Math 30820 Honors Algebra 4
Homework 10

Andrei Jorza

Due Wednesday, 4/5/2017

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. Suppose K/F is a finite Galois extension and H is a subgroup of $\mathrm{Gal}(K/F)$. Show that $\sigma(K^H) = K^{\sigma H \sigma^{-1}}$.

   Proof. Note that $y = \sigma(x) \in \sigma(K^H)$ if and only if $x = \sigma^{-1}(y) \in K^H$, i.e., iff $h(x) = x$ iff $h(\sigma^{-1}(y)) = \sigma^{-1}(y)$ iff $y \in K^{\sigma H \sigma^{-1}}$ as desired. □

2. Let $P(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree 4 with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Let $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$ and $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$. Show that $Q(X) = (X - \beta_1)(X - \beta_2)(X - \beta_3)$ is an separable polynomial in $\mathbb{Q}[X]$.

   Proof. Note that $\beta_1 - \beta_2 = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$ so $\beta_1 \neq \beta_2$ as $P(X)$ is separable (irreducible over perfect base). Similarly we get $Q(X)$ is separable.

   The entire symmetric group S_4 acts transitively on $\{\beta_1, \beta_2, \beta_3\}$ (see Exercise 9-10 from Homework 6 last semester). Therefore $\mathrm{Gal}(K/\mathbb{Q}) \subset S_4$ permutes the set of roots of $Q(X)$ and so fixes $Q(X)$. So $Q(X) \in K^{\mathrm{Gal}(K/\mathbb{Q})}[X] = \mathbb{Q}[X]$. □

3. Let $p > 2$ be a prime such that $\mathbb{Q}(\zeta_p, \sqrt[p]{2}) \cap \mathbb{Q}(\zeta_p, \sqrt[p]{3}) = \mathbb{Q}(\zeta_p)$. Find a homomorphism $\phi : \mathbb{F}_p^\times \to \mathrm{GL}(2, \mathbb{F}_p) = \mathrm{Aut}(\mathbb{F}_p^2)$ such that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p, \sqrt[p]{2}, \sqrt[p]{3})/\mathbb{Q}) \cong \mathbb{F}_p^2 \rtimes_\phi \mathbb{F}_p^\times$$

   Proof. In class I showed that $\mathrm{Gal}(\mathbb{Q}(\zeta_p, \sqrt[p]{2}, \sqrt[p]{3})/\mathbb{Q})$ consists of pairs $\{\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & d \\ 0 & 1 \end{pmatrix}\right)\}$. This is in bijection with $\mathbb{F}_p^2 \rtimes_\varphi \mathbb{F}_p^\times$ the pair $\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & d \\ 0 & 1 \end{pmatrix}\right)$ corresponding to $(a, (b, c))$. It suffices to check this bijection is a homomorphism for a suitable choice of φ..

   We compute products in the Galois group as

$$\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & d \\ 0 & 1 \end{pmatrix}\right)\left(\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a' & d' \\ 0 & 1 \end{pmatrix}\right) = \left(\begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} aa' & ad' + d \\ 0 & 1 \end{pmatrix}\right)$$

   In the semidirect product this product is

$$(a, (b, d)) \cdot_\varphi (a', (b', d')) = (aa', (b, d) + \varphi_a(b', d'))$$

   and comparing with the above formula we see that $\varphi_a(b', d') = (ab', ad')$ works. Therefore the Galois group is $\cong \mathbb{F}_p^2 \rtimes_\varphi \mathbb{F}_p^\times$ where $\varphi : \mathbb{F}_p^\times \to \mathrm{GL}(2, \mathbb{F}_p)$ is $\varphi(a) = aI_2$. □

4. Artin 16.1.1 on page 505.

Proof. Let P be the given polynomial, $\sigma = (12)$, and $\tau = (123)$.

(a): Clearly $\tau P = P$ so A_3 fixes P. However, $\sigma P = u_1u_2^2 + u_2u_3^2 + u_3u_1^2 = Q$ and we deduce that $S_3P = \{P, Q\}$.

(b): This is symmetric and the easiest way to find the polynomial expression is that

$$P = (s_1 - u_1)(s_1 - u_2)(s_1 - u_3) = s_1^3 - s_1s_1^2 + s_2s_1 - s3 = s_1s_2 - s_3$$

(c): This is the discriminant of the polynomial $(X - u_1)(X - u_2)(X - u_3)$ so P is fixed by A_3 and any transposition changed the sign of P so $S_3P = \{\pm P\}$.

(d): Again $\tau P = P$ by inspection and $\sigma P = -P$ so the orbit is $S_3P = \{\pm P\}$.

(e): P is symmetric and since $u_i^3 - s_1u_i^2 + s_2u_i - s_3 = 0$ for all i we deduce that

$$\sum u_i^3 = s_1 \sum u_i^2 - s_2 \sum u_i + \sum s_3 = s_1(s_1^2 - 2s_2) - s_1s_2 + ns_3$$

□

5. Artin 16.5.2 on page 507.

Proof. $\mathrm{Aut}(\mathbb{C}(t)/\mathbb{C}) \cong \mathrm{PGL}(2, \mathbb{C})$ and σ corresponds to the matrix $A = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$ while τ corresponds to the matrix $\begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}$. Then $A^3 = (2i + 2)I_2$ and A has order 3 in $\mathrm{PGL}(2, \mathbb{C})$ while $B^3 = (2 - 2i)I_2$ so B has order 3 in $\mathrm{PGL}(2, \mathbb{C})$. We further compute that $C = AB$ has order 2. From last semester we know that A_4 is generated by 3-cycles and in fact for A_4 two 3-cycles suffice ((123) and (234) for example). The map $A \mapsto (123)$ and $B \mapsto (234)$ is then a group isomorphism.

To find $\mathbb{C}(t)^{A_4}$ first find $\mathbb{C}(t)^V$ where $V \lhd A_4$ is the unique proper normal subgroup, isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ and consisting of products of disjoint transpositions. Explicitly in terms of the maps σ, τ, $V = \{1, \sigma\tau, \tau\sigma, \sigma^2\tau\sigma^2\}$ where $\sigma\tau(t) = -t$, $\tau\sigma(t) = -1/t$ and $\sigma^2\tau\sigma^2(t) = 1/t$. Clearly $P = t^2 + 1/t^2$ is fixed by V and since $P = (t^4 + 1)/t^2$ with numerator of degree 4 we deduce that $[\mathbb{C}(t) : \mathbb{C}(P)] = 4$ and so $\mathbb{C}(P) = \mathbb{C}(t)^V$.

Next, we compute $\mathbb{C}(t)^{A_4} = \mathbb{C}(P)^\sigma$ as A_4 is generated by V and a 3-cycle. We compute $\sigma(P) = 2(P - 6)/(P + 2)$ and $\sigma^2(P) = -2(P + 6)/(P - 2)$. The rational function $Q = P + \sigma(P) + \sigma^2(P) = (t^4 + 1)(t^8 - 34t^4 + 1)/(t^2(t^4 - 1)^2)$ is then invariant by σ clearly and so $Q \in \mathbb{C}(t)^{A_4}$. Again as the numerator has degree 12 we deduce that $\mathbb{C}(Q) = \mathbb{C}(t)^{A_4}$. □

6. Artin 16.9.14 on page 509.

Proof. (a): Write $\zeta = \zeta_3$, $\alpha = \sqrt[3]{2 + \sqrt{2}}$, $u = \sqrt[3]{2}$ and $\beta = \sqrt[3]{2 - \sqrt{2}} = u/\alpha$. The splitting field is $K = \mathbb{Q}(\zeta, \alpha, \beta) = \mathbb{Q}(\zeta, u, \alpha)$. Every automorphism fixing F must take $u \mapsto \zeta^* u$ and α to either $\zeta^*\alpha$ or $\zeta^*\beta$. Let $\sigma(u) = \zeta u$ and $\sigma(\alpha) = \alpha$ so necessarily $\sigma(\beta) = \sigma(u/\alpha) = \zeta\beta$ and let $\tau(u) = \zeta u$ and $\tau(\alpha) = \beta$ so necessarily $\tau(\beta) = \tau(u/\alpha) = \zeta u/\beta = \zeta\alpha$. Then σ has order 3 and $\tau^2(\alpha) = \tau(\beta) = \zeta\alpha$, $\tau^3(\alpha) = \tau(\zeta\alpha) = \zeta\beta$, $\tau^4(\alpha) = \tau(\zeta\beta) = \zeta^2\alpha$, $\tau^5(\alpha) = \zeta^2\beta$ and finally $\tau^6(\alpha) = \alpha$. We deduce that τ has order 6. Together σ and τ generate all possible 18 choices for $u \mapsto \zeta^* u$ and $\alpha \mapsto \zeta^*\alpha$ or $\zeta^*\beta$.

Also note that if $\eta = \tau^2\sigma^2$ then η has order 3 and $\sigma\eta = \eta\sigma$ so $\langle\sigma, \eta\rangle \cong (\mathbb{Z}/3\mathbb{Z})^2$ is the necessarily unique normal Sylow 3-subgroup of this order 18 group (it is normal as it has index 2). The order 2 element τ^3 permutes σ and η and therefore the order 18 group $\langle\sigma, \tau\rangle \cong (\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$ where the homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/3\mathbb{Z})^2)$ sends 1 to the antidiagonal matrix in $\mathrm{GL}(2, \mathbb{F}_3)$.

Now α satisfies the degree 6 polynomial $(X^3-2)^2-2$ over F and this is irreducible by Eisenstein as from last semester 2 is a prime in $\mathbb{Z}[\zeta]$ as $2 \equiv 2 \pmod 3$. We deduce that $6 \mid [K:F]$ and so the Galois group $G = \mathrm{Gal}(K/F)$ is a subgroup of $(\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$ of order divisible by 6. Therefore either G is the whole order 18 semidirect product or is it $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. We'll show that in fact $G \cong (\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

We'll argue by contradiction. Suppose G has order 6 in which case it is generated by an order 3 and an order 2 element. The order 3 element is in $\langle \sigma, \eta \rangle$ and therefore it will stabilize an element γ which is cubic over $\mathbb{Q}(\sqrt{2})$. E.g., $\sigma\eta = \tau^2$ stabilizes $\gamma = \alpha/\beta = \sqrt[3]{\frac{2+\sqrt{2}}{2-\sqrt{2}}}$, etc. Since cubic fields don't contain quadratic subfields, γ is then also stabilized by the order 2 element of G so $\gamma \in K^G = \mathbb{Q}$, which is not true as γ is cubic over $\mathbb{Q}(\sqrt{2})$.

(b): Again, write $\zeta = \zeta_3$ and $\alpha_i = \sqrt{2+\zeta^i u}$. The polynomial $P(X) = (X^2-2)^3 - 2 = X^3 - 6X^4 + 12X^2 - 10$ is irreducible over F again by the Eisenstein irreducibility criterion as 2 is prime in $\mathbb{Z}[\zeta]$. Therefore K is the splitting field of $P(X)$ with roots $\pm\alpha_i$. Order the roots $r_1 = \alpha_0, r_2 = -\alpha_0, r_3 = \alpha_1, r_4 = -\alpha_1, r_5 = \alpha_2, r_6 = -\alpha_2$ and so $6 \mid [K:\mathbb{Q}]$. If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ then σ permutes $\{r_1, \ldots, r_6\}$ and $\sigma \in S_6$. Since $\alpha_0^2 = \alpha_1^2/\zeta = \alpha_2^2/\zeta^2$ we deduce that $\sigma(\alpha_0)^2 = \sigma(\alpha_1)^2/\zeta = \sigma(\alpha_2)^2/\zeta^2$. This implies that σ permutes the pairs $\{(r_1,r_2),(r_3,r_4),(r_5,r_6)\}$ and therefore G is in the subset of S_6 generated by S_3 and $(12)(34)(56)$ where S_3 is the group of permutations of the set of three pairs from before. Let H be this subgroup of S_6. Since $S_3 < H$ has index 2 it is normal and we see that $H = S_3 \rtimes \mathbb{Z}/2\mathbb{Z}$. But conjugating by $(12)(34)(56)$ doesn't affect the pairs $(r_1,r_2),(r_3,r_4),(r_5,r_6)$ and so the conjugation homomorphism $\langle (12)(34)(56) \rangle \cong \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(S_3)$ is trivial and therefore $H \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$. We'll show that $G = H$.

We know that $6 \mid |G|$ and so $G < S_3 \times \mathbb{Z}/2\mathbb{Z}$ of order divisible by 6. We only need to exclude the case $|G| = 6$. Let $\sigma \in G$ of order 3. Then σ generates A_3 in S_3 and therefore cycles through the pairs $(r_1,r_2),(r_3,r_4),(r_5,r_6)$. But the σ fixes $\alpha_0\alpha_1\alpha_2 = \sqrt{10}$. Comparing degrees it would have to be that $K^\sigma = \mathbb{Q}(\zeta, \sqrt{10})$. However, σ also fixes the sum $\gamma = \alpha_0 + \alpha_1 + \alpha_2$ so it would suffice to show that $\gamma \notin \mathbb{Q}(\zeta, \sqrt{10})$. Otherwise $\alpha_0 + \alpha_1 + \alpha_2 = a + b\sqrt{10}$ for $a, b \in \mathbb{Q}(\zeta)$ so $(\alpha_0 + \alpha_1 + \alpha_2 - a)^2 = 10b^2$. Expanding the LHS yields a cubic whereas $10b^2$ is quadratic over $\mathbb{Q}$. □

7-8 (This is worth 2 problems) Let p be an odd prime. The point of this exercise is to show that $\mathbb{Q}(\zeta_{p^2}) \cap \mathbb{Q}(\sqrt[p^2]{2}) = \mathbb{Q}$. Write $K = \mathbb{Q}(\zeta_{p^2}) \cap \mathbb{Q}(\sqrt[p^2]{2})$.

(a) Show that $\mathbb{Q}(\zeta_{p^2}) \cap \mathbb{Q}(\sqrt[p]{2}) = \mathbb{Q}$.

(b) If $K \neq \mathbb{Q}$ show that $K/\mathbb{Q}$ is Galois of order p.

(c) Show that $K\mathbb{Q}(\sqrt[p]{2}) = \mathbb{Q}(\sqrt[p^2]{2})$ and deduce that $\mathbb{Q}(\sqrt[p^2]{2})/\mathbb{Q}(\sqrt[p]{2})$ is Galois.

(d) Show that this extension is never Galois and therefore $K = \mathbb{Q}$.

(e) Show that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^2}, \sqrt[p^2]{2})/\mathbb{Q})$ is isomorphic to the matrix group $\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/p^2\mathbb{Z})^\times, b \in \mathbb{Z}/p^2\mathbb{Z}\}$.

Proof. (a): If $L = \mathbb{Q}(\zeta_{p^2}) \cap \mathbb{Q}(\sqrt[p]{2})$ then $[L:\mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}] = p$ so either $L = \mathbb{Q}$ as desired or $\mathbb{Q}(\sqrt[p]{2}) \subset \mathbb{Q}(\zeta_{p^2})$. This cannot be as the former is not Galois over $\mathbb{Q}$ whereas every subfield of the cyclotomic field is Galois as $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times$ is abelian.

(b): Again, $K \subset \mathbb{Q}(\zeta_{p^2})$ and so $K/\mathbb{Q}$ must be Galois. Moreover, $[K:\mathbb{Q}] \mid \gcd([\mathbb{Q}(\zeta_{p^2}):\mathbb{Q}][\mathbb{Q}(\sqrt[p^2]{2}):\mathbb{Q}]) = \gcd(p(p-1), p^2) = p$. So if $K \neq \mathbb{Q}$ then $[K:\mathbb{Q}] = p$.

(c): As $\mathbb{Q}(\sqrt[p]{2})/\mathbb{Q}$ is not Galois but $K/\mathbb{Q}$ is Galois we deduce, as in (a), that $K \cap \mathbb{Q}(\sqrt[p]{2}) = \mathbb{Q}$. Therefore $[K\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}(\sqrt[p]{2})] = [K:\mathbb{Q}] = p$ and by comparing degrees we get $K\mathbb{Q}(\sqrt[p]{2}) = \mathbb{Q}(\sqrt[p^2]{2})$. Moreover, $K\mathbb{Q}(\sqrt[p]{2})/\mathbb{Q}(\sqrt[p]{2})$ is Galois with Galois group isomorphic to $\mathrm{Gal}(K/\mathbb{Q})$ and so $\mathbb{Q}(\sqrt[p^2]{2})/\mathbb{Q}(\sqrt[p]{2})$ is Galois with Galois group necessarily isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

(d): If $\mathbb{Q}(\sqrt[p^2]{2})/\mathbb{Q}(\sqrt[p]{2})$ is Galois then the minimal polynomial $X^p - \sqrt[p]{2}$ of $\sqrt[p^2]{2}$ over $\mathbb{Q}[\sqrt[p]{2})$ would have all roots in $\mathbb{Q}(\sqrt[p^2]{2})$. But then $\zeta_p \in \mathbb{Q}(\sqrt[p^2]{2})$ and this field is in $\mathbb{R}$ whereas ζ_p is not.

(e): Every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2}, \sqrt[p^2]{2})/\mathbb{Q})$ sends ζ_{p^2} to $\zeta_{p^2}^a$ for some $a \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ and $\sqrt[p^2]{2}$ to $\zeta_{p^2}^b \sqrt[p^2]{2}$ for some $b \in \mathbb{Z}/p^2\mathbb{Z}$. There are $p^3(p-1)$ choices for (a, b) and the Galois group has $[\mathbb{Q}(\zeta_{p^2}, \sqrt[p^2]{2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{p^2}, \sqrt[p^2]{2}) : \mathbb{Q}(\sqrt[p^2]{2})][\mathbb{Q}(\sqrt[p^2]{2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}][\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p^3(p-1)$. □