Math 30820 Honors Algebra 4
Homework 11

Andrei Jorza

Due Wednesday, 4/12/2017

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.

Let $C_5 = \mathbb{Z}/5\mathbb{Z}$, D_5 the dihedral group with 10 elements, $F_{20} = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_5)\} \cong \mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/5\mathbb{Z})^\times$. You may take for granted that every transitive subgroup of S_5 is isomorphic to one of the groups C_5, D_5, F_{20}, A_5 and S_5.

1. Let G be a group, F a field, and $\chi_1, \dots, \chi_n : G \to F^\times$ distinct group homomorphisms. Show that the functions χ_i are F-linearly independent, i.e., if $a_1, \dots, a_n \in F$ and $g \mapsto a_1\chi_1(g)+a_2\chi_2(g)+\cdots+a_n\chi_n(g)$ is the 0 function then all the coefficients a_i are 0. [Hint: Choose a minimal linear dependence and mimick the proof of the fact that a minimal spanning set for a vector space is a basis.]

   Proof. Consider a linear dependence with smallest (nonzero) number of nonzero coefficients. We can renumber the characters such that this minimal linear dependence is $a_1\chi_1(x) + \cdots + a_m\chi_m(x) = 0$ for all $x \in G$. Since $\chi_1 \neq \chi_m$ there exists $a \in G$ such that $\chi_1(a) \neq \chi_m(a)$. Then for each $x \in G$ have $\sum a_i\chi_i(ax) = 0$ as well which is equivalent to $\sum a_i\chi_i(a)\chi_i(x) = 0$. Subtracting these two dependences we get

   $$0 = \sum_{i=1}^{m} a_i(\chi_i(a) - \chi_m(a))\chi_i(x) = \sum_{i=1}^{m-1} a_i(\chi_i(a) - \chi_m(a))\chi_i(x)$$

   so we get a nontrivial dependence (as $a_1(\chi_1(a) - \chi_m(a)) \neq 0$) with fewer tham m terms contradicting the choice of m. □

2. Let $P(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree n and K its splitting field over $\mathbb{Q}$. Fixing an ordering of the roots of $P(X)$ consider $\mathrm{Gal}(K/\mathbb{Q})$ as a subgroup of S_n. Let $H < S_n$ be a subgroup and write $S_n/H = \{\sigma_1 H, \dots, \sigma_d H\}$. Suppose there exists $\theta \in K$ such that $h(\theta) = \theta$ for all $h \in H$ and $\{\sigma_1(\theta), \dots, \sigma_d(\theta)\}$ are all distinct. Show that $R(X) = \prod_{i=1}^{d}(X - \sigma_i(\theta))$ is a separable polynomial in $\mathbb{Q}[X]$.

   Proof. The polynomial is separable by the assumption on its roots. Let $g \in \mathrm{Gal}(K/\mathbb{Q}) \subset S_n$. Then $g \in \sigma_i H$ for some σ_i. In this case

   $$g(R(X)) = \prod_{i=1}^{d}(X - g(\sigma_i(\theta)))$$

   As $g\sigma_i \in G$ we can write it as $g\sigma_i = \sigma_{i,g}h_{i,g}$ for some $h_{i,g} \in H$. Moreover, for g fixed, if $\sigma_{i,g} = \sigma_{j,g}$ then $g\sigma_i$ and $g\sigma_j$ would be in the same G/H coset. This is impossible as we know that multiplication by g permutes the G/H cosets. Therefore $\{\sigma_{i,g}\}$ is a permutation of $\{\sigma_i\}$ for any fixed $g \in G$.

Now $g(\sigma_i(\theta)) = \sigma_{i,g}(h_{i,g}(\theta)) = \sigma_{i,g}(\theta)$ as H fixed θ. We conclude that

$$g(R(X)) = \prod_{i=1}^{d}(X - g(\sigma_i(\theta))) = \prod_{i=1}^{d}(X - \sigma_{i,g}(\theta)) = \prod_{i=1}^{d}(X - \sigma_i(\theta)) = R(X)$$

so $R(X) \in K^{\mathrm{Gal}(K/\mathbb{Q})}[X] = \mathbb{Q}[X]$. $\square$

3. Let K be the splitting field over $\mathbb{Q}$ of the polynomial $P(X) = X^5 - 5X + 12 \in \mathbb{Q}[X]$.
   (a) Show that $P(X)$ is irreducible.
   (b) Show that $10 \mid [K : \mathbb{Q}]$. [Hint: $P(X)$ has two pairs of complex conjugate roots.]
   (c) Assume that $P(X)$ is solvable by radicals (it is). Show that $\mathrm{Gal}(K/\mathbb{Q}) \cong D_5$, the dihedral group with 10 elements. [Hint: What is the discriminant of $P(X)$?]

   Proof. (a): If $P(X)$ had a linear term it would have a rational root and as P is monic it would have an integer root. But then this root a would satisfy $a(a^4 - 5) = 12$ so $a \mid 12$ and no divisor of 12 is a root of $P(X)$. If $P(X)$ were reducible it would therefore be a product $P(X) = A(X)B(X)$ where A is monic quadratic and B is monic cubic of the form $A = X^2 + aX + b$ and $B = X^3 + cX^2 + dX + e$. Multiplying out we'd need $a + c = 0$, $b + ac + d = 0$, $e + ad + bc = 0$, $bd + ae = -5$ and $be = 12$. Therefore $c = -a$, $d = a^2 - b$, $e = (b - d)a$. We need $a \mid e \mid 12$, $b = 12/e$. From $bd + ae = -5$ we get b and e are of opposite parity so $e \in \{\pm1, \pm3, \pm4\}$. We test each of these e and each $a \mid e$ and compute $b = 12/e$, $d = b - e/a$ and get contradictions. Explicitly: if $e = \pm1$ then $b = \pm12$ (same sign) and $a = \pm1$ (any sign). Then $bd = -5 - ae \in \{-4, -6\}$ and ±12 does not divide these. If $e = \pm3$ then $b = \pm4$ (same sign). We need $b - d = 2b - a^2 \mid e/a \mid 3$. This is impossible if $a = \pm1$ as $b = \pm4$ so we'd need $a = \pm3$ and $2b - 9 = \pm8 - 9 \mid e/a = \pm1$ in which case we'd need $e = 3$, $b = 4$, $d = a^2 - b = 5$. This contradicts $bd + ae = -5$. Finally, suppose $e = \pm4$ and $b = \pm3$ (same sign). Then $2b - a^2 = \pm6 - a^2 \mid e/a \mid 4$. The only possibility for this divisibility with $a \mid 4$ is $a = \pm2$ and $b = 3$. Then $e = 4$ and $d = a^2 - b = 1$. Then we get $a = e/(b - d) = 2$ but this then contradicts $bd + ae = -5$.

   (b): Complex conjugation on $\mathbb{C}$ yields an automorphism of K that fixes $\mathbb{Q}$ as $K/\mathbb{Q}$ is normal. It is nontrivial on K as it interchanges the complex conjugate roots of $P(X)$. Indeed, if P had 5 real roots it would have 4 real critical point but $P'(X) = 5X^4 - 5$ which has only two real roots.

   Therefore $2 \mid [K : \mathbb{Q}]$ as we just identified an order 2 element of $\mathrm{Gal}(K/\mathbb{Q})$. Also as $P(X)$ is irreducible we know that $5 = [\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [K : \mathbb{Q}]$ where α is any root of $P(X)$.

   (c): We assume that $P(X)$ is solvable by radicals. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is one of $S_5, A_5, F_{20}, D_5, C_5$. Solvability gets rid of the nonsolvable groups S_5 and A_5 and part (b) gets rid of C_5. Therefore $\mathrm{Gal}(K/\mathbb{Q})$ is one of D_5 or F_{20}. The discriminant of $P(X)$ is 8000^2 so $\mathrm{Gal}(K/\mathbb{Q}) \subset A_5$. To show that $\mathrm{Gal}(K/\mathbb{Q}) \cong D_5$ it therefore suffices to show that $F_{20} \not\subset A_5$. But from class we know that F_{20} is the Galois group of $X^5 - 2$ with discriminant 50000 which is not a perfect square. Therefore $F_{20} \not\subset A_5$. $\square$

4. Artin 16.9.12 on page 509.

   Proof. The polynomials are all irreducible except for $X^4 + X^2 + 1 = (X^2 + 1)^2 - X^2 = (X^2 + X + 1)(X^2 - X + 1)$.

   Recall the criterion from class for Galois groups of irreducible quartics. If the discrimiant is a square then either A_4 or V. If the resolvent is irreducible it has to be A_4. If the resolvent splits completely then it has to be V.

   If the discriminant is not a square then either S_4 or D or C. It's S_4 only if the resolvent is irreducible. To tell apart D and C recall that it's D if and only if P is irreducible over $\mathbb{Q}(\sqrt{\Delta})$.

Polynomial	Resolvent	Factorization	Discriminant
X^4+4X^2+2	$X^3-4X^2-8X+32$	$(X-4)\cdot(X^2-8)$	$2\cdot 32^2$
X^4+2X^2+4	$X^3-2X^2-16X+32$	$(X-4)\cdot(X-2)\cdot(X+4)$	96^2
X^4+1	X^3-4X	$(X-2)\cdot X\cdot(X+2)$	16^2
X^4+X+1	X^3-4X-1	irreducible	229
$X^4+X^3+X^2+X+1$	X^3-X^2-3X+2	$(X-2)\cdot(X^2+X-1)$	125

(a): Since R has a root and Δ is not a square the Galois group is either D or C. From class it is D iff P is irreducible over $\mathbb{Q}(\sqrt{\Delta})=\mathbb{Q}(\sqrt{2})$. But $P=(X^2+2)^2-2=(X^2+2+\sqrt{2})(X^2+2-\sqrt{2})$ so the Galois group is C.

(b): $G=V$ (square Δ, R splits).

(c): $G=V$ in fact $K=\mathbb{Q}(\zeta_8)$ with Galois group $(\mathbb{Z}/8\mathbb{Z})^\times\cong(\mathbb{Z}/2\mathbb{Z})^2$. Using the criterion it's as for (b).

(d): $G=S_4$ (not square Δ, R irreducible).

(e): This is $\mathbb{Q}(\zeta_5)$ with Galois group $(\mathbb{Z}/5\mathbb{Z})^\times\cong\mathbb{Z}/4\mathbb{Z}$.

(f): $P(X)$ has roots $(\pm1\pm\sqrt{-3})/2$ so the splitting field is $\mathbb{Q}(\sqrt{-3})$ with $\mathbb{Z}/2\mathbb{Z}$ Galois group over $\mathbb{Q}$. $\square$

5. Artin 16.9.13 on page 509.

Proof. P is irreducible (the easiest way is to note that $P(X+1)=X^4+4X^3+4X^2-2$ is an Eisenstein polynomial), has discriminant -2^{10} and has resolvent $(X+2)(X^2+4)$. Therefore the Galois group is either D or C. To tell them apart we'd have to factor $P(X)$ over $\mathbb{Q}(\sqrt{-1024})=\mathbb{Q}(i)$. The roots of P are $\pm\sqrt{1\pm\sqrt{2}}$ and none of them are in $\mathbb{Q}(i)$ so if P factors it factors into quadratics $P(X)=(X^2+aX+b)(X^2+cX+d)$. Then $c=-a$ and $bd=-1$. But Gauss' lemma implies that the two polynomials are in $\mathbb{Z}[i]$ and $bd=-1$ in $\mathbb{Z}[i]$ means b and d are units in $\{\pm1,\pm i\}$. Comparing the coefficients of X^2 we get $b-a^2+d=-2$ and the coefficients of X that $a(d-b)=0$. If $a\neq0$ then $b=d$ and $bd=-1$ so $b=d=i$. But in this case we'd need $a^2=2+2i$ and so $|a|^2=|2+2i|=8$ so a cannot be in $\mathbb{Z}[i]$. If $a=0$ then $b+d=-2$ so $b=d=-1$ (as $b,d\in\{\pm1,\pm i\}$) which contradicts $bd=-1$.

We deduce that $\mathrm{Gal}(K/\mathbb{Q})=D$ is the dihedral group with 8 elements $\langle F,R\rangle$ satisfying $F^2=R^4=1$ and $FRF=R^3$. This group has 8 proper subgroups (see for example exercise 9 on homework 8 last semester), namely: 5 subgroups of order 2 with generators R^2,F,FR,FR^2,FR^3, the cyclic group $\langle R\rangle$, the group $\langle F,R^2\rangle=\{1,F,R^2,FR^2\}\cong(\mathbb{Z}/2\mathbb{Z})^2$ and the group $\langle R^2,FR\rangle=\{1,R^2,FR,FR^3\}\cong(\mathbb{Z}/2\mathbb{Z})^2$.

Order the roots of $P(X)$ as $\alpha_1=\sqrt{1+\sqrt{2}}$, $\alpha_2=\sqrt{1-\sqrt{2}}$, $\alpha_3=-\alpha_1$, $\alpha_4=-\alpha_2$. Since $\alpha_1\alpha_2=i$ we see that $K=\mathbb{Q}(i,\alpha_1)$ and F sends i to $-i$ keeping α_1 fixed while R sends i to $-i$ and it sends α_1 to $\alpha_2=i/\alpha_1$. As permutations F corresponds to $(24)=\begin{pmatrix}\alpha_1&\alpha_2&-\alpha_1&-\alpha_2\\\alpha_1&-\alpha_2&-\alpha_1&\alpha_2\end{pmatrix}$ (swaps α_2 and α_4) while R corresponds to $(1234)=\begin{pmatrix}\alpha_1&\alpha_2&-\alpha_1&-\alpha_2\\\alpha_2&-\alpha_1&-\alpha_2&\alpha_1\end{pmatrix}$.

The fixed fields of order 2 subgroups are quartic over $\mathbb{Q}$ and the fixed fields of order 4 subgroups are quadratic over $\mathbb{Q}$. Start with the order 4 subgroups. The obvious three quadratic subextensions are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i\sqrt{2})$. Since $Ri=-i$, $R^2i=i$, $FRi=i$, $Fi=-i$, $R\sqrt{2}=R(\alpha_1^2-1)=\alpha_2^2-1=-\sqrt{2}$ and $F(\sqrt{2})=\sqrt{2}$ we see that i is fixed by $\langle R^2,FR\rangle$, $\sqrt{2}$ is fixed by $\langle F,R^2\rangle$ and $i\sqrt{2}$ by R.

Now for the order 2 subgroups. We already know that R^2 fixes i and $\sqrt{2}$ so $K^{R^2}=\mathbb{Q}(i,\sqrt{2})$. Similarly F fixes α_1 so $K^F=\mathbb{Q}(\alpha_1)$, FR fixes $\alpha_1-\alpha_2$ so $K^{FR}=\mathbb{Q}(\alpha_1-\alpha_2)$, FR^2 fixes α_2 so $K^{FR^2}=\mathbb{Q}(\alpha_2)$ and FR^3 fixes $\alpha_1+\alpha_2$ so $K^{FR^3}=\mathbb{Q}(\alpha_1+\alpha_2)$. $\square$

6. Artin 16.9.18 on page 509.

Proof. Suppose K/F is a Galois extension with $\mathrm{Gal}(K/F) \cong D_4$. Then $K/K^{\langle F \rangle}/K^{\langle F,R^2 \rangle}/F$ are successive quadratic separable extensions. Therefore $K^{\langle F,R^2\rangle} = F(\sqrt{d})$ for $d \in F$ and $K^{\langle F \rangle} = K^{\langle F,R^2\rangle}(\sqrt{u})$ for $u \in F(\sqrt{d})$, i.e., $K^{\langle F \rangle} = F(\sqrt{e + f\sqrt{d}})$. But then $\sqrt{e+f\sqrt{d}}$ has minimal polynomial of the form $X^4 + bX^2 + c$. To show K is the splitting field of this polynomial we only need to show that $F(\sqrt{e+f\sqrt{d}})/F$ is not normal. If it were then $\langle F \rangle \lhd D_4$ and we know this to not be true. $\square$

7. Artin 16.M.7 part (b) on page 512. (Part (a) we did in class.)

   Proof. Write $\sigma \cdot P(x_1, \dots, x_n) = P(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. This is a group action of S_n on $F[x_1, \dots, x_n]$. Suppose P is 1/2-symmetric and define

$$f(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \sigma \cdot P(x_1, \dots, x_n)$$

   and

$$h(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\sigma \cdot P(x_1, \dots, x_n)$$

   Then $\sigma \cdot f = \sum_{\tau \in S_n} \sigma \cdot (\tau \cdot P) = \sum_{\tau \in S_n} (\sigma\tau) \cdot P = \sum_{\tau \in S_n} \tau \cdot P = f$ so f is symmetric. Similarly $\sigma \cdot h = \sum_{\tau \in S_n} \sigma \cdot (\varepsilon(\tau)\tau \cdot P) = \sum_{\tau \in S_n} \varepsilon(\tau)(\sigma\tau) \cdot P = \varepsilon(\sigma) \sum_{\tau \in S_n} \varepsilon(\tau)\tau \cdot P = \varepsilon(\sigma)h$ so h is skew-symmetric. It therefore suffices to show that $h = \Delta g$ where g is a symmetric polynomial.

   First, if $x_i = x_j$ then $h = (ij)h = \varepsilon((ij))h = -h$ so $h = 0$. Treating h as a polynomial in x_i shows that h has roots x_j for $j \neq i$. This implies that h is a polynomial multiple of $\prod_{j \neq i}(x_i - x_j)$. Doing this for all i implies that $h = \Delta g$ for a polynomial $g \in F[x_1, \dots, x_n]$. Now $\sigma \cdot g = \sigma \cdot (h/\Delta) = \sigma \cdot h/\sigma \cdot \Delta = \varepsilon(\sigma)h/(\varepsilon(\sigma)\Delta) = h/\Delta = g$ so g is a symmetric polynomial. $\square$

8. Let k be a field and t an indeterminate. Recall from a previous homework that we have identified $\mathrm{Aut}(k(t)/k)$ with the group $\mathrm{PGL}(2, k)$ via fractional linear transformations. Suppose $H < \mathrm{PGL}(2, k)$ is a subgroup of order n.

   (a) Let $P_H(X) = \prod_{h \in H} (X - h(t))$. Show that $P_H(X) \in k(t)^H[X]$.

   (b) Show that $k(t)^H$ is generated over k by the coefficients of $P_H(X)$.

   (c) Suppose $k = \mathbb{F}_2$. Show that

$$\mathbb{F}_2(t)^{\mathrm{Aut}(\mathbb{F}_2(t)/\mathbb{F}_2)} = \mathbb{F}_2\left(\frac{(t^2+t+1)^3}{t^2(t+1)^2}\right)$$

   [Hint: Recall from last semester that $\mathrm{PGL}(2, \mathbb{F}_2) = \mathrm{GL}(2, \mathbb{F}_2) \cong S_3$. You don't need the computationally intensive part (b), although it would lead to the same answer..]

   Proof. (1): If $g \in H$ then $g(P_H(X)) = \prod(X - gh(t)) = P_H(X)$ as multiplication by g permutes H. Thus $P_H(X) \in k(t)[X]^H = k(t)^H[X]$.

   (2): Write L for the field generated by the coefficients of $P_H(X)$. Part (1) gives $L \subset k(t)^H$. Then $k(t)$ is the splitting field of $P_H(X)$ over L. Clearly H acts transitively on the roots of $P_H(X)$ (by definition) and so $P_H(X)$ is irreducible over L. Indeed, otherwise H would permute the roots of the irreducible factors of $P_H(X)$ but would not be able to take the root of one irreducible factor to a root of another. Thus $k(t)$ is the splitting field of the irreducible polynomial $P_H(X)$ over L.

   Now $[k(t) : L] = \deg P_H(X)$ since $k(t)$ is generated by a single root. But also H is finite so $[k(t) : k(t)^H] = |H|$ from the theorem proven in class. Since these two orders are equal we deduce $k(t)^H = L$ as desired.

(3): Since $\mathrm{GL}(2, \mathbb{F}_2) \cong S_3$ it is generated by $\begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$. These correspond to $t \mapsto 1/(t+1)$ and $t \mapsto 1/t$. Certainly $R(t) = \frac{(t^2+t+1)^3}{t^2(t+1)^2}$ is invaried by both and so $k(R(t)) \subset k(t)^{\mathrm{Aut}}$. From the Exercise 2 on Homework 5 we deduce that $[k(t) : k(R(t))] = 6$ is the largest degree of the numerator and denominator of $R(t)$ and from class $[k(t) : k(t)^{\mathrm{Aut}}] = |\,\mathrm{Aut}\,| = 6$. We conclude that $k(R(t)) = k(t)^{\mathrm{Aut}}$.

$\square$