Math 566 - Homework 10

SOLUTIONS

Prof Arturo Magidin

1. Let K be an extension of F, and let $u \in K$. Show that if u is the root of a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$, and each a_i is algebraic over F, then u is algebraic over F.

   Proof. Let $F_{-1} = F$, $F_0 = F(a_0)$, $F_1 = F(a_0, a_1)$, $\ldots$, $F_n = F(a_0, \ldots, a_n)$. Since each a_i is algebraic over F, they are algebraic over F_{i-1}. And since $F_i = F_{i-1}(a_i)$, with a_i algebraic over F_{i-1}, then $[F_i : F_{i-1}]$ is finite for $i = 0, \ldots, n$.

   Moreover, u is algebraic over F_n, so $[F_n(u) : F_n]$ is finite.

   Thus, we have that

   $$[F_n(u) : F] = [F_n(u) : F_n][F_n : F_{n-1}] \cdots [F_0 : F] < \infty.$$

   Thus, $F_n(u)$ is finite dimensional over F, and therefore algebraic over F. That means that every element of $F_n(u)$, and in particular u, is algebraic over F. $\square$

2. Let K be an extension of F, and let L and M be intermediate extensions (so $F \subseteq L \subseteq K$ and $F \subseteq M \subseteq K$).

   (i) Prove that $[LM : M] \leq [L : L \cap M]$.

   Proof. Let $\mathcal{B} = \{\ell_i\}_{i \in I}$ be a basis for L over $L \cap M$. Note that $\mathcal{B} \subseteq L \subseteq LM$.

   We prove that this set spans LM over M; this will prove that this collection contains a basis for LM over M, and therefore that the dimension of LM over M is at most the dimension of L over $L \cap M$.

   First, let $u \in L$. Then we know that u is in the $(L \cap M)$-span of $\mathcal{B}$. Thus, there exist $i_1, \ldots, i_m \in I$, and $a_1, \ldots, a_m \in L \cap M$ such that

   $$u = a_1\ell_{i_1} + \cdots + a_m\ell_{i_m}.$$

   Since the a_i also lie in M, we have that u lies in the M-span of $\mathcal{B}$.

   This proves that $L \subseteq \mathrm{span}_M(\mathcal{B})$. In particular, 1 lies in the span, and hence so does the span of 1 over M, which is M. Thus, $M, L \subseteq \mathrm{span}_M(\mathcal{B})$.

   Look at LM as $LM = M(L)$. If every element of L is algebraic over M, then this is equal $M[L]$, and since we can obtain any element of L and every element of M as M-linear combinations of $\mathcal{B}$, we can also obtain any power of elements of L and products of elements of L. Thus, any polynomial expression $p(\ell_1, \ldots, \ell_k)$ with coefficients in M and $\ell_i \in L$ is expressible as an M-linear combination of elements of $\mathcal{B}$.

   If there are element of L, $x_1, \ldots, x_n$ that are transcendental over M, then they are also transcendental over $M \cap L$. So any rational expression with coefficients in M can be expressed as an M-linear combination of rational expressions with coefficients in $L \cap M$, which were already expressible in terms of $\mathcal{B}$. Thus, the M-span of $\mathcal{B}$ will yield every element of $M(L)$.

   Thus, $ML \subseteq \mathrm{span}_M(\mathcal{B})$. On the other hand, every element of $\mathcal{B}$ lies in L, so $\mathrm{span}_M(\mathcal{B}) \subseteq M(L)$. Hence we have equality.

   Therefore, $[LM : M] \leq |\mathcal{B}| = [L : L \cap M]$, proving the desired inequality. $\square$

   (ii) Conclude that $[LM : M] \leq [L : F]$.

   Proof. Note that $F \subseteq L \cap M$. Thus, $[L \cap M : F] \geq 1$, so

   $$[LM : M] \leq [L : L \cap M] \leq [L : L \cap M][L \cap M : F] = [L : F],$$

   as desired. $\square$

3. Let K be an extension of F, and let $u, v \in K$ be algebraic over F with $[F(u) : F] = n$ and $[F(v) : F] = m$.

   (i) Prove that $[F(u, v) : F] \leq nm$.

   Proof. Note that

   $$[F(u, v) : F] = [F(u, v) : F(u)][F(u) : F].$$

   We know that $[F(u) : F] = n$. Let $L = F(v)$ and $M = F(u)$. Then Problem 2(ii) says that $[F(u, v) : F(u)] \leq [F(v) : F] = m$. So we have

   $$[F(u, v) : F] = [F(u, v) : F(u)][F(u) : F] \leq [F(v) : F][F(u) : F] = nm,$$

   as desired. $\square$

   (ii) Show that if $\gcd(m, n) = 1$, then $[F(u, v) : F] = nm$.

   Proof. We have

   $$[F(u, v) : F] = [F(u, v) : F(u)][F(u) : F] = n[F(u, v) : F(u)],$$

   so $n \mid [F(u, v) : F]$. Symmetrically, we have $m \mid [F(u, v) : F]$. Therefore, we know that $\operatorname{lcm}(m, n) \mid [F(u, v) : F]$.

   Since $\gcd(m, n) = 1$, we have $\operatorname{lcm}(m, n) = mn$. So we know that mn divides $[F(u, v) : F]$. On the other hand, part (i) shows that $[F(u, v) : F]$ is at most mn. Hence, $[F(u, v) : F] = mn$, as claimed. $\square$

4. Let K be a finite dimensional extension of F and let L and M be intermediate extensions.

   (i) Show that if $[LM : F] = [L : F][M : F]$, then $L \cap M = F$.

   Proof. Proceeding as in Problem 2, we have

   $$\begin{aligned}[LM : F] = [LM : M][M : F] &\leq [L : L \cap M][M : F] \\ &\leq [L : L \cap M][L \cap M : F][M : F] \\ &= [L : F][M : F] = [LM : F].\end{aligned}$$

   Since we have equality, that means that $[L : L \cap M] = [L : L \cap M][L \cap M : F]$, and therefore we have $[L \cap M : F] = 1$. That means that $L \cap M = F$. $\square$

   (ii) Show that if $[L : F] = 2$ or $[M : F] = 2$, and $L \cap M = F$, then we will have $[LM : F] = [L : F][M : F]$.

   Proof. Assume first that $[L : F] = 2$. Since $[LM : M] \leq [L : L \cap M] = [L : F] = 2$, it follows that either $[LM : M] = 1$ or $[LM : M] = [L : F] = 2$.

   But $[LM : M] = 1$ implies that $LM = M$, so $L \subseteq M$. Therefore, $F = L \cap M = L$, which is impossible since $[L : F] = 2$. Therefore, $[LM : M] = [L : F] = 2$. So

   $$[L : F][M : F] = [LM : M][M : F] = [LM : F],$$

   as desired. The case where $[M : F] = 2$ follows symmetrically. $\square$

   (iii) Use a real and a nonreal cube root of 2 to give an example of a finite dimensional extension K of $\mathbb{Q}$, and intermediate fields L and M, such that $L \cap M = \mathbb{Q}$ and $[L : \mathbb{Q}] = [M : \mathbb{Q}] = 3$, but $[LM : \mathbb{Q}] < 9$.

   Proof. Let $L = \mathbb{Q}[\sqrt[3]{2}]$; let ω be a (complex) primitive cubic root of unity, and let $M = \mathbb{Q}[\omega\sqrt[3]{2}]$. Since both $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$ are roots of the irreducible polynomial $x^3 - 2$, there is an isomorphism $\phi\colon L \to M$ that restricts to the identity on $\mathbb{Q}$ and maps $\sqrt[3]{2}$ to $\omega\sqrt[3]{2}$;

in particular, $[L:\mathbb{Q}] = [M:\mathbb{Q}] = 3$. Since $L \neq M$, and $\mathbb{Q} \subseteq L \cap M \subseteq M$ with $[M:\mathbb{Q}] = 3$ a prime number, we must have $L \cap M = \mathbb{Q}$.

But $LM = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Note that ω is a root of x^2+x+1, as it is a root of the polynomial $x^3-1 = (x-1)(x^2+x+1)$ but is not 1. So letting $K = \mathbb{Q}(\omega)$, we have $[L:\mathbb{Q}] = 3$, $[K:\mathbb{Q}] = 2$, and hence by Problem 3(ii), $[KL:\mathbb{Q}] = 6$. Since $KL = LM$, we have $[LM:\mathbb{Q}] = 6 < 9$. $\square$

5. Prove that $\mathbb{Q}(\sqrt{2})$ is not isomorphic to $\mathbb{Q}(\sqrt{3})$. NOTE: We know there is no isomorphism from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(\sqrt{3})$ that sends $\sqrt{2}$ to $\sqrt{3}$; but this, in and of itself, does not preclude the possibility of an isomorphism where $\sqrt{2}$ is mapped to some other element of $\mathbb{Q}(\sqrt{3})$.

   Proof. It is enough to show that $\mathbb{Q}(\sqrt{2})$ does not have an element α with $\alpha^2 = 3$. This, because any putative isomorphism $\varphi\colon \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{2})$ must send each rational to itself, so $(\varphi(\sqrt{3}))^2 = \varphi(\sqrt{3}^2) = \varphi(3) = 3$ would hold.

   But this fact was proven in Homework 9 Problem 5(i), where we showed that x^2-3 is irreducible over $\mathbb{Q}(\sqrt{2})$.

   Thus $\mathbb{Q}(\sqrt{2})$ cannot be isomorphic to $\mathbb{Q}(\sqrt{3})$. $\square$

6. Let K be an extension of F, where $\mathrm{char}(F) \neq 2$. Prove that $[K:F] = 2$ if and only if $K = F(\sqrt{d})$ for some $d \in F$ that is not a square in F.

   Proof. If d is not a square, then $\sqrt{d}$ is a root of the monic irreducible polynomial $x^2 - d$, so $[F(\sqrt{d}):F] = 2$, as desired.

   Conversely, suppose that $[K:F] = 2$, a prime. Then $K \neq F$, so there exists $u \in K$ such that $u \notin F$. Since $F \subseteq F(u) \subseteq K$ and $u \notin F$, we must have $F(u) = K$.

   Since $[F(u):F] = 2$, then $1, u, u^2$ are linearly dependent over F, but $1, u$ are linearly independent (because $u \notin F$). So there exist $a, b, c \in F$ such that

   $$c + bu + au^2 = 0, \qquad a \neq 0.$$

   Let $d = b^2 - 4ac$. If $d = r^2$ for some $r \in F$, then since $\mathrm{char}(F) \neq 2$, we have

   $$a\left(u - \frac{-b+r}{2a}\right)\left(u - \frac{-b-r}{2a}\right) = a\left(u^2 - \frac{-2b}{2a}u + \frac{b^2-r^2}{4a^2}\right) = au^2 + bu + c = 0.$$

   Since $a \neq 0$, either $u = \frac{-b+r}{2a}$ or $u = \frac{-b-r}{2a}$, contradicting that $u \notin F$. That means that d is not a square in F. In particular, $[F(\sqrt{d}):F] = 2$.

   We claim that $K = F(\sqrt{d})$. Indeed, the calculation we just did, with $\sqrt{d}$ replacing r, shows that $u \in F(\sqrt{d})$, so $K = F(u) \subseteq F(\sqrt{d})$. On the other hand, we have

   $$2 = [F(\sqrt{d}):F] = [F(\sqrt{d}):F(u)][F(u):F] = 2[F(\sqrt{d}):F(u)].$$

   Therefore, $F(u) = F(\sqrt{d})$, as required. $\square$

7. Let K be an extension of F where $\mathrm{char}(F) \neq 2$. Prove that if $[K:F] = 2$, then K is Galois over F.

   Proof. From Problem 6 we know that there exists $d \in F$, d not a square, such that $K = F(\sqrt{d})$. The elements of K can be written uniquely as $a + b\sqrt{d}$ with $a, b \in F$.

   Since $\mathrm{char}(F) \neq 2$, the two roots of $x^2 - d$ are $\sqrt{d}$ and $-\sqrt{d}$, which are distinct from each other. And there is an isomorphism $\sigma\colon F(\sqrt{d}) \to F(-\sqrt{d})$ such that $\sigma(a) = a$ for all $a \in F$, and $\sigma(\sqrt{d}) = -\sqrt{d}$. And since $F(\sqrt{d}) = F(-\sqrt{d})$, we have $\sigma \in \mathrm{Aut}_F(K)$.

   Let $u = a + b\sqrt{d} \in K$. If $\sigma(u) = u$, then

   $$a + b\sqrt{d} = u = \sigma(u) = a - b\sqrt{d}.$$

Therefore, $b = -b$. Since $\text{char}(F) \neq 2$, this means that $b = 0$, so $u \in F$.

Thus, the fixed field of σ is F. Therefore, $F \subseteq (\text{Aut}_F(K))' \subseteq \langle\sigma\rangle' = F$, so F is the fixed field of $\text{Aut}_F(K)$. This proves that K is Galois over F, as claimed. $\square$

8. Let K be a finite dimensional Galois extension of F, and let L and M be intermediate fields. Use the Fundamental Theorem of Galois Theory to prove the following:

   (i) $\text{Aut}_{LM}(K) = \text{Aut}_L(K) \cap \text{Aut}_M(K)$.

   Proof. Note that LM is the smallest field that contains L and M. By the correspondence clause of the Fundamental Theorem, that means that $\text{Aut}_{LM}(K)$ is the *largest* subgroup that is *contained* in $\text{Aut}_L(K)$ and in $\text{Aut}_M(K)$. This is their intersection. $\square$

   (ii) $\text{Aut}_{L\cap M}(K) = \big\langle \text{Aut}_L(K), \text{Aut}_M(K)\big\rangle$.

   Proof. Since $L \cap M$ is the largest intermediate field contained in both L and M, then $\text{Aut}_{L\cap M}(K)$ is the smallest subgroup that contains both $\text{Aut}_L(K)$ and $\text{Aut}_M(K)$. This is the subgroup they generate. $\square$