Mid-Semestral Exam 2014-2015

January 31, 2016

Problem 1.(a). State true or false with justification. For fields $F \subseteq K$, and $\alpha \in K$, if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.

Proof. Suppose $F(\alpha) \neq F(\alpha^2)$. Clearly this implies that $\alpha \notin F(\alpha^2)$. We can also conclude that the minimal polynomial of α over $F(\alpha^2)$ is $x^2 - \alpha^2$. Hence $[F(\alpha) : F(\alpha^2)] = 2$. But we know that $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$. Hence we must have $2|[F(\alpha) : F]$ and thus we arrive at a contradiction. So $F(\alpha) = F(\alpha^2)$ and the given statement is **true.** $\square$

Problem 1.(b). State true or false with justification. The regular 5-gon is not constructible by straightedge and compass.

Proof. The problem of constructing the regular n-gon is equivalent to the problem of constructing the angle $2\pi/n$ which in turn is equivalent to the problem of constructing $\cos(2\pi/n)$. In our problem we need to check the constructibility of $\cos(2\pi/5)$. Now $\cos(2\pi/5) = (\exp^{2\pi i/5} + \exp^{-2\pi i/5})/2$. So we have $\mathbb{Q} \subset \mathbb{Q}(\cos(2\pi/5)) \subset \mathbb{Q}(\cos(\exp^{2\pi i/5}))$. Now $\mathbb{Q}(\cos(\exp^{2\pi i/5}))/\mathbb{Q}$ is a cyclotomic extension of degree $5-1 = 4$. Also $[\mathbb{Q}(\cos(\exp^{2\pi i/5})) : \mathbb{Q}(\cos(2\pi/5))] = 2$ because $\cos(\exp^{2\pi i/5})$ satisfies the polynomial $x^2 - 2\cos(2\pi/5)x + 1$ and these two fields can not be equal. Hence $[\mathbb{Q}(\cos(2\pi/5)) : \mathbb{Q}] = 2$. By the fundamental theorem of Galois theory this extension is Galois. We know that if a real number α is contained in a subfield of $\mathbb{R}$ that is Galois of degree 2^r, $r \in \mathbb{N}$, over $\mathbb{Q}$ then α is constructible. Hence $\cos(2\pi/5)$ is constructible and the given statement is **false.** $\square$

Problem 1.(c). State true or false with justification. If $F \subseteq E \subseteq K$ are fields, such that K/E and E/F are both Galois extensions, then K/F is also a Galois extension.

Proof. Let $F = \mathbb{Q}, E = \mathbb{Q}(\sqrt{2}), K = \mathbb{Q}(\sqrt[4]{2})$. Both E/F and K/E are Galois extensions because in either case we have a degree 2 extension which is the splitting field of a degree 2 irreducible polynomial and also we are working in characteristic zero, hence the polynomials are separable. But K/F is not Galois. This is because the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is $x^4 - 2$. The roots of this polynomial (in some algebraic closure of $\mathbb{Q}$) are $\sqrt[4]{2}, \sqrt[4]{2}\zeta, \sqrt[4]{2}\zeta^2, \sqrt[4]{2}\zeta^3$ where ζ is a primitive 4-th root of unity. Clearly not all the roots of $x^4 - 2$ lie in $\mathbb{Q}(\sqrt[4]{2})$. Hence K/F is separable but not normal and hence it is not a Galois extension. Thus the given statement is **false.**

$\square$

Problem 1.(d). State true or false with justification. A polynomial over a field of characteristic zero is separable if and only if it is the product of distinct irreducible polynomials.

Proof. Suppose we have a polynomial $f = g_1^{e_1} \cdots g_r^{e_r}$ where g_i's are distinct irreducible polynomials (upto multiplication by scalars) and $e_i \in \mathbb{N}, \forall i$. Now if we have $e_i > 1$ for some i, then clearly any root of g_i would be a repeated root of f. So if f is separable, then we must have $e_i = 1, \forall i$. Conversely, we assume that $f = g_1 \cdots g_r$. We know that over a field of characteristic zero irreducible polynomials are separable. Hence all the g_i's are separable. So if f has a repeated root, it can not be a repeated root of any of the g_i's. The only other possibility is that it must be a root of two or more different g_i's. Now by the uniqueness of minimal polynomials, clearly the above situation can not happen. So f is separable and the given statement is **true.** $\square$

Problem 1.(e). State true or false with justification. If K is a finite field of characteristic p, then every element of K has a unique p-th root in K.

Proof. Let $\mathbb{F}_p$ be the field with p elements with a fixed algebraic closure $\overline{\mathbb{F}_p}$. Without loss of generality we may assume that $K \subset \overline{\mathbb{F}_p}$. Let ϕ denote the p-th power map from $\overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$. We know that ϕ fixes $\mathbb{F}_p$ and it is clear that $\phi(K) \subseteq K$. As we are dealing with maps between fields obviously ϕ is injective. Hence $[\phi(K) : \mathbb{F}_p] = [K : \mathbb{F}_p]$ and linear algebra tells us that $\phi(K) = K$. Hence every element in K has a unique p-th root in K and the given statement is **true.** $\square$

Problem 2.(a). Show that if F is a field with $char(F) \neq 2$, and if K is a quadratic extension of F, then $K = F(\sqrt{d})$ for some $d \in F$, d not a square in F.

Proof. Let $\alpha \in K$, $\alpha \notin F$. Then $[K : F] = [K : F(\alpha)][F(\alpha) : F]$. By our choice of α, $[F(\alpha) : F] \geq 2$ and it is given that $[K : F] = 2$. Hence we must have $[K : F(\alpha)] = 1 \Rightarrow K = F(\alpha)$. So the minimal polynomial of α over F must be a polynomial of degree 2, say $x^2 + ax + b$. Now

$$\alpha^2 + a\alpha + b = 0 \Rightarrow (\alpha + a/2)^2 - (a^2/4 - b) = 0$$

(here we are using the fact that $char(F) \neq 2$, hence we have $1/2 \in F$). Put $\beta = \alpha + a/2, d = a^2/4 - b$, then $\beta = \sqrt{d}$. d is obviously not a square in F because otherwise β and hence α would belong to F. Clearly $K = F(\alpha) = F(\beta) = F(\sqrt{d})$ and we are done. $\square$

Problem 2.(b). Find all quadratic extensions of $\mathbb{Q}$ which contain a primitive p-th root of unity ζ for some prime $p \neq 2$.

Proof. Let K be a quadratic extension of $\mathbb{Q}$ containing a primitive p-th root of unity ζ for some prime $p \neq 2$. We know that ζ is a root of the polynomial $x^{p-1} + \cdots + x + 1$ which is irreducible for any prime p. Hence $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Now clearly we must have $p - 1 \leq 2 \Rightarrow p \leq 3$. Hence by our assumptions the only possible value for p is 3. In that situation $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2 \Rightarrow K = \mathbb{Q}(\zeta)$. This is the only possible quadratic extension. $\square$

Problem 3. Prove that there exists finite fields of order p^n for any prime p and any integer $n \geq 1$, and unique upto isomorphism.

Proof. Consult any text book on Galois theory. $\square$

Problem 4.(a). Let $f(x) \in F[x]$ be a polynomial of degree n. Let K be its splitting field. Show that $[K : F]$ divides $n!$.

Proof. We will prove this by induction on n. The statement is obviously true for $n = 1, n = 2$. So let us assume that the result is true for any natural number $d < n$ i.e. for any polynomial $g(x) \in F[x]$ of degree d with splitting field E, $[E : F]|n!$. Now we can split the proof into two cases.

In the first case, assume that $f(x)$ is an irreducible polynomial. Let $\alpha \in K$ be a root of $f(x)$, then $[F(\alpha) : F] = n$. Let $h(x) = f(x)/(x - \alpha)$. Then $h(x) \in F(\alpha)[x]$ is a polynomial of degree $n - 1$. It is clear that K is also the splitting field of $h(x)$. Hence by our induction hypothesis, $[K : F(\alpha)]|(n-1)!$ (the induction hypothesis is valid for any field). But $[K : F] = [K : F(\alpha)][F(\alpha) : F] = [K : F(\alpha)]n$, and hence $[K : F]|n!$.

Now let us assume that $f(x)$ is an arbitrary polynomial. Let us write $f(x) = g(x)h(x)$ where $g(x) \in F[x]$ is an irreducible polynomial of degree r and $h(x) \in F[x]$ ia a polynomial of degree s. We have $n = r + s, 0 < r \leq n, 0 \leq s$. E be the splitting field of $g(x)$ contained in K. Then by the first case and induction hypothesis, $[E : F]|r!$ (it may happen that $r = n$ and for that we need the first case). Now K is also the splitting field of $h(x)$ over E. Hence by induction hypothesis, $[K : E]|s!$. So we have $[E : F][K : E]|r!s! \Rightarrow [K : F]|r!s!$. But $n = r + s \Rightarrow r!s!|n!$, hence $[K : F]|n!$.Thus the induction step is complete and we have proved the statement. $\square$

Problem 4.(b). Describe the splitting field of the polynomial $x^5 - 7$ over $\mathbb{Q}$, and find the degree of the splitting field over $\mathbb{Q}$.

Proof. Let us fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Now the polynomial $f(x) = x^5 - 7$ must have 5 roots in $\overline{\mathbb{Q}}$. Note that $x^5 - 7$ is an irreducible polynomial (by Eisenstein's criterion) and as we are working in characteristic zero, it must be separable. Hence the roots must all be distinct. There must be a real root of the polynomial (because it has odd degree and complex roots occur in pairs), let us denote it by α. Let ζ be a primitive 5th root of unity. Clearly $\alpha, \alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4$ are the distinct roots of $f(x)$. Hence the splitting field K of $f(x)$ over $\mathbb{Q}$ can be described as

$$K = \mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4) = \mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(\alpha)\mathbb{Q}(\zeta).$$

To compute the degree of K over $\mathbb{Q}$, we compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}]$. From the properties of $f(x)$ stated above, clearly $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. We know that over $\mathbb{Q}$ the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible and ζ is a root of this polynomial (this the 5th cyclotomic polynomial). So $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. Now we note that 4 and 5 are coprime hence $[K : \mathbb{Q}] = 4 \cdot 5 = 20$ (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 $[E : F] = d_1d_2$). $\square$

Problem 5.(a). Let n be an odd integer such that F contains a primitive n-th root of unity and $char(F) \neq 2$. Show that F also contains a primitive $2n$-th root of unity.

Proof. Let ζ be the primitive n-th root in F. We have $(-\zeta)^{2n} = 1$. Note that $\zeta \neq -\zeta$ because $char(F) \neq 2$. Let us denote $-\zeta$ by ω and we claim that ω is the required primitive $2n$-th root of unity. If not, let ω be a primitive d-th root of unity for $d < 2n$. Hence

$$\omega^d = 1 \Rightarrow \zeta^d = (-1)^d.$$

Now there are two possibilities. If d is odd, then

$$\zeta^d = -1 \Rightarrow \zeta^{2d} = 1 \Rightarrow n|2d$$

(by definition of ζ). As n is odd, we must have $n|d$. Hence the only possibility is $d = n$, but clearly $\omega^n \neq 1$. So we arrive at a contradiction. If d is even, then

$$\zeta^d = 1 \Rightarrow n|d.$$

Following the same argument as before we again arrive at a contradiction. Hence ω is the required $2n$-th root of unity contained in F. $\square$

Problem 5.(b). Let K be a finite extension of $\mathbb{Q}$. Show that there is only a finite number of roots of unity in K.

Proof. Let S be the set of roots of unity in K. Now every root of unity is a primitive n-th root of unity for some $n \in \mathbb{N}$ and this integer n is uniquely determined by the root. Let S_n be the set of primitive n-th roots of unity in K. Clearly $S_n \bigcap S_m = \emptyset$ for $n \neq m$. Hence we can write

$$S = S_1 \bigsqcup S_2 \bigsqcup S_3 \bigsqcup \cdots .$$

We should note that some of the sets S_n may be empty. Now if possible let us assume that the set S has infinitely many elements. As each of the sets S_n has atmost n many elements (because it is the solution set of the polynomial $x^n - 1$ in K), we must have an increasing sequence of integers $n_1 < n_2 < \cdots$, which is unbounded, such that $S_{n_i} \neq \emptyset$. But for $\alpha \in S_{n_i}$ we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \phi(n_i)$ where ϕ is the Euler's phi function ($\because$ over $\mathbb{Q}$ the nth cyclotomic polynomial is irreducible of degree $\phi(n)$ for any $n \in \mathbb{N}$). From the definition of ϕ it is clear that $\phi(n_i) \to \infty$ as $n_i \to \infty$. Now $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)]\phi(n_i)$, hence $\phi(n_i)|[K : \mathbb{Q}]$. But given that $[K : \mathbb{Q}]$ is finite and $\phi(n_i) \to \infty$ by our assumption, we have arrived at a contradiction. So $|S| < \infty$.

$\square$

Problem 6. Prove that the extension K/F is Galois if and only if K is the splitting field of some separable polynomials over F.

Proof. Consult any text book on Galois theory. $\square$

Problem 7. Consider the polynomial $f(x) = x^4 - 3x^2 - 10 \in \mathbb{Q}[x]$. Find the splitting field K of $f(x)$ over $\mathbb{Q}$. Describe the Galois group G of the extension $K/\mathbb{Q}$. Show the correspondence between all the subgroups of G and all the subfields of K containing $\mathbb{Q}$.

Proof. We have the following factorization of $f(x)$ over $\mathbb{Q}$

$$f(x) = x^4 - 3x^2 - 10 = (x^2 - 5)(x^2 + 2).$$

Fixing an algebraic closure of $\mathbb{Q}$ we can write down the roots of these two polynomials, which are $\{\sqrt{5}, -\sqrt{5}\}, \{\sqrt{2}i, -\sqrt{2}i\}$ where $i = \sqrt{-1}$. Hence we can describe the splitting field as $K = \mathbb{Q}(\sqrt{5}, -\sqrt{5}, \sqrt{2}i, -\sqrt{2}i) = \mathbb{Q}(\sqrt{5}, \sqrt{2}i)$.

Clearly $f(x)$ is a separable polynomial and hence $K/\mathbb{Q}$ is a Galois extension. Let $g(x) = x^2 - 5, h(x) = x^2 + 2$ and E, F be the splitting fields of $g(x), h(x)$ respectively. Clearly $E = \mathbb{Q}(\sqrt{5}), F = \mathbb{Q}(\sqrt{2}i)$. Both g and h are irreducible over $\mathbb{Q}$ and $E/\mathbb{Q}, F/\mathbb{Q}$ are Galois extensions of degree 2. Hence the Galois group in each case is a group of order 2 and hence isomorphic to $\mathbb{Z}_2$. Now any element of G is determined by its action on $\sqrt{5}$ and $\sqrt{2}i$. We know that roots of an irreducible polynomial are permuted by elements of the Galois group. Hence elements of G must take $\sqrt{5} \mapsto \pm\sqrt{5}$ and $\sqrt{2}i \mapsto \pm\sqrt{2}i$. Thus there are only 4 possible elements in G. Let σ, τ be elements of G defined as follows:

$$\sigma(\sqrt{5}) = -\sqrt{5}, \sigma(\sqrt{2}i) = \sqrt{2}i \text{ and } \tau(\sqrt{5}) = \sqrt{5}, \tau(\sqrt{2}i) = -\sqrt{2}i.$$

It is easy to see that:

$$\sigma^2 = Id, \tau^2 = Id, \sigma\tau = \tau\sigma.$$

Hence it follows that $G \cong \langle\sigma\rangle \oplus \langle\tau\rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

The only possible subgroups of G are : $\{1\}, \langle\sigma\rangle, \langle\tau\rangle, G$. Corresponding to $\{1\}$ and G, we get the subfields K and $\mathbb{Q}$ respectively. Clearly σ fixes $\sqrt{2}i$, hence $F = \mathbb{Q}(\sqrt{2}i)$ is contained in the fixed field of $\langle\sigma\rangle$. But by fundamental theorem of Galois theory, the degree of the fixed field of $\langle\sigma\rangle$ over $\mathbb{Q}$ is $|G|/|\langle\sigma\rangle| = 2$. Hence F is the field corresponding to $\langle\sigma\rangle$. Similarly we can argue that the field corresponding to $\langle\tau\rangle$ is E. Thus we have all the correspondences. $\square$