cycle, and up to reordering the roots we can assume it is the cycle $(1\ 2\ \cdots\ p) \in H$. The transposition in H from Point 1 can be written as $(a\ b)$ for some $a, b \in \{1, \dots, p\}$, and clearly $b - a$ is coprime with p, so that we can apply the previous Exercise to get that $H = S_p$.

The polynomial $f(X) = X^5 - 4X + 2$ has prime degree $p = 5$, and is irreducible by Eisenstein's criterion. We have $\frac{d}{dX} f(X) = 5X^4 - 4$, and this derivative is positive when evaluated on $x \in \mathbb{R}$ if and only if $|x| \geq \sqrt[4]{\frac{4}{5}}$, so that f, viewed as a function $\mathbb{R} \longrightarrow \mathbb{R}$,

Please turn over!

has stationary points $\pm\sqrt[4]{\frac{4}{5}}$. The negative is a maximum, the positive is a minimum. Evaluating the function there we get

$$f(\sqrt[4]{-\frac{4}{5}}) = -\frac{4}{5}(\frac{4}{5} - 4) + 2 > 0$$
$$f(\sqrt[4]{\frac{4}{5}}) = \frac{4}{5}(\frac{4}{5} - 4) + 2 < 0.$$

Then f is easily seen to have three real zeroes (two smaller than $\frac{4}{5}$ and one bigger), so that it has precisely 2 non-real roots and we are in position to apply what we proved and conclude that the Galois group of L_f is S_5.