Math 30820 Honors Algebra 4
Homework 12

Andrei Jorza

Due Wednesday, 4/26/2017

Do 8 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.

1. Consider the variables $x_1, \dots, x_n, t$ and the Taylor expansion

$$\phi_t(x) = \frac{xt}{1-e^{-xt}} = 1 + \frac{x}{2}t + \frac{x^2}{12}t^2 - \frac{x^4}{720}t^4 + O(t^6)$$

Let $c_1 = x_1 + \cdots + x_n$, $c_2 = \sum x_i x_j$, $\dots$, $c_n = x_1 \cdots x_n$ be the elementary symmetric polynomials. Show that

$$\phi_t(x_1)\phi_t(x_2)\cdots\phi_t(x_n) = 1 + \frac{c_1}{2}t + \frac{c_1^2+c_2}{12}t^2 + \frac{c_1c_2}{24}t^3 + \frac{-c_1^4+4c_1^2c_2+c_1c_3+3c_2^2-c_4}{720}t^4 + O(t^5)$$

[Hint: This is really just a question about symmetric polynomials written in terms of elementary symmetric polynomials.] (The LHS is referred to as the Todd class while the c_i are referred to as Chern classes.)

Proof.

$$\prod \phi_t(x_i) = \prod_i (1 + x_i t/2 + x_i^2t^2/12 - x_i^4t^4/720 + O(t^5)) = 1 + \sum x_i t/2 + t^2(\sum x_i^2/12 + \sum_{i<j} x_ix_j/4) +$$

$$+t^3(\sum_{i<j} x_i^2x_j/24 + x_ix_j^2/24 + \sum_{i<j<k} x_ix_jx_k/8) +$$

$$t^4(-\sum x_i^4/720 + \sum_{i<j} x_i^2x_j^2/144 + \sum_{i<j<k}(x_i^2x_jx_k + x_ix_j^2x_k + x_ix_jx_k^2)/48 + \sum_{i<j<k<l} x_ix_jx_kx_l/16) + O(t^5)$$

and we just need to check that

$$c_1 = \sum x_i$$

$$c_1^2 + c_2 = \sum x_i^2 + 3\sum_{i<j} x_ix_j$$

$$c_1c_2 = \sum_{i<j} x_i^2x_j + x_ix_j^2 + 3\sum_{i<j<k} x_ix_jx_k$$

$$-c_1^4 + 4c_1^2c_2 + c_1c_3 + 3c_2^2 - c_4 = -\underbrace{\sum x_i^4}_{A} + 5\underbrace{\sum_{i<j} x_i^2x_j^2}_{B} + 15\underbrace{\sum_{i<j<k}(x_i^2x_jx_k + x_ix_j^2x_k + x_ix_jx_k^2)}_{C} + 45\sum_{i<j<k<l} x_ix_jx_kx_l$$

Of these only the last one is not straightforward. But $\sum x_i^2 = c_1^2 - 2c_2$ so $(c_1^2-2c_2)^2 = (\sum x_i^2)^2 = A + 2B$, $c_2^2 = B + 6c_4 + 2C$ and $c_1c_3 - 4c_4 = C$. Putting everything together yields the desired formula.

□

2. Let $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Q}[X]$ be any monic polynomial. Show that for every $\varepsilon > 0$ there exists a polynomial $Q(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in \mathbb{Q}[X]$ such that (a) $|b_k - a_k| < \varepsilon$ for all k and (b) $Q(X)$ is irreducible in $\mathbb{Q}[X]$. [Hint: You can produce $Q(X)$ that satisfies the hypotheses of the Eisenstein irreducibility criterion for a ring of the form $R = \frac{1}{N}\mathbb{Z}$ where N is large enough.]

   Proof. Let p be a prime number that doesn't divide the denominators of the coefficients a_k and let N be a large integer coprime to p and divisible by all the denominators of the a_k and such that $p/N < \varepsilon/2$. We can always choose N large enough with this latter property. Clearly denominators we may write $a_k = s_k/N$ for each k and let $t_k = \lfloor s_k/p \rfloor$. Then $b_k = pt_k/N$ satisfies $|a_k - b_k| = |s_k - pt_k|/N < p/N < \varepsilon$. Moreover, b_k are all divisible by p in the ring $\frac{1}{N}\mathbb{Z}$. If $p^2 \mid b_0$, i.e., if $p \mid b_0$ replace t_0 by $t_0' = t_0 + 1$ in which case $|a_0 - b_0'| = |s_0 - pt_0'|/N < 2p/N < \varepsilon$. Finally the polynomial $Q(X) = \sum X^i b_i$ is an Eisenstein polynomial (see exercise 4 on homework 1) so is irreducible in $\mathbb{Q}[X]$ by Gauss' lemma. □

3. Let p be a prime. Show that there exists a monic irreducible polynomial $P(X)$ of degree p with 2 complex conjugate roots are $p - 2$ real roots. [Hint: Use the previous problem.]

   Proof. This is easy. Take $P(X) = (X^2 + X + 1)\prod_{i=1}^{p-2}(X - i)$. For ε sufficiently small the graphs of $P(X)$ and any polynomial $Q(X)$ satisfying the previous problem are almost the same and therefore $Q(X)$ will also have $p - 2$ real roots. To be more precise it suffices to take ε to be smaller than $|P(c)|$ for every critical point c that is located between two real roots of $P(X)$. Then $Q(X)$ is irreducible of degree p and has $p - 2$ real roots. □

4. Show that if G is any finite group there exist finite extensions $L/K/\mathbb{Q}$ such that L/K is Galois with $\mathrm{Gal}(L/K) \cong G$. [Hint: Embed G into S_p for some prime p and find L as the splitting field of a degree p irreducible polynomial with exactly two complex roots. Use the previous exercise.]

   Proof. Since multiplication by elements of G permutes the set G we get an injection $G \to S_n$ where $n = |G|$. Let p be a prime $p > n$ and put $S_n \subset S_p$ by permuting the first n elements only. Then $G \subset S_p$. Let Q be an irreducible monic degree p polynomial as in the previous exercise and let K be its splitting field over $\mathbb{Q}$. If $L = K^G$ then K/L is Galois with $\mathrm{Gal}(K/L) = G$ as desired. □

5. Artin 16.12.6 on page 511.

   Proof. In this case the Galois group has only 1 and G as subgroups. Since G is not abelian, $G/1$ is not abelian and so G is not solvable. The theorem in class then implies that P is not solvable by radicals. □

6. Artin 16.12.7 on page 511.

   Proof. $P(X) = X^7 - X - 1$ is irreducible mod 7 (see midterm) so it is irreducible in $\mathbb{Z}[X]$ as well. Let $G \subset S_7$ be the Galois group. The theorem from class implies that G contains a permutation of cycle type 7, i.e., a 7-cycle. Mod 3 we have $X^7 - X - 1 \equiv (X^2 + X + 2) \cdot (X^5 + 2X^4 + 2X^3 + 2X + 1) \pmod 3$ and so G contains an element σ of cycle type $(2, 5)$, i.e., $\sigma = c\tau$ where c is a transposition and τ is a 5-cycle disjoint from c. Since c and τ commute we see that $\sigma^5 = c^5\tau^5 = c$ so G contains a transposition. Since 7 is a prime a previous homework shows that $G = S_7$ as a 7-cycle and a transposition generate S_7.

   The theorem in class also shows that you should see the cycle type of this transposition directly factoring $P(X) \mod p$ for some prime p. The smallest such prime is $p = 191$. □

7. Artin 16.M.10 on page 512.

Proof. Let $g(x) = \prod_{\sigma \in \mathrm{Gal}(K/F), \sigma \neq 1} \sigma(f(x)) \in K[X]$. Then $h(x) = f(x)g(x) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(f(x))$ and so $g(h(x)) = \prod g\sigma(f(x)) = h(x)$ as multiplication by $g \in \mathrm{Gal}(K/F)$ permutes the elements of the Galois group. Therefore $h(x) \in K[X]^{\mathrm{Gal}(K/F)} = F[X]$. $\square$

8-10 (Worth 3 problems) Artin 16.M.11 on page 512. As stated part (c) is incorrect (in fact the example from class $X^4 + 5X + 5$ gives a contradiction). Prove instead the following version of (c): Show that $\gamma\delta$ and $\gamma\varepsilon$ are in F.

Proof. First, $P(X)$ is separable because otherwise $D = 0$ is a square in F.

(a): Write $\beta_1 = \beta$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$ and $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$. Then S_4 permutes the set $\{\beta_1, \beta_2, \beta_3\}$ so we get a homomorphism $\phi : S_4 \to S_3$. The question can be reformulated as finding $H = \{\sigma \in S_4 \mid \sigma(\beta) = \beta\} = \{\sigma \in S_4 \mid \phi(\sigma)(\beta) = \beta\}$, i.e., $\phi(\sigma) \in \langle 1, (23)\rangle = \{\tau \in S_3 \mid \tau(1) = 1\}$.

Clearly $V = \{1, (12)(34), (13)(24), (14)(23)\}$ stabilizes β. To find the group H we only need to determine $\phi(\sigma)$ for σ among the representatives of S_4/V. But $S_4/A_4 = (12)A_4$ and $A_4/V = \{V, (123)V, (132)V\}$ so S_4/V has as complete set of representatives the permutations $\sigma = (12)^a(123)^b$ where $a = 0, 1$ and $b = 0, 1, 2$. Since $(123)\beta_1 = \beta_3$ and $(123)\beta_2 = \beta_1$ and $(123)\beta_3 = \beta_2$ it follows that $\phi((123)) = (231) \in S_3$. Similarly $(12)\beta_1 = \beta_1$, $(12)\beta_2 = \beta_3$ and $(12)\beta_3 = \beta_2$ so $\phi((12)) = (23) \in S_3$. Here we used that $R(X)$ is separable as $P(X)$ is separable.

Therefore $(12) \in H$ but $(123) \notin H$. Let $T = \langle (12), V\rangle$. Then $V \subsetneq T \subset H$ and so $[T : V] \geq 2$. Moreover, $[S_4 : H] \geq 3$ (as $(123) \notin H$) so $[S_4 : T] \geq 3$. Therefore $[T : H] \leq 4!/(3 \cdot 2 \cdot 4) = 1$ so $H = T = \langle (12), V\rangle$ which then contains V as an index 2 subgroup so $H = V \sqcup (12)V$ is the dihedral group of order 8.

Alternatively you could have listed the 24 permutations of S_4 and found the 8 that fix β.

(b): $\gamma^2 = \beta^2 - 4\prod \alpha_i \in F$ as $\beta \in F$ (from assumptions) and $\prod \alpha_i = P(0) \in F$. Also $\varepsilon^2 = (\sum \alpha_i)^2 - 4(\alpha_1+\alpha_2)(\alpha_3+\alpha_4) = (\sum \alpha_i)^2 - 4(\beta_2+\beta_3)$. It suffices to show that $\beta_2+\beta_3 \in F$. But this is $\sum b_i - \beta \in F$ as $\sum \beta_i$ is a coefficient of the resolvent which is in $F[X]$.

(c): The group D_4 from part (a) is generated by (12) and (1324) and $(12)(\gamma\delta) = \gamma\delta$ and similarly for (1324). This implies that $\gamma\delta \in F$ and analogously $\varepsilon\delta \in F$.

(d): If $\gamma = \varepsilon = 0$ then $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = A$ and $\alpha_1\alpha_2 = \alpha_3\alpha_4 = B$ so α_1, α_2 and α_3, α_4 are the roots of $X^2 - AX + B = 0$ which contradicts separability. $\square$