Mid-Semestral Exam 2013-2014

February 3, 2016

Problem 1.(i). Prove that $X^5 + 12X^3 - 12X + 12$ is irreducible over the field $\mathbb{Q}(e^{2\pi i/7})$.

Proof. Let $f(X) = X^5 + 12X^3 - 12X + 12$ and $\zeta = e^{2\pi i/7}$. We are going to use the following facts :

- for any integer $n \geq 1$, let ζ be a primitive nth root of unity. Then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ where ϕ is the Euler's phi function.

For us $n = 7$, hence $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(7) = 6$. Also by using Eisenstein's criterion we may conclude that the polynomial $f(X)$ is irreducible over $\mathbb{Q}$ (use the prime 3). Hence for a root α of $f(X)$ we must have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Now note that 6 and 5 are coprime and hence $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 5 \cdot 6 = 30$ (here we are using the following result : E_1, E_2 be two extensions over F of degree d_1, d_2 respectively where $(d_1, d_2) = 1$ and let $E = E_1E_2$, then $[E : F] = d_1d_2$). It follows that $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\zeta)] = 5$. But α satisfies the polynomial $f(X) \in \mathbb{Q}(\zeta)[X]$, hence its minimal polynomial must divide $f(X)$. From the degree computation done above, clearly the minimal polynomial is also of degree 5. Hence $f(X)$ must be irreducible over $\mathbb{Q}(\zeta)$. $\square$

Problem 1.(ii). Determine what the characteristic must be for the polynomial $X^4+2X^3+3X^2 + 8X + 1$ to have a multiple root.

Proof. Let $f(X) = X^4 + 2X^3 + 3X^2 + 8X + 1$ be the given polynomial and let $g(X) = 4X^3 + 6X^2 + 6X + 8$ be its derivative with respect to X. If α is a multiple root of $f(X)$, in some characteristic, then we must have both $f(\alpha) = 0$ and $g(\alpha) = 0$. Now observe that

$$4f(\alpha) - \alpha \cdot g(\alpha) = 2\alpha^3 + 6\alpha^2 + 24\alpha + 4 = h(\alpha) \Rightarrow h(\alpha) = 0.$$

Further

$$2h(\alpha) - g(\alpha) = 6\alpha^2 + 42\alpha = 0.$$

Clearly $\alpha = 0$ is not possible in any characteristic (because then $1 = 0$). Hence we must have:

$$6\alpha + 42 = 0.$$

Note that the relations that we have derived involving α are valid in any characteristic (because the operations wwe have performed are deined in any characteristic). Now it is clear that if the characteristic of the field is neither 2 nor 3 then $\alpha = -7$. But then $f(-7) = 0 \Rightarrow 1807 = 0 \ \& \ 1807 = 13 \times 139$ where $13, 139$ are both primes. Similarly $g(-7) = 0 \Rightarrow 1112 = 0 \ \& \ 1112 = 8 \times 139$. Clearly if the characteristic of the base field is 139, we have -7 as a multiple root.

Now if the characteristic of the base field is 2, then $f(X) = X^4 + X^2 + 1 = (X^2 + X + 1)^2$, hence clearly $f(X)$ has multiple roots. If the characteristic of the base field is 3, then $f(X) = X^4 - X^3 - X + 1 = (X-1)^2(X^2 + X + 1)$, then 1 is a multiple root of $f(X)$. Thus, the only characteristics for which $f(X)$ has a multiple root are $2, 3,$ and 139. □

Problem 2.(i). If f is a monic irreducible polynomial of degree n over $\mathbb{Q}$, show :

(a) the Galois group of f acts transitively on the set of roots of f in a splitting field;

(b) the discriminant of f is a square in $\mathbb{Q}$ if and only if the Galois group of f consists of even permutations.

Proof. Consult any text book of Galois theory. □

Problem 2.(ii). Determine the Galois group of the polynomial $X^4 - 2$ over $\mathbb{Q}$. Use this to find the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})$.

Proof. Let $f(X) = X^4 - 2$. Let K be the splitting field of $f(X)$ over $\mathbb{Q}$. Now we have factorization:

$$X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2}) = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - \sqrt[4]{2}i)(X + \sqrt[4]{2}i)$$

where $i = \sqrt{-1}$ and $\sqrt[4]{2}$ is the real 4-th root of 2. Then $K = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$. Observe that $f(X)$ is irreducible in $\mathbb{Q}[X]$ because none of its roots lie in $\mathbb{Q}$ hence it can not have a linear factor and from the above factorization clearly its degree 2 factors also do not lie in $\mathbb{Q}[X]$. Hence the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is $f(X)$. Also the minimal polynomial of i over $\mathbb{Q}$ is $X^2 + 1$. As $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R} \Rightarrow i \notin \mathbb{Q}(\sqrt[4]{2})$, hence $X^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\sqrt[4]{2})$. It follows that $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4, [K : \mathbb{Q}(\sqrt[4]{2})] = 2 \Rightarrow [K : \mathbb{Q}] = 8$. Moreover $K/\mathbb{Q}$ is a Galois extension.

Let $G = Gal(K/\mathbb{Q})$. Hence $|G| = 8$. Now element of G can be described by its action on $\sqrt[4]{2}$ and i. But as elements of Galois group permutes the roots of irreducible polynomials, we see that any element of G must take $i \mapsto \pm i$ and $\sqrt[4]{2} \mapsto \pm\sqrt[4]{2}, \pm\sqrt[4]{2}i$. Thus there are 8 possibilities which agrees with our previous conclusion. Let σ, τ be elements of G defined as follows:

$$\sigma(i) = i, \sigma(\sqrt[4]{2}) = \sqrt[4]{2} \ \ and \ \ \tau(i) = -i, \tau(\sqrt[4]{2}) = \sqrt[4]{2}.$$

It is easy to see that

$$\sigma^4 = Id, \tau^2 = Id \ \ and \ \ \tau\sigma\tau^{-1} = \sigma^{-1}.$$

Hence clearly

$$G = \{Id, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\},$$

and we have $G \cong D_8$, the dihedral group with 8 elements.

Let H be the subgroup generated by τ. As τ fixes $\sqrt[4]{2}$ and sends $i \mapsto -i$, clearly the fixed field of H is $\mathbb{Q}(\sqrt[4]{2})$. So to find the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})$ we must find the subgroups of G containing H. If σ belongs to this subgroup then we would get the whole group G and correspondingly we have $\mathbb{Q}$. So the only possibility is the subgroup generated by σ^2 and τ (note that $(\sigma^3)^3 = \sigma$). The order of this subgroup is 4, and hence the degree of the fixed field will be 2 over $\mathbb{Q}$. Now $\sigma^2(\sqrt[4]{2}) = -\sqrt[4]{2} \Rightarrow \sigma^2(\sqrt{2}) = \sqrt{2}$. Clearly the field $\mathbb{Q}(\sqrt{2})$ is contained in the fixed field. But as $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, it must be the fixed field. By the fundamental theorem of Galois theory, this is the only intermediate field between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})$. $\square$

Problem 3.(i). If $q = p^n$ and $\alpha \in \mathbb{F}_q$, show that

$$(X - \alpha)(X - \alpha^p) \cdots (X - \alpha^{p^{n-1}}) \in \mathbb{F}_p[X].$$

Proof. We know that $\mathbb{F}_q/\mathbb{F}_p$ is a cyclic Galois extension of degree n where the Galois group is generated by the automorphism $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ such that $\sigma(a) = a^p$ for any $a \in \mathbb{F}_q$. If we denote the given polynomial by $f(X)$, then

$$\begin{aligned}(\sigma \cdot f)(X) &= (X - \sigma(\alpha))(X - \sigma(\alpha^p)) \cdots (X - \sigma(\alpha^{p^{n-1}})) \\ &= (X - \alpha^p)(X - \alpha^{p^2}) \cdots (X - \alpha^{p^{n-1}})(X - \alpha^{p^n}) \\ &= (X - \alpha)(X - \alpha^p) \cdots (X - \alpha^{p^{n-1}}) \ \ (\because \sigma^n = Id) \\ &= f(X).\end{aligned}$$

In other words $f(X)$ is fixed by the automorphism σ and hence by $Gal(\mathbb{F}_q/\mathbb{F}_p)$ as σ generates the Galois group. So we can conclude that $f(X) \in \mathbb{F}_p[X]$. $\square$

Problem 3.(ii). Show that all the irreducible polynomials of degree n over $\mathbb{F}_p$ divide $X^{p^n} - X$ in $\mathbb{F}_p[X]$.

Proof. We are going to use the following fact : there exists finite fields of order p^n for any prime p and any integer $n \geq 1$, and are unique up to isomorphism. In particular, such a field can be realised as the set of solutions of the polynomial $X^{p^n} - X$ inside a given algebraic closure of $\mathbb{F}_p$.

Now let $f(X) \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree n. Let α be a root of $f(X)$ in some algebraic closure of $\mathbb{F}_p$. Now $[\mathbb{F}_p(\alpha) : \mathbb{F}] = deg(f) = n$. Hence $\mathbb{F}_p(\alpha)$ is a finite field of order p^n. By the above fact all of its elements are roots of the polynomial $X^{p^n} - X$. In particular α is a root of this polynomial. But by our choice the minimal polynomial of α is $f(X)$ (or some scalar multiple). Hence $f(X)$ must divide $X^{p^n} - X$. $\square$

Problem 4.(i). Prove that there exists a Galois extension of $\mathbb{Q}$ whose Galois group is cyclic of order 13.

Proof. To construct an extension $K/\mathbb{Q}$ which is Galois and $Gal(K/\mathbb{Q}) \cong \mathbb{Z}_{13}$. Let E be the splitting field of $x^{53} - 1$ over $\mathbb{Q}$. We now use the following facts:

- for any integer $n \geq 1$, let L be the splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$, then there exists a primitive nth root of unity in L and $L = \mathbb{Q}(\zeta)$ where ζ is a primitive nth root;
- the extension $L/\mathbb{Q}$ is Galois;
- the nth cyclotomic polynomial is irreducible in $\mathbb{Q}[x]$ and $Gal(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

In our situation $n = 53$ which is a prime number. Hence we know that the 53rd cyclotomic polynomial $x^{52} + x^{51} + \cdots + x + 1$ is irreducible, which implies that $[E : \mathbb{Q}] = 52$ and $Gal(E/\mathbb{Q}) \cong (\mathbb{Z}/53\mathbb{Z})^*$ which is a cyclic group of order 52. Let σ be a generator of this group. Now consider the element $\tau = \sigma^{13}$ and let H be the subgroup generated by τ. As the Galois group is cyclic, H is a normal subgroup. In fact it is easy to check that $|H| = 4$. Now by fundamental theorem of Galois theory, $E^H/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to $Gal(E/\mathbb{Q})/H$. But this group is clearly cyclic and has order 13. Thus $E^H = K$ serves our purpose. □

Problem 4.(ii). Let E/F be n extension and let $a \in E$ be algebraic and purely inseparable over F, where $char(F) = p > 0$. Prove that $min(F, a) = (X - a)^{p^n}$ for some n.

Proof. Consult any text book of Galois theory. □

Problem 5.(i). Let $char(K) = p > 0$, and let $a \in K$. If the polynomial $X^p - X - a$ is reducible in $K[X]$, prove that all its roots lie in K.

Proof. Let $f(X) = X^p - X - a$. Assume that this polynomial is reducible in $K[X]$. We also know that this polynomial is separable (because $(f, f^{'}) = 1$). In fact if α is a root of $f(X)$ so is $\alpha + 1, \cdots, \alpha + p - 1$. Thus we have accounted for the p distinct roots of $f(X)$. Note that if any one of the roots lie in K, all of the roots lie in K. So if any of the factors of $f(X)$ in $K[X]$ is linear we are done.

Let $g(X) \in K[X]$ be an irreducible factor of $f(X)$. Let E (respectively F) be the splitting field of $f(X)$ (respectively of $g(X)$. Then $F \subset E$. Now let β be a root of $g(X)$ in F. Obviously β is also a root of $f(X)$ in E. Following the argument in the previous paragraph, it is clear that $\beta + 1, \cdots, \beta + p - 1$ are also roots of $f(X)$ and all of them lie in F. Hence $F = E = K(\beta)$ and consequently $[F : K] = deg(g) \Rightarrow [E : K] = deg(g)$. But the same argument works for any irreducible factor of $f(X)$ and it follows that all of them have degree $= [E : K]$. As $f(X)$ is separable, it must be product of distinct irreducible polynomials .So if the number of distinct irreducible factors of $f(X)$ is r, then we have $p = r[E : K]$. As p is a prime, we must have $r = 1$ or $r = p$. If $r = 1$, then $f(X)$ itself becomes irreducible, thus violating our assumption. So we must have $r = p$ which implies that all the factors are linear and hence we are done. □

Problem 5.(ii). Let L/K be an extension such that each $\alpha \in L$ is algebraic and separable over K with degree at the most d (independent of α). Show that $[L : K] \leq d$.

Proof. By our assumption L/K is a separable extension. Let

$$\mathcal{S} = \{\text{all subfields of } L \text{ containing } K \text{ of degree} \leq d \text{ over } K\}.$$

By our hypothesis $\mathcal{S} \neq \emptyset$, in fact for any $\alpha \in L$, $K(\alpha) \in \mathcal{S}$. By Zorn's lemma, there exists maximal elements in $\mathcal{S}$. Let E be a maximal element in $\mathcal{S}$. We claim that $E = L$. If not, pick $\alpha \in L - E$. Now E/K is a finite, separable extension and hence $E(\alpha)/K$ is a finite separable extension. By primitive element theorem, we must have $E(\alpha) = K(\beta)$ for some element $\beta \in E(\alpha) \subset L$. But we know that $[K(\beta) : K] \leq d$, which implies that $[E(\alpha) : K] \leq d$. Hence $E(\alpha) \in \mathcal{S}$. By maximality of E, then we must have $E(\alpha) = E \Rightarrow \alpha \in E$. Thus we have reached a contradiction. Hence $E = L \Rightarrow [L : K] \leq d$. $\square$

Problem 6.(i). Let L/K be a (finite) Galois extension. If the quotient group L^*/K^* contains an element of order n, show that L^* must contain an element of order n.

Proof. Let $a \in L^*$ be an element such that its image in L^*/K^* has order n. Hence $a^n = b$ for some $b \in K^*$. Consider the polynomial $f(x) = (x^n - b) \in K[x]$. Then a is a root of $f(x)$. As $a \notin K$, there must be some $\sigma \in Gal(L/K)$ such that $\sigma(a) \neq a$ (because $\sigma(a) = a \ \ \forall \sigma \in Gal(L/K) \Rightarrow a \in K$). Note that $\sigma(a)$ is also a root of $f(x)$ i.e $(\sigma(a))^n = b$. Let $\sigma_1, \cdots, \sigma_r$ be all the elements in $Gal(L/K)$ such that $\sigma_i(a) \neq a$. Define $c_i = \sigma_i(a)/a \Rightarrow c_i \neq 1, c_i^n = 1$. Let us assume that the order of c_i is m_i, which implies $m_i | n, 1 \leq i \leq r$. Let m be the l.c.m of the m_i's, then $m|n$. Now for $1 \leq i \leq r$, we have

$$c_i^{m_i} = 1 \Rightarrow \sigma_i(a^{m_i}) = a^{m_i} \Rightarrow \sigma_i(a^m) = a^m.$$

Hence for any $\sigma \in Gal(L/K)$ we have $\sigma(a^m) = a^m$ (if $\sigma \neq \sigma_i$, then $\sigma(a) = a$). So $a^m \in K \Rightarrow n|m \Rightarrow m = n$. Let $H = \langle c_1, \cdots, c_r \rangle$ be the subgroup of L^* generated by the c_i's. Clearly H is a finite abelian group. But we know that any finite multiplicative subgroups of fields are cyclic. Hence H must be cyclic, say $H = \langle x \rangle$, and order of x ($= |H|$) must be equal to the exponent of H. But clearly exponent of H is m, and hence order of x is $m = n$. $\square$

Problem 6.(ii). Prove that $\mathbb{Q}(\zeta_n)$ can not contain a 4-th root of 2 for any n.

Proof. Let us fix an algebraic closure of $\mathbb{Q}$. We will always be working within this field. Let ϕ be the Euler's phi function. We will use the following facts:

- for any $n \in \mathbb{N}$, $\mathbb{Q}(\zeta_n)$ is a Galois extension over $\mathbb{Q}$ where ζ_n is a primitive nth root of unity;
- $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ and $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$;
- for any prime $p > 2$ we have $(\mathbb{Z}/p^k\mathbb{Z})^* \cong \mathbb{Z}/\phi(p^k)\mathbb{Z}$;
- $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/2^k\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2^{k-1}\mathbb{Z}$ for $k \geq 3$.

If possible, let us assume that $\alpha \in \mathbb{Q}(\zeta_n)$ for some n. Now $X^4 - 2$ is irreducible over $\mathbb{Q}$ (look at Problem 2.(ii)). If one of its roots lie in $\mathbb{Q}(\zeta_n)$, then it must split completely in $\mathbb{Q}(\zeta_n)$ (because $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois). Let K be the splitting field of $X^4 - 2$ in $\mathbb{Q}(\zeta_n)$. We know that $K/\mathbb{Q}$ is Galois of degree 8 and $Gal(K/\mathbb{Q}) \cong D_8$ (look at Problem 2.(ii)). By fundamental theorem of Galois theory $Gal(K/\mathbb{Q})$ must be a quotient of $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. In other words the group D_8 must be a quotient of $(\mathbb{Z}/n\mathbb{Z})^*$. From the facts stated above it is clear that $(\mathbb{Z}/n\mathbb{Z})^*$ can be written as a direct product of cyclic groups. Hence it must be abelian and the same is true for its quotient groups. But we know that D_8 is a nonabelian group and thus we have arrived at a contradiction. So $\mathbb{Q}(\zeta_n)$ can not contain a 4-th root of unity for any n. $\square$