ABSTRACT ALGEBRA 2 SOLUTIONS TO THE PRACTICE EXAM AND HOMEWORK

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, 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. We have seen (Mini-Midterm II) that 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 22, 2010.

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

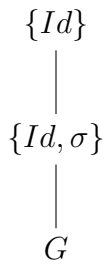
$$\mathrm{irr}(\zeta, \mathbb{Q}) = \Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

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

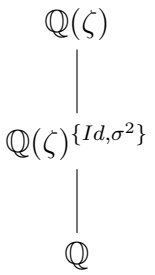
From our theorem on simple extensions, we see that if $\sigma \in G$, then $\sigma(\zeta) = \zeta^i$ for some $1 \leq i \leq 4$. Now for the sake of fixing notation, let us take $\sigma \in G$ such that

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

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 F be a field, and let t be a variable. Let

$$s = \frac{p(t)}{q(t)} \in F(t).$$

and let $F(s) \hookrightarrow F(t)$ be the associated inclusion of fields. Assuming $s \notin F$, and $p(t)$ and $q(t)$ have no common irreducible factors, show that

$$[F(t) : F(s)] = \max(\deg(p(t)), \deg(q(t))).$$

[Hint: Consider the polynomial $p(X) - sq(X) \in F(s)[X]$ and recall that if D is a UFD with field of fractions K, and $f(X) \in D[X]$ is a primitive polynomial, then $f(X)$ is irreducible in $D[X]$ if and only if it is irreducible in $K[X]$.]

Solution to G. To begin, we have that $t \in F(t)$ is a root of the polynomial

$$p(X) - q(X)s \in F(s)[X].$$

I claim that this polynomial is irreducible. We will use the fact that if D is a UFD and $p(X) \in D[X]$ is a primitive polynomial, then $p(X)$ is irreducible in $D[X]$ if and only if it is irreducible in $K(D)[X]$ [This is standard, and is not hard to show. See for example Lemma 45.27]. In particular, since $F[s]$ is a UFD, to show that $p(X) - q(X)s$ is irreducible in $F(s)[X]$, it suffices to show that it is primitive and irreducible in $F[s][X]$. It is clearly primitive. So suppose there are polynomials $A(s, X)$ and $B(s, X)$ in $F[s, X]$ such that

$$A(s, X)B(s, X) = p(X) - q(X)s.$$

We may write

$$A(s, X) = \sum_{i=0}^{n} a_i(X)s^i \text{ and } B(s, X) = \sum_{i=0}^{m} b_i(X)s^i$$

for some $a_i(X), b_i(X) \in F[X]$ with $a_n(X) \neq 0, b_m(X) \neq 0$. Then, multiplying the polynomials, we have that $s^{m+n} = s$. WLOG we may assume $n = 1$ and $m = 0$. Then we have

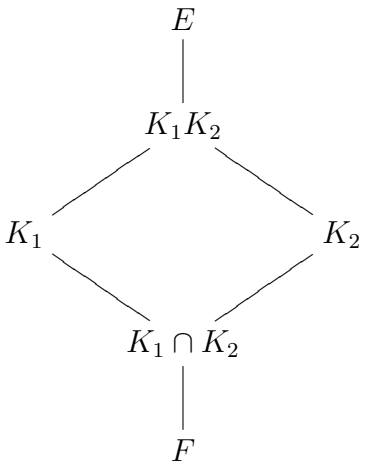
$$\left(a_0(X) + a_1(X)s\right) b_0(X) = p(X) - q(X)s,$$

so that $b_0(X)$ divides $p(X)$ and $q(X)$. It follows that $b_0(X)$, and hence $B(s, X)$, is a constant. Thus $p(X) - q(X)s$ is irreducible. Since the degree of $p(X) - q(X)s$ in $F(s)[X]$ is $\max(\deg p, \deg q)$, we have completed the proof.

Problem H. 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 H. We are given that K_1 is finite and normal over F. Suppose that $K_1 = F(\alpha_1, \ldots, \alpha_n)$. Let $f_i(x) = \text{irr}(\alpha_i, F) \in F[x]$. 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.

Problem I (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 I. 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 J. 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 J. 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 $K_1^H = K_1 \cap K_2$.

2. Homework on $\mathbb{P}GL_2(F)$

Problem K. Let F be a field, and let $M_2(F)$ be the set of 2×2 matrices with entries in F. The group of invertible matrices, $GL_2(F)$, is the subset consisting of those matrixes $A \in M_2(F)$ such that $\det(A) \neq 0$. For $\lambda \in F$, we will denote by $[\lambda]$ the matrix entries λ on the diagonal, and zeros in every other entry. In other words,

$$[\lambda] = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

(1) Show that we may define an equivalence relation on $GL_n(F)$ by setting

$$A \sim A'$$

whenever $A, A' \in GL_n(F)$ and there exists $\lambda \in F^*$ such that $A = [\lambda]A'$.

(2) We define a set $\mathbb{P}GL_2(F)$ to be the quotient of $GL_2(F)$ by this equivalence relation. I.e.

$$\mathbb{P}GL_2(F) = GL_2(F)/\sim .$$

We will use the notation $\bar{A}$ for the equivalence class of a matrix $A \in GL_2(F)$ in $PGL_2(F)$. Show that $\mathbb{P}GL_2(F)$ is a group under the composition law given by $\bar{A}\bar{A'} = \overline{AA'}$.

Solution to K. (1) We have $A \sim A$ taking $\lambda = 1$. If $A \sim B$ there exists $\lambda \in F^*$ such that $A = [\lambda]B$. Then $B = [\lambda^{-1}]A$ so $B \sim A$. The final condition, that $A \sim B$ and $B \sim C$ imply that $A \sim C$, is similar. (2) First we check the operation is well defined. We have $[\lambda_1]A_1[\lambda_2]A_2 = [\lambda_1\lambda_2]A_1A_2 \sim A_1A_2$. In other words $\overline{A_1A_2}$ is independent of the choice of representative for the classes $\bar{A}_1$ and $\bar{A}_2$. Now let us check that $\mathbb{P}GL_2$ is a group under this operation. It is easy to check that the identity in the group is given by $\overline{[1]}$. We have $(\bar{A})^{-1} = \overline{A^{-1}}$. Finally, we have $\bar{A}_1(\bar{A}_2\bar{A}_3) = \bar{A}_1(\overline{A_1A_2}) = \overline{A_1A_2A_3} = (\overline{A_1A_2})\bar{A}_3 = (\bar{A}_1\bar{A}_2)\bar{A}_3$.

Problem L. Let F be a field. Let G be the subset of $F(x)^*$ consisting of elements of the form

$$\frac{ax+b}{cx+d}$$

such that there does not exist $\lambda \in F^*$ such that $ax + b = \lambda(cx + d)$.

(1) Show that

$$G = \left\{ \frac{ax+b}{cx+d} \in F(x)^* : ad - bc \neq 0 \right\}.$$

(2) Show that G is a group under composition.

(3) Show that there is a group isomorphism

$$G \to \mathbb{P}GL_2(F)$$

given by

$$\frac{ax+b}{cx+d} \mapsto \overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}.$$

Solution to L. (1) This is just the observation that an $n \times n$ matrix is nonsingular (nonzero determinant) if and only if the row rank of the matrix is equal to n. (2) and (3) Let us observe that we have

$$\frac{a\left(\frac{a'x+b'}{c'x+d'}\right)+b}{c\left(\frac{a'x+b'}{c'x+d'}\right)+d} = \frac{a(a'x+b')+b(c'x+d')}{c(a'x+b')+d(c'x+d')} = \frac{(aa'+bc')x+(ab'+bd')}{(ca'+dc')x+(cb'+dd')}.$$

Moreover,

$$(aa'+bc')(cb'+dd') - (ab'+bd')(ca'+dc') =$$

$$\det\begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix}\det\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

The remainder of the problem is straightforward.

3. Optional homework problems on $\mathbb{P}^1_F$

Problem M. Let F be a field.

(1) Show that we may define an equivalence relation on $F^2 - (0,0)$ by setting

$$(x_0, x_1) \sim (x_0', x_1')$$

if and only if there exists $\lambda \in F^*$ such that $(x_0, x_1) = (\lambda x_0', \lambda x_1')$.

(2) We define the projective line over F, denoted $\mathbb{P}^1_F$, to be the quotient of $F^2 - (0,0)$ by this equivalence relation. I.e.

$$\mathbb{P}^1_F = \big(F^2 - (0,0)\big) / \sim .$$

We use the notation $[x_0 : x_1]$ for the equivalence class of (x_0, x_1) in $\mathbb{P}^1$. Now let

$$U_0 = \{[x_0 : x_1] \in \mathbb{P}^1_F : x_0 \neq 0.\}$$

Show that there is a bijection of sets

$$F \to U_0 \subset \mathbb{P}^1_F$$

given by $a \mapsto [1 : a]$.

(3) Show that

$$\mathbb{P}^1_F = U_0 \sqcup [0 : 1].$$

In other words, using (2) we can think of the projective line as our field F together with one "extra" point. This point is typically called the point at infinity.

Solution to M. (1) We check the definition of an equivalence relation. We have $(x_0, x_1) \sim (x_0, x_1)$ taking $\lambda = 1$. The condition of symmetry and transitivity are similar. (2) The map is injective since $[1 : a] = [1 : b]$ if and only if $a = b$. The map is surjective since for any $[x_0 : x_1] \in U_0$, we have $[x_0 : x_1] = [1 : x_1/x_0]$ so that $[x_0 : x_1]$ is the image of $x_1/x_0 \in F$. (3) If $[x_0 : x_1] \notin U_0$ then it follows that $x_0 = 0$. Thus $[x_0 : x_1] = [0 : x_1] = [0 : 1]$.

Problem N. Let F be a field. A polynomial $f(X_0, X_1) \in F[X_0, X_0]$ is homogeneous of degree $d \in \mathbb{Z}_{\geq 0}$ if each monomial (with non-zero coefficient) in $f(X_0, X_1)$ is of degree d. For instance, $X_0^2 - X_0X_1$ is homogeneous of degree 2, whereas $X_0^2 - X_1$ is not homogeneous. In general, we may write a homogeneous polynomial of degree d in the form

$$f(X_0, Y_0) = \sum_{i=0}^{d} a_i X_0^{d-i} X_1^i,$$

for some $a_0, \ldots, a_d \in F$.

(1) Show that if $f(X_0, X_1) \in F[X_0, X_1]$ is homogenous of degree d then for each $\lambda \in F$,

$$f(\lambda X_0, \lambda X_1) = \lambda^d f(X_0, X_n).$$

(2) Use part (1) to show that if $f_0(X_0, X_1)$ and $f_1(X_0, X_1)$ are homogeneous polynomials of degree $d > 0$ with no common roots in F, then there is a well defined map of sets

$$f : \mathbb{P}^1_F \to \mathbb{P}^1_F$$

given by $[x_0 : x_1] \mapsto [f_0(x_0, x_1) : f_1(x_0, x_1)]$.

(3) Assume that F is algebraicly closed and $\mathrm{char}(F) = p$. Show that the map in (2) is bijective if and only if $f_0 = (a_0X_0 + b_0X_1)^{p^m}$ and $f_1 = (a_1X_0 + b_1X_1)^{p^m}$ for some integer $m \geq 0$, and some $a_0, a_1, b_0, b_1 \in F$. We use the convention that $0^m = 1$ for all m.

Solution to N. I will leave (1) and (2) to you, and will prove (3). I will also leave it to you to prove that if f_0 and f_1 have degree 1, then f is bijective. Suppose that f_0 and f_1 are of degree $d > 1$. Then $f^{-1}([0:1])$ consists of at least two points, unless $f_0 = (a_0X_0 + b_0X_1)^d$. Similarly, $f^{-1}([1:0])$ consists of at least two points, unless $f_1 = (a_1X_0 + b_1X_1)^d$. So assume that $f_0 = (a_0X_0 + b_0X_1)^d$ and $f_1 = (a_1X_0 + b_1X_1)^d$. Then f can be decomposed into two maps

$$\mathbb{P}^1_F \xrightarrow{g} \mathbb{P}^1_F \xrightarrow{h} \mathbb{P}^1_F$$

where $f = h \circ g$ and g is defined by the polynomials $a_0X_0 + b_0X_1$ and $a_1X_0 + b_1X_1$, and h is defined by the polynomials X_0^d and X_1^d. Since g is bijective, f is bijective if and only if h is bijective. We recall (and prove below) that for each $\alpha \in F$, $t^d - \alpha$ has exactly one root in $\bar{F}(= F)$ if and only if $d = p^m$. It follows that h is injective if and only if $d = p^m$. Indeed, consider $h^{-1}([1:\alpha])$. This consists of all $[1:t]$ such that $t^d = \alpha$. The argument for points of the form $[\alpha : 1]$ is identical. Since F is algebraicly closed, this also shows that the map is surjective. This completes the proof, up to recalling the proof of the claim above.

We now recall the proof of the fact that for each $\alpha \in F$, $t^d - \alpha$ has exactly one root in $\bar{F}$ if and only if $d = p^m$. To begin, recall that $t^d - 1$ has exactly one root if and only if $d = p^m$. Indeed, let $d = p^m d'$ where p does not divide d'. Then

$$t^d - 1 = (t^{d'} - 1)^{p^m}.$$

Now $t^{d'} - 1$ is separable, so it has exactly d' roots in $\bar{F}$. Thus $t^d - 1$ has exactly one root if and only if $d' = 1$; in other words, if and only if $d = p^m$.

Now any two roots of $t^d - \alpha$ differ by multiplication by a d-th root of unity. Indeed, if β and γ are roots of $t^d - \alpha$, then $(\beta/\gamma)^d = \alpha/\alpha = 1$, so that β/γ is a d-th root of unity. Thus there will be exactly one root of $t^d - \alpha$ in $\bar{F}$ if and only if $d = p^m$.

Problem O. Let F be a field.

(1) Consider the subset

$$F(X_0, X_1)_0 := \left\{ \frac{p(X_0, X_1)}{q(X_0, X_1)} \in F(X_0, X_1) : p, q \in F[X_0, X_1], q \neq 0, \text{and} \right.$$

$$\left. p, q \text{ are homogeneous of the same degree} \right\}$$

Show that this is a subfield of $F(X_0, X_1)$.

(2) Show that there is an isomorphism of fields

$$\Phi : F(x) \to F(X_0, X_1)_0$$

given by

$$\frac{\sum_{i=0}^n a_i x^i}{\sum_{j=0}^m b_j x^j} \mapsto X_0^{m-n} \frac{\sum_{i=0}^n a_i X_0^{n-i} X_1^i}{\sum_{j=0}^m b_j X_0^{m-j} X_1^j}$$

Solution to O. (1) We have $1 = 1/1$ and $0 = 0/1$ are in $F(X_0, X_1)_0$. If $a = p/q$ and $b = r/s$ are in $F(X_0, X_1)_0$ then $a + b = (ps + qr)/qs$ is in $F(X_0, X_1)$. The rest is similar. (2) The inverse map is given by $p(X_0, X_1)/q(X_0, X_1) \mapsto p(1, x)/q(1, x)$. I leave it to you to show that these are ring homomorphisms.