Math 30820 Honors Algebra 4
Homework 8

Andrei Jorza

Due Wednesday, 3/22/2017

Do 6 of the following questions. Some questions may be obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.

Throughout this problem set $\Phi_n(X)$ is the n-th cyclotomic polynomial.

1. For a positive integer n we denote by $s(n)$ the largest square-free divisor of n. Show that
$$\Phi_n(X) = \Phi_{s(n)}(X^{n/s(n)})$$
[Hint: Use the Möbius inversion formula.]

Proof. From class
$$\Phi_n(X) = \prod_{d|n}(X^{n/d}-1)^{\mu(d)}$$
and since $\mu(d) = 0$ unless d is square-free we get
$$\Phi_n(X) = \prod_{d|n, d \text{ square-free}}(X^{n/d}-1)^{\mu(d)}$$
The set of square-free divisors d of n is the same as the set of divisors of $s(n)$ (by factorization into primes) so
$$\Phi_n(X) = \prod_{d|s(n)}(X^{n/d}-1)^{\mu(d)} = \prod_{d|s(n)}((X^{n/s(n)})^{s(n)/d}-1)^{\mu(d)} = \Phi_{s(n)}(X^{n/s(n)})$$
□

2. Show that
$$\Phi_n(1) = \begin{cases} 0 & n = 1 \\ p & n = p^a \\ 1 & n = p_1^{a_1}\cdots p_k^{a_k}, k \geq 2 \end{cases}$$
[Hint: Use induction.]

Proof. Since $\Phi_1(X) = X - 1$ we get that
$$(X^n-1)/(X-1) = \prod_{d|n, d\neq 1}\Phi_d(X)$$

so using L'Hôpital we get $n = \prod_{d|n, d\neq 1} \Phi_d(1)$. We now prove by induction on n. Suppose we know the formula for integers $< n$. Then

$$\Phi_n(1) = \frac{n}{\prod_{d|n, d\neq 1, n} \Phi_d(1)}$$

As $\Phi_d(1) = 1$ if $d < n$ is not a prime power by the inductive hypothesis we can rewrite this as

$$\Phi_n(1) = \frac{n}{\prod_{p^k|n} \Phi_{p^k}(1)} = \frac{n}{\prod_{p^k|n, p^k\neq n} p}$$

When n is not a prime power then $\prod_{p^k|n, p^k\neq n} p$ is exactly the power of p in the factorization of n, for each prime p. Therefore the answer is $\Phi_n(1) = 1$. If $n = p^m$ then $\prod_{p^k|n, p^k\neq n} p = p^{m-1}$ as we need to omit the divisor p^m. Then $\Phi_{p^m}(1) = p$. □

3. Show that

$$\prod_{1\leq k\leq n, (k,n)=1} \sin\left(\frac{k\pi}{n}\right) = \frac{\Phi_n(1)}{2^{\varphi(n)}}$$

where φ is Euler's function. Remark that $\Phi_n(1)$ is computed in the previous problem. [Hint: Write $\Phi_n(1)$ as a product over the primitive roots of 1 and use double angle formulas.]

Proof. We have

$$\begin{aligned}
\Phi_n(1) &= \prod_{(k,n)=1} (1 - \zeta_n^k) \\
&= \prod_{(k,n)=1} (1 - \cos(2\pi k/n) - i\sin(2\pi k/n)) \\
&= \prod_{(k,n)=1} 2\sin(\pi k/n)(\sin(\pi k/n) - i\cos(\pi k/n)) \\
&= 2^{\varphi(n)} \prod_{(k,n)=1} \sin(\pi k/n) \prod_{(k,n)=1} e^{\pi ik/n - \pi i/2}
\end{aligned}$$

therefore it suffices to show that the last product is 1. But this is

$$\prod_{(k,n)=1} e^{\pi ik/n - \pi i/2} = e^{-\pi i\varphi(n)/2} e^{\sum_{(k,n)=1} \pi ik/n}$$

Note that $(k, n) = 1$ iff $(n - k, n) = 1$ so in the sum $\sum_{(k,n)=1} k$ we can pair k and $n - k$ and we find $\sum_{(k,n)=1} k = n\varphi(n)/2$. Therefore the last product is

$$e^{\pi in\varphi(n)/(2n) - \pi i\varphi(n)/2} = 1$$

□

4. Let p be a prime. Let F be the union of the fields of rational functions $\mathbb{F}_p(x) \subset \mathbb{F}_p(\sqrt[p]{x}) \subset \mathbb{F}_p(\sqrt[p^2]{x}) \subset \ldots \subset \mathbb{F}_p(\sqrt[p^n]{x}) \subset \ldots$. Show that F is the smallest perfect field containing $\mathbb{F}_p(x)$.

Proof. First, note that the union F of these fields of rational functions is a field itself. Indeed, if $F_0 \subset F_1 \subset \dots$ are fields then $F = \bigcup F_n$ is a field. If $x, y \in F$ then $x, y \in F_n$ for n large enough and then $x + y, xy, x/y \in F_n \subset F$ so F is a field. If $a \in F = \bigcup \mathbb{F}_p(\sqrt[p^n]{x})$ then $a = f(\sqrt[p^n]{x})$ for a rational function $f(y) \in \mathbb{F}_p(y)$ and n large enough. But then $(f(\sqrt[p^{n+1}]{x})^p = f(\sqrt[p^n]{x}) = a$ and since $f(\sqrt[p^{n+1}]{x}) \in \mathbb{F}_p(\sqrt[p^{n+1}]{x}) \subset F$ we deduce that $\phi(y) = y^p$ is surjective on F. Therefore F is perfect.

Suppose F is perfect and contains $\mathbb{F}_p(x)$. We'll prove by induction that $\mathbb{F}_p(\sqrt[p^n]{x}) \subset F$. The base case is $n = 1$. There exists $a \in F$ such that $\phi(a) = x$ and so $a^p = x$. But then $(a - \sqrt[p]{x})^p = 0$ so $a = \sqrt[p]{x}$ which means that $\sqrt[p]{x} \in F$ and so $\mathbb{F}_p(\sqrt[p]{x}) \subset F$ as well. For the inductive step we can use the above argument replacing x by $\sqrt[p^n]{x}$. □

5. Let p be a prime and $K = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$ be the splitting field of $X^p - 2 \in \mathbb{Q}[X]$. Show that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$ consisting of matrices of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. (Recall from last semester that this group, in turn, is of the form $\mathbb{F}_p \rtimes \mathbb{F}_p^\times$.)

Proof. In class we showed that if $g = \begin{pmatrix} a & b \\ & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_p)$ then we get $\sigma_g \in \mathrm{Gal}(K/\mathbb{Q})$ that sends ζ_p to ζ_p^a and $\zeta = \sqrt[p]{2}$ to $\zeta_p^b \alpha$. We also showed that this was a bijection. It suffices to check that it is a group homomorphism. Certainly σ_{I_2} is the identity automorphism so we only need to show that $\sigma_g \circ \sigma_h = \sigma_{gh}$. If $g = \begin{pmatrix} a & b \\ & 1 \end{pmatrix}$ and $h = \begin{pmatrix} c & d \\ & 1 \end{pmatrix}$ then $gh = \begin{pmatrix} ac & ad + b \\ & 1 \end{pmatrix}$. To verify the composition we only need to show that the two sides agree on ζ_p and on α. But

$$\sigma_g \circ \sigma_h(\zeta_p) = \sigma_g(\zeta_p^c) = \sigma_g(\zeta_p)^c = \zeta_p^{ac} = \zeta_{gh}(\zeta_p)$$

and

$$\zeta_g \circ \zeta_h(\alpha) = \zeta_g(\zeta_p^d \alpha) = \zeta_g(\zeta_p)^d \zeta_g(\alpha) = \zeta_p^{ad} \zeta_p^b \alpha = \zeta_{gh}(\alpha)$$

□

6. Let K be the splitting field over $\mathbb{Q}$ of $X^8 - 2$. Show that $\mathrm{Gal}(K, \mathbb{Q}(i)) \cong \mathbb{Z}/8\mathbb{Z}$ and $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{2})) \cong D_8$, the dihedral group with 8 elements.

Proof. Write $\alpha = \sqrt[8]{2}$. We saw in class that $\zeta_8 = (1 + i)/\sqrt{2}$ and so $K = \mathbb{Q}(\zeta_8, \alpha) = \mathbb{Q}(i, \alpha)$. Then $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is uniquely determined by $\sigma(i) \in \{\pm i\}$ and $\sigma(\alpha) \in \{\zeta_8^a \alpha | 0 \le a < 8\}$. Since there are 16 possible choices for $\pm i$ and a, and $[K : \mathbb{Q}] = 16$ (from class), each choice yields a Galois automorphism. Denote by $\sigma_{\pm,a}$ the Galois automorphism such that $\sigma_{\pm,a}(i) = \pm i$ and $\sigma_{\pm,a}(\alpha) = \zeta_8^a \alpha$.

If $\sigma_{\pm,a} \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{2}))$ it follows that $\sigma_{\pm,a}(\sqrt{2}) = \sqrt{2}$. But $\sigma_{\pm,a}(\sqrt{2}) = \sigma_{\pm,a}(\alpha)^4 = \zeta_8^{4a} \alpha^4 = (-1)^a \sqrt{2}$. Therefore $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{2})) = \{\sigma_{\pm,a} \mid 2 \mid a\}$. Let $\sigma = \sigma_{+,2}$, sending i to i and α to $i\alpha$, and $\tau = \sigma_{-,0}$, sending i to $-i$ and α to α. Then $\sigma^4 = 1$ and $\tau^2 = 1$ and $\tau\sigma\tau = \sigma^{-1}$ as they both send i to i and α to $-i\alpha$. Since σ and τ generated D_8 and $\mathrm{Gal}(\mathbb{Q}(i, \alpha)/\mathbb{Q}(\sqrt{2}))$ has order 8 we deduce that $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{2})) \cong D_8$.

Similarly, $\sigma_{\varepsilon,a} \in \mathrm{Gal}(K/\mathbb{Q}(i))$ iff $\sigma_{\varepsilon,a}(i) = i$, i.e., iff $\varepsilon = 0$. Write $\sigma = \sigma_{0,1}$. Then $\sigma(\alpha) = \zeta_8 \alpha$, $\sigma(i) = i$ and $\sigma(\zeta_8) = (1 + i)/\sigma(\sqrt{2}) = (1 + i)/\sigma(\alpha)^4 = -\zeta_8$. We deduce that σ has order 8 and therefore $\mathrm{Gal}(K/\mathbb{Q}(i)) = \langle\sigma\rangle \cong \mathbb{Z}/8\mathbb{Z}$. □

7. Let $\alpha_1 = \sqrt{1 + \sqrt{3}}$, $\alpha_2 = \sqrt{1 - \sqrt{3}}$, two roots of the irreducible polynomial $X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$.
   (a) Show that $\mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2) = \mathbb{Q}(\sqrt{3})$.
   (b) Show that $\mathbb{Q}(\alpha_1)$, $\mathbb{Q}(\alpha_2)$ and $\mathbb{Q}(\alpha_1, \alpha_2)$ are Galois over $\mathbb{Q}(\sqrt{3})$ and that $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2)/\mathbb{Q}(\sqrt{3})) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. (a): Since $\mathbb{Q}(\alpha_1)$ and $\mathbb{Q}(\alpha_2)$ have order 4 over $\mathbb{Q}$ and it's clear that $\mathbb{Q}(\sqrt{3})$ is in the intersection, either the intersection is $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$. However, $\mathbb{Q}(\alpha_1) \subset \mathbb{R}$ whereas $\mathbb{Q}(\alpha_2)$ is not in $\mathbb{R}$.

(b): $\mathbb{Q}(\alpha_1)$ and $\mathbb{Q}(\alpha_2)$ are quadratic over $\mathbb{Q}(\sqrt{3})$ so they are Galois with Galois group $\mathbb{Z}/2\mathbb{Z}$. Therefore their composite $\mathbb{Q}(\alpha_1, \alpha_2)$ is also Galois over $\mathbb{Q}$ and has Galois group $(\mathbb{Z}/2\mathbb{Z})^2$. □

8. Show that $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is Galois over $\mathbb{Q}$ and that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

Proof. The roots of the minimal polynomial $(X^2-2)^2 - 2 = X^4 - 4X^2 + 2$ (irreducible by Eisenstein) are $\pm\sqrt{2 \pm \sqrt{2}}$. To show $K/\mathbb{Q}$ is Galois it suffices to show that $\sqrt{2-\sqrt{2}} \in K$ as well. But $\sqrt{2-\sqrt{2}} = \sqrt{2}/\sqrt{2+\sqrt{2}}$ and the RHS fraction is clearly in K.

Let $\alpha = \sqrt{2+\sqrt{2}}$ in which case $\sqrt{2} = \alpha^2 - 2$ and $\sqrt{2-\sqrt{2}} = \sqrt{2}/\alpha$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ defined by $\sigma(\alpha) = \sqrt{2-\sqrt{2}}$. Then clearly $\sigma(\sqrt{2}) = -\sqrt{2}$ so $\sigma(\sqrt{2-\sqrt{2}}) = -\alpha$. Therefore $\sigma^2(\alpha) = -\alpha$ and so $\sigma^4 = 1$ with $\sigma^2 \neq 1$. Thus $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}/4\mathbb{Z}$. □