ABSTRACT ALGEBRA 2 SOLUTIONS TO THE PRACTICE EXAM

1. Practice exam problems

Problem A. Find $\alpha \in \mathbb{C}$ such that $\mathbb{Q}(i, \sqrt[3]{2}) = \mathbb{Q}(\alpha)$.

Solution to A. Either one can use the proof of the primitive element theorem, or one can just do this by hand. A little experimenting leads to the guess $\alpha = i\sqrt[3]{2}$. This clearly lies in the field $\mathbb{Q}(i, \sqrt[3]{2})$. On the other hand we have $2^{1/3} = (i2^{1/3})^4$ and $i = (i2^{1/3})^9$.

Problem B. Let ϕ_2 be the Frobenius automorphism of $\mathbb{F}_4$, the field with 4 elements. Let $0, 1, \alpha, \beta$ be the elements of $\mathbb{F}_4$. Describe ϕ_2 by indicating the image of each element of $\mathbb{F}_4$ under this map (e.g. $\phi_2(0) = 0$).

Solution to B. The field of four elements consists exactly of the solutions to $x^4 - x$ in $\bar{\mathbb{Z}}_2$. The polynomial factors as $x(x-1)(x^2+x+1)$. The last polynomial has two roots in $\mathbb{F}_4$: α and $\beta = \alpha + 1$. It follows that $\phi_2(0) = 0^2 = 0$, $\phi_2(1) = 1^2 = 1$, $\phi_2(\alpha) = \alpha^2 = \alpha + 1 = \beta$, and $\phi_2(\alpha + 1) = (\alpha + 1)^2 = \alpha^2 + 1 = \alpha$.

Alternatively, there exists $\zeta \in \mathbb{F}_{p^n}$ such that $\mathbb{F}_{p^n} = \mathbb{Z}_p(\zeta)$ and $\mathbb{F}_{p^n}^* = \langle \zeta \rangle$. We have by definition $\sigma_p(y) = y^p$ for all $y \in \mathbb{F}_{p^n}$. Since $|\mathbb{Z}_p^*| = p - 1$ it follows that $\sigma_p(z) = z$ for all $z \in \mathbb{Z}_p$. In our situation, with $p = 2$ and $n = 2$, we see that either $\alpha = \zeta$ and $\beta = \zeta^2$ or $\alpha = \zeta^2$ and $\beta = \zeta$. In any case $\phi_2(\alpha) = \beta$.

Problem C. Give an example of a degree two field extension that is not Galois.

Solution to C. Let t be a variable. The extension $\mathbb{Z}_2(t)$ of $\mathbb{Z}_2(t^2)$ is not separable, and thus is not Galois.

Problem D. Let $\zeta \in \mathbb{C}$ be a primitive 5-th root of unity. Find all field extensions K of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta)$. For each such field extension, find an element $\alpha \in \mathbb{Q}(\zeta)$ such that $K = \mathbb{Q}(\alpha)$.

Solution to D. We have shown that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a cyclic extension. We would like now to describe the cyclic group $G = G(\mathbb{Q}(\zeta)/\mathbb{Q})$ more carefully. The book has a discussion of this; I rehash that here. To begin, ζ is a root of the polynomial $x^5 - 1 \in \mathbb{Q}[x]$. One can check that for a prime p, the polynomial

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1$$

is irreducible over $\mathbb{Q}$ by checking with Eisenstein's criterion that $\Phi_p(x+1)$ is irreducible over $\mathbb{Q}$. Note also, that if ξ is a primitive p-th root of unity, then $\xi, \xi^2, \ldots, \xi^{p-1}$ are also primitive p-th roots of unity, and

$$\Phi_p(x) = (x - \zeta) \cdot \ldots \cdot (x - \zeta^{p-1}).$$

Date: April 26, 2012.

As an aside, more generally, one can define for any natural number n an irreducible monic polynomial $\Phi_n(x) \in \mathbb{Q}[x]$ of degree $\varphi(n)$ whose roots are exactly the primitive n-th roots of unity; see e.g. Lang Theorem VI.3.1.

In any case, we see that

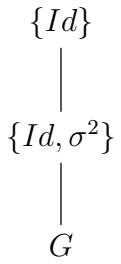
$$\mathrm{irr}(\zeta, \mathbb{Q}) = \Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

and the roots of $\mathrm{irr}(\zeta, \mathbb{Q})$ are $\zeta, \zeta^2, \zeta^3, \zeta^4$.

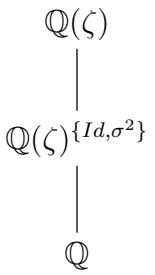
From our theorem on simple extensions, we see that if $\sigma \in G$, then $\sigma(\zeta) = \zeta^i$ for some $1 \leq i \leq 4$. Now for the sake of fixing notation, let us take $\sigma \in G$ such that

$$\sigma(\zeta) = \zeta^2.$$

We clearly have $G = \langle \sigma \rangle \cong \mathbb{Z}_4$, since $\sigma^2(\zeta) = \zeta^4$, $\sigma^3(\zeta) = \zeta^3$ and $\sigma^4(\zeta) = \zeta$. Thus the subgroups of G are described by the diagram below.



By the FTGT we have the corresponding diagram of field extensions describing all field extensions requested in the problem.



The only thing left to do is to find $\alpha \in \mathbb{Q}(\zeta)$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)^{\{Id, \sigma^2\}}$. Since $\{Id, \sigma^2\}$ is normal in G, it follows from the FTGT that $[\mathbb{Q}(\zeta)^{\{Id,\sigma^2\}} : \mathbb{Q}] = |G/\{Id, \sigma^2\}| = 2$. Thus an elementary argument in linear algebra shows that it suffices to find an element $\alpha \notin \mathbb{Q}$ such that $\sigma^2(\alpha) = \alpha$ (show that if $\alpha \notin \mathbb{Q}$, then $1, \alpha$ are linearly independent).

To do this, we use the basis $1, \zeta, \zeta^2, \zeta^3$ for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. We have that $\sigma^2(1) = 1$, $\sigma^2(\zeta) = \zeta^4 = -1 - \zeta - \zeta^2 - \zeta^3$, $\sigma^2(\zeta^2) = \zeta^8 = \zeta^3$ and $\sigma^2(\zeta^3) = \zeta^{12} = \zeta^2$. Thus

$$\begin{aligned} \sigma^2(a + b\zeta + c\zeta^2 + d\zeta^3) &= a + b(-1 - \zeta - \zeta^2 - \zeta^3) + c\zeta^3 + d\zeta^2 \\ &= (a - b) - b\zeta + (d - b)\zeta^2 + (c - b)\zeta^3. \end{aligned}$$

It follows that we can take $a = b = 0$ and $c = d$. In other words $\sigma^2(\zeta^2 + \zeta^3) = \zeta^2 + \zeta^3$ so that $\mathbb{Q}(\zeta)^{\{Id,\sigma^2\}} = \mathbb{Q}(\zeta^2 + \zeta^3)$. To be clear, a solution to the problem is given by taking $\alpha = \zeta^2 + \zeta^3$.

Problem E. Let F be a field. For a polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ we define the derivative $f'(x)$ of $f(x)$ to be the polynomial

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

(a) Show that the map $D : F[x] \to F[x]$ given by $D(f(x)) = f'(x)$ is a linear map of vector spaces.
(b) Find $\ker(D)$. [Hint: The answer may depend on the characteristic of F.]
(c) Show that D satisfies the Leibniz rule: $D(f(x)g(x)) = D(f(x))g(x) + f(x)D(g(x))$ for all $f(x), g(x) \in F[x]$.
(d) Show that $D((f(x)^m)) = mf(x)^{m-1}D(f)$ for each $m \in \mathbb{Z}_{\geq 0}$.

Solution to E. To prove (a), let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$. WLOG we may assume that $n \geq m$. Define $b_{m+1} = \ldots = b_n = 0$. Then

$$D(f(x) + g(x)) = D\left(\sum_{i=0}^{n} (a_i + b_i)x^i\right) = \sum_{i=1}^{n} i(a_i + b_i)x^{i-1} = D(f(x)) + D(g(x)).$$

A similar proof shows that $D(af(x)) = aD(f(x))$ for all $a \in F$. Thus D is a linear map of vector spaces.

(b) Let the charactersitic of F be p. Let $f(x) = \sum_{i=0}^{n} a_i x^i$. Then $D(f) = 0$ if and only if $ia_i = 0$ for $1 \leq i \leq n$. This holds if and only if $a_i = 0$ for all i not divisible by p. In other words,

$$\ker(D) = \{f(x) = a_0 + a_p x^p + \ldots + a_{np} x^{np} : n \in \mathbb{Z}_{\geq 0}\}.$$

In particular, if $p = 0$, then $\ker(D) = F$.

(c) Let $g(x) = \sum_{i=0}^{m} b_i x^i$. I claim first that for $n \in \mathbb{Z}_{\geq 0}$, $D(x^n g) = D(x^n)g + x^n D(g)$. The proof is similar to part (a) so I leave it to you. We can now prove part (c) easily using induction on the degree of $f(x)g(x)$. If the degree is zero, then $D(fg) = 0 = 0 \cdot g + f \cdot 0 = D(f)g + fD(g)$. Now assume that $f(x)$ has degree $n > 0$ and $f(x) = \sum_{i=0}^{n} a_i x^i$. Let $f_{n-1}(x) := \sum_{i=1}^{n-1} a_i x^i$. Let $g(x) = \sum_{i=0}^{m} b_i x^i$. WLOG assume that $n \geq m$. Set $b_{m+1} = \ldots = b_n = 0$. Then using induction, and our first observation, we have

$$D(fg) = D((a_n x^n + f_{n-1})g) = D(a_n x^n g + f_{n-1} g) = a_n D(x^n g) + D(f_{n-1} g) =$$

$$a_n \left(nx^{n-1} g + x^n D(g)\right) + D(f_{n-1})g + f_{n-1} D(g) = \left(na_n x^{n-1} + D(f_{n-1})\right) g + (a_n x^n + f_{n-1})\, D(g)$$

$$= D(f)g + fD(g),$$

completing part (c) of the problem.

(d) This is done by induction on m using part (c). The case $m = 1$ is obvious. Then

$$D(f^m) = D(f \cdot f^{m-1}) = D(f)f^{m-1} + fD(f^{m-1}) = D(f)f^{m-1} + f((m-1)f^{m-2}D(f))$$

$$= mf^{m-1}D(f),$$

completing the problem.

Problem F. Let $\bar{F}$ be an algebraic closure of a field F. Show that $f(x) \in F[x]$ has a root $\alpha \in \bar{F}$ of multiplicity $\mu > 1$ if and only if α is a root of both $f(x)$ and $f'(x)$. [Hint: Consider the factorization $f(x) = (x - \alpha)^\mu g(x)$ in $\bar{F}[x]$ and use the previous problem.]

Solution to F. If $f(x) \in F[x]$ has a root $\alpha \in \bar{F}$ of multiplicity $\mu \geq 0$ then

$$f(x) = (x-\alpha)^{\mu} g(x)$$

for some $g(x)$ with $g(\alpha) \neq 0$. If $\mu \geq 1$ then we have using the previous problem that

$$f'(x) = \mu(x-\alpha)^{\mu-1} g(x) + (x-\alpha)^{\mu} g'(x) = (x-\alpha)^{\mu-1} \left[\mu + (x-\alpha)g'(x)\right].$$

Thus if α is a root of $f(x)$ of degree $\mu > 1$, then $f(\alpha) = f'(\alpha) = 0$. Conversely, suppose that $f(\alpha) = f'(\alpha) = 0$, then it must be that $\mu \geq 1$ since $f(\alpha) = 0$. On the other hand, from the formula above

$$0 = f'(\alpha) = (\alpha - \alpha)^{\mu-1}[\mu].$$

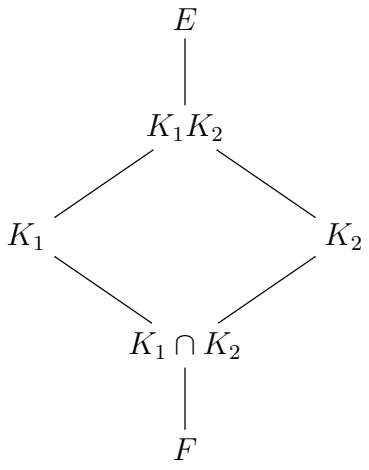
Thus $\mu > 1$.

Problem G. Let E/F be an extension of fields. Let K_1, K_2 be two finite field extensions of F contained in E. Show that if K_1 is a normal extension of F, then K_1K_2 is a normal extension of K_2.

Solution to G. We are given that K_1 is finite and normal over F. Suppose that $K_1 = F(\alpha_1, \ldots, \alpha_n)$. Let $f_i(x) = \mathrm{irr}(\alpha_i, F) \in F[x]$. Then we certainly have that K_1 is the splitting field for the product $f(x) = f_1(x) \ldots f_n(x)$. We also have that $f(x) \in K_2[x]$. Let K' be the splitting field of $f(x)$ over K_2. I claim that $K' = K_1K_2$. Certainly $f(x)$ splits in K_1K_2. Thus $K' \subseteq K_1K_2$. On the other hand, in order for $f(x)$ to split in K' it must be that $\alpha_i \in K'$ for all i. Thus $K_1K_2 = K_2(\alpha_1, \ldots, \alpha_n) \subseteq K'$. It follows that $K_1K_2 = K'$ is the splitting field of $f(x)$ over K_2, and thus is a normal extension of K_2.

Remark 1.1. We can give a similar proof in the case where the extensions are allowed to be infinite normal extensions. Let $I = K_1$, and let $f_\alpha = \mathrm{irr}(\alpha, F)$ for each $\alpha \in I$. Then K_1 is a splitting field for the collection of polynomials $\{f_\alpha\}_{\alpha \in I}$. Note we also have that $f_\alpha \in K_2[x]$. Let K' be the splitting field of $\{f_\alpha\}_{\alpha \in I}$ over K_2. I claim that $K' = K_1K_2$. Certainly $\{f_\alpha\}_{\alpha \in I}$ split in K_1K_2. Thus $K' \subseteq K_1K_2$. Now by definition we have $K_2 \subseteq K'$. To show that $K_1K_2 \subseteq K'$ it suffices to show $K_1 \subseteq K'$. So let $k_1 \in K_1$. We have that k_1 is a root of $f_{k_1} = \mathrm{irr}(k_1, F) \in K_2[x]$. By the definition of a splitting field $k_1 \in K'$. Thus $K_1 \subseteq K'$ and we are done.

Problem H (Optional)**.** Let E be a finite Galois extension of a field F. Let K_1 and K_2 be two extensions of F contained in E. We obtain a diagram of field extensions



Show that $G(E/(K_1K_2)) = G(E/K_1) \cap G(E/K_2) \subseteq G(E/F)$ and $G(E/(K_1 \cap K_2)$ is the subgroup G of $G(E/F)$ generated by the set

$$G(E/K_1)G(E/K_2) = \{\sigma_1\sigma_2 : \sigma_1 \in G(E/K_1), \sigma_2 \in G(E/K_2)\}.$$

[Hint: For the first part, to show $G(E/(K_1K_2)) \supseteq G(E/K_1) \cap G(E/K_2)$, come up with a useful description of the elements of K_1K_2 in terms of those in K_1 and K_2. For the second part, use Galois theory to show $E^G = K_1 \cap K_2$.]

Solution to H. We begin by proving $G(E/(K_1K_2)) = G(E/K_1) \cap G(E/K_2)$. We show first that $G(E/(K_1K_2)) \subseteq (G(E/K_1) \cap G(E/K_2))$. So let $\sigma \in G(E/K_1K_2)$. Then certainly $\sigma \in G(E/K_1)$ and $\sigma \in G(E/K_2)$. Consequently, $\sigma \in G(E/K_1) \cap G(E/K_2)$ proving that $G(E/(K_1K_2)) \subseteq (G(E/K_1) \cap G(E/K_2))$. Conversely, suppose that $\sigma \in G(E/K_1)$ and $\sigma \in G(E/K_2)$. Then $\sigma \in G(E/K_1K_2)$ since any element of K_1K_1 is obtained as the quotient of polynomials generated by a finite number of elements of K_1 and K_2, both of which are fixed by σ by assumption. This proves the opposite inclusion, and hence gives the equality desired.

We now show that $G(E/(K_1 \cap K_2)$ is the subgroup G of $G(E/F)$ generated by the set $G(E/K_1)G(E/K_2)$. I claim that $E^G = K_1 \cap K_2$. By Artin's theorem, this implies that $G = G(E/(K_1 \cap K_2)$, completing the problem, so it suffices to prove the claim.

To begin, it is clear that $K_1 \cap K_2 \subseteq E^G$. We now need to show the opposite inclusion. So let $e \in E^G$. Then since $G(E/K_1) \subseteq G$, we have $e \in E^{G(E/K_1)} = K_1$; the last equality follows from the FTGT that E/K_1 is Galois. Similarly $e \in K_2$. Thus $e \in K_1 \cap K_2$, and so we have $E^G \subseteq K_1 \cap K_2$. This completes the proof of the claim.

Problem I. Let E/F be an extension of fields. Let K_1, K_2 be two field extensions of F contained in E. If K_1 is a finite Galois extension of F, then K_1K_2 is Galois over K_2. Moreover, there is an isomorphism

$$\phi : G(K_1K_2/K_2) \to G(K_1/(K_1 \cap K_2))$$

given by $\sigma \mapsto \sigma|_{K_1}$.

Solution to I. Since K_1 is normal and separable over F, we have seen that it follows that K_1K_2 is normal and separable over K_2. We proved this above for normal extensions, and the proof for separable extensions is similar. You may also simply cite the theorem we stated in class on distinguished classes of extensions. In any case, K_1K_2 is Galois over K_2. We also point out that since K_1 is Galois over F, it follows from the FTGT that K_1 is Galois over $K_1 \cap K_2$.

Now let us consider the definition of the map ϕ. Given $\sigma \in G(K_1K_2/K_2)$, the restriction of σ to K_1 is an embedding of K_1 over F; since K_1 is normal over F, this is indeed an automorphism of K_1. Clearly it fixes $K_1 \cap K_2$, and so we see that indeed $\sigma|_{K_1} \in G(K_1/(K_1 \cap K_2))$. Thus we get a well defined map $\phi : G(K_1K_2/K_2) \to G(K_1/(K_1 \cap K_2))$. It is easy to see that this is a homomorphism of groups.

We now check that it is bijective. First let us check that it is injective. So suppose that $\sigma \in G(K_1K_2/K_2)$ and $\sigma|_{K_1}$ is the identity. Then since every element of K_1K_2 is obtained as the quotient of polynomials generated by a finite number of elements of K_1 and K_2, both of which are fixed by σ by assumption, we see that in fact σ was the identity on K_1K_2. This establishes that $\ker(\phi) = \{Id_{K_1K_2}\}$, and thus ϕ is injective.

Now we show that ϕ is surjective. To do this, let $H = \mathrm{Im}(\phi)$. I claim that $K_1^H = K_1 \cap K_2$. Then by Artin's theorem, it follows that $H = G(K_1/(K_1 \cap K_2))$ and we are done. So let us prove the claim. By definition, $K_1 \cap K_2 \subseteq K_1^H$. On the other hand, let $\alpha \in K_1^H \subseteq K_1 \subseteq K_1K_2$. Then α is also fixed by each $\sigma \in G(K_1K_2/K_2)$ and consequently, it must be in K_2. Thus $\alpha \in K_1 \cap K_2$. In other words, we have proven the claim that $K_1^H = K_1 \cap K_2$.