MATH 830 FALL 2021: HOMEWORK 1, SOLUTIONS

You may work together on these homework problems, but each student in the class must write up the solutions to this assignment entirely on their own. You may freely use the class notes, but please do not consult any textbooks, the internet, graduate students not in this class, or any professor except your Math 830 instructor - who is always happy to discuss any algebra problem. You have two weeks to work on this assignment. Please upload a pdf copy of your solutions to Blackboard no later than 10pm on September 20.

1. Let $F \subseteq K$ be fields and suppose $\alpha \in K$ is algebraic over F and has the property that $[F(\alpha) : F]$ is odd. Prove that $F(\alpha^2) = F(\alpha)$.

Solution. We clearly have $F \subseteq F(\alpha^2) \subseteq F(\alpha)]$. Note that α satisfies $x^2 - \alpha^2$ over $F(\alpha^2)$. It follows that, $[F(\alpha) : F(\alpha^2)] \leq 2$. Since$[F(\alpha) : F]$ is odd and divisible by $[F(\alpha) : F(\alpha^2)]$, it must hold that $[F(\alpha) : F(\alpha^2)] = 1$. That is, $F(\alpha^2) = F(\alpha)$.

2. Suppose $F \subseteq K$ are fields and $\alpha, \beta \in K$ satisfy $[F(\alpha) : F] = n$ and $[F(\beta) : F] = m$.
   (i) Show that $[F(\alpha, \beta) : F(\alpha)] = m$ if and only if $[F(\alpha, \beta) : F(\beta)] = n$.
   (ii) Prove that the conditions in (i) hold if n and m are relatively prime.

Solution. For (i), we have

$$\begin{aligned}[F(\alpha, \beta) : F] &= [F(\alpha, \beta) : F(\alpha)] \cdot [F(\alpha) : F] = [F(\alpha, \beta) : F(\alpha)] \cdot n \\ &= [F(\alpha, \beta) : F(\beta)] \cdot [F(\beta) : F] = [F(\alpha, \beta) : F(\beta)] \cdot m.\end{aligned}$$

Thus $[F(\alpha, \beta) : F(\alpha)] \cdot n = [F(\alpha, \beta) : F(\beta)] \cdot m$, from which the result follows.

For part (ii), from part (i) we have

$$[F(\alpha, \beta) : F(\alpha)] \cdot n = [F(\alpha, \beta) : F(\beta)] \cdot m.$$

If n and m are relatively prime, then n divides $[F(\alpha, \beta) : F(\beta)]$. Since $[F(\alpha, \beta) : F(\beta)] \leq n$, we must have $n = [F(\alpha, \beta) : F(\beta)]$. It follows immediately that the conditions in (i) hold, and in fact, $[F(\alpha, \beta) : F] = n \cdot m$.

3. Let $F \subseteq K$ be fields and L, M intermediate fields between K and F. Write LM for the intersection of all subfields of K containing L and M. Thus, LM is the smallest subfield of K containing both L and M, and is called the *compositum* of L and M.
   (i) Show that LM is the set of elements E in K of the form $(\alpha_1\beta_1 + \cdots + \alpha_n\beta_n) \cdot (u_1v_1 + \cdots + u_sv_s)^{-1}$, with $\alpha_i, u_j \in L$ and $\beta_i, v_j \in M$, and any $n, s \geq 1$.
   (ii) Show that $[LM : F] < \infty$ if and only $[L : F] < \infty$ and $[M : F] < \infty$. (Hint: For the *if* direction, show that LM is the set of elements in K of the form $\alpha_1\beta_1 + \cdots + \alpha_n\beta_n$ with $\alpha_i \in L$ and $\beta_i \in M$.)
   (iii) Prove that if the conditions in (ii) hold, then $[LM : F]$ is a common multiple of $[L : F]$ and $[M : F]$ and is less than or equal to $[L : F] \cdot [M : F]$.
   (iv) Show that if $[L : F]$ and $[M : F]$ are relatively prime, then $[LM : F] = [L : F] \cdot [M : F]$.

Solution. For (i), since LM is a field containing L and M, every expression of the form

$$(\alpha_1\beta_1 + \cdots + \alpha_n\beta_n) \cdot (u_1v_1 + \cdots + u_sv_s)^{-1},$$

with $\alpha_i, u_j \in L$ and $\beta_i, v_j \in M$, and any $n, s \geq 1$ belongs to LM, so $E \subseteq LM$. Conversely, by definition, E is a subset of K that is closed under multiplication, addition and taking inverses, and thus E is a subfield of K. Since L and M are contained in E, it follows that E is a subfield of K containing L and M, and therefore $LM \subseteq E$. Thus, $E = LM$, as required.

For (ii), since $L, M \subseteq LM$, it follows immediately that $[L : F]$ and $[M : F]$ are finite if $[LM : F]$ is finite. Conversely, suppose $[L : F]$ and $[M : F]$ are finite. Let $l_1, \ldots, l_r$ be a basis for L over F (so that $[L : F] = r$) and $m_1, \ldots, m_t$ be a basis for M over F (so that $[M : F] = t$). Since every element in L is an

F-linear combination of $l_1, \ldots, l_r$ and such elements are closed under addition and multiplication, and every element in M is an F-linear combination of $m_1, \ldots, m_t$, and these elements are closed under addition and multiplication, it follows that the set T of all F-linear combinations of $\{l_i m_j\}_{1 \le i \le r, 1 \le j \le t}$ is closed under addition and multiplication. Note that T is also a vector space over F of dimension at most rt. If $0 \neq u \in T$, then $1, u^2, \ldots, u^{rt}$ are linearly independent over F. Let $a_0 + a_1 u + \cdots + a_c u^c = 0$ be a shortest dependence relation. Then $a_0 \neq 0$, so we may divide by a_0 to obtain a relation $1 + a_1' u + \cdots + a_c' u^c = 0$, with each $a_j' \in F$. It follows that $u(-a_1 - \cdots - a_c u^{c-1}) = 1$. Since $-a_1 - \cdots - a c u^{c-1} \in T$, this shows that T is closed under taking multiplicative inverses. Thus, T is a subfield of K. Since T contains L and M, we have $LM \subseteq T \subseteq LM$, and thus $T = LM$, showing that $[LM : F]$ is finite.

For (iii), suppose $[L : F] = r$ and $[M : F] = t$, with r and t relatively prime. Then by part (i), $[LM : F] < \infty$. We have

$$[LM : F] = [LM : L] \cdot [L : F] = [LM : L] \cdot r \quad \text{and} \quad [LM : F] = [LM : M] \cdot [M : F] = [LM : M] \cdot t.$$

Since r and t are relatively prime, r divides $[LM : M]$, so that $[LM : F] = [LM : M] \cdot t \ge rt$. But part (ii) shows that $[LM : F] \le rt$, which gives $[LM : F] = rt$, which is what we want.

4. For $f(x) = x^3 + x + 1$ and $g(x) = x^4 + 3x^2 + x + 7$ in $\mathbb{Q}[x]$, find rational polynomials $a(x), b(x) \in \mathbb{Q}[x]$ such that $1 = a(x)f(x) + b(x)g(x)$.

Solution. The first step is to use the Euclidean algorithm to find, the GCD, i.e., the last non-zero remainder upon repeated applications of the division algorithm. This leads to:

$$\begin{aligned} g(x) &= x f(x) + (2x^2 + 7) \\ f(x) &= \frac{x}{2}(2x^2 + 7) + (-\frac{5}{2}x + 1) \\ 2x^2 + 7 &= -(\frac{4}{5}x + \frac{8}{25})(-\frac{5}{2}x + 1) + \frac{183}{25}. \end{aligned}$$

Recalling that GCDS are unique up to units, we see that 1 is the GCD of $f(x)$ and $g(x)$. We use backwards substitution with the equations above to solve for $\frac{183}{25}$ in terms of $f(x)$ and $g(x)$.

$$\begin{aligned} \frac{183}{25} &= 1 \cdot (2x^2 + 7) + (\frac{4}{5}x + \frac{8}{25})(-\frac{5}{2}x + 1) \\ \frac{183}{25} &= 1 \cdot (2x^2 + 7) + (\frac{4}{5}x + \frac{8}{25})(f(x) - \frac{x}{2}(2x^2 + 7)) \\ \frac{183}{25} &= (\frac{4}{5}x + \frac{8}{25})f(x) + (1 - \frac{2}{5}x^2 - \frac{4}{25}x)(2x^2 + 7) \\ \frac{183}{25} &= (\frac{4}{5}x + \frac{8}{25})f(x) + (1 - \frac{2}{5}x^2 - \frac{4}{25}x)(g(x) - x f(x)) \\ \frac{183}{25} &= (\frac{8}{25} - \frac{1}{5}x + \frac{4}{25}x^2 + \frac{2}{5}x^3)f(x) + (1 - \frac{2}{5}x^2 - \frac{4}{25}x)g(x). \end{aligned}$$

Multiplying the last equation by $\frac{25}{183}$, we obtain

$$a(x) = \frac{8}{183} - \frac{5}{183}x + \frac{4}{183}x^2 + \frac{10}{183}x^3 \quad \text{and} \quad b(x) = \frac{25}{183} - \frac{10}{183}x^2 - \frac{4}{183}x.$$

5. Prove that $g(x)$ from the previous problem is irreducible over $\mathbb{Q}$. Then, let $\alpha \in \mathbb{C}$ be a root of $g(x)$. For $f(x)$ as in 2, find $f(\alpha)^{-1}$ as an element of $\mathbb{Q}(\alpha)$, written in terms of the basis $1, \alpha, \alpha^2, \alpha^3$. Similarly, find $f(\alpha)h(\alpha)$ as an element of $\mathbb{Q}(\alpha)$, written in terms of the basis, for $h(x) = x^3 + 4x^2 + x$.

Solution. Note that $g(x)$ is a primitive polynomial, thus, by Gauss's Lemma, to see that $g(x)$ is irreducible over $\mathbb{Q}$, it suffices to see that $g(x)$ is irreducible over $\mathbb{Z}$. By the Rational Root Test, $g(x)$ does not have a root in $\mathbb{Q}$, so $g(x)$ does not factor as a product of a linear polynomial and a cubic polynomial with coefficients in $\mathbb{Z}$. Suppose $g(x) = (x^2 + a_1 x + a_0)(x^2 + b_1 x + b_0)$, with each $a_i, b_i \in \mathbb{Z}$. This single equation in $\mathbb{Z}[x]$ gives

rise to the system of equations over $\mathbb{Z}$

$$\begin{aligned} a_1 + b_1 &= 0 \\ a_1b_1 + a_0 + b_0 &= 3 \\ a_0b_1 + a_1b_0 &= 1 \\ a_0b_0 &= 7. \end{aligned}$$

I will leave it to you to verify that this system of equations has no solutions over $\mathbb{Z}$, which implies that $g(x)$ is irreducible over $\mathbb{Z}$.

To find $f(\alpha)^{-1}$, upon substituting α in the the last displayed equation above in problem 3 involving $\frac{183}{25}$, we see that

$$f(\alpha)^{-1} = a(\alpha) = \frac{8}{183} - \frac{5}{183}\alpha + \frac{4}{183}\alpha^2 + \frac{10}{183}\alpha^3.$$

Moreover, one calculates $f(x)h(x) = (x^2 + 4x - 1)g(x) + (-8x^3 - 3x^2 - 26x + 7)$, so writing $f(\alpha)g(\alpha)$ in terms of the basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ we get $f(\alpha)h(\alpha) = -8\alpha^3 - 3\alpha^2 - 26\alpha + 7$.

6. Show that the degree of the minimal polynomial of $\sqrt{3} + \sqrt{5}$ over $\mathbb{Q}$ is four. Use this to prove that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$. Find the minimal polynomial of $\sqrt{3} + \sqrt{5}$ over $\mathbb{Q}$.

Solution. We first note that $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$. This follows, since $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$, the proof of which is similar to the proof that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ that we gave in class. Now, $1, \sqrt{3}, \sqrt{5}, \sqrt{15}$ is a basis for for $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$. Set $\beta := \sqrt{3} + \sqrt{5}$ and multiply each basis element by β. This yields the set of equations

$$\begin{aligned} \beta \cdot 1 &= 0 \cdot 1 + 1 \cdot \sqrt{3} + 1 \cdot \sqrt{5} + 0 \cdot \sqrt{15} \\ \beta \cdot \sqrt{3} &= 3 \cdot 1 + 0 \cdot \sqrt{3} + 0 \cdot \sqrt{5} + 1 \cdot \sqrt{15} \\ \beta \cdot \sqrt{5} &= 5 \cdot 1 + 0 \cdot \sqrt{3} + 0 \cdot \sqrt{5} + 1\sqrt{15} \\ \beta \cdot \sqrt{15} &= 0 \cdot 1 + 5 \cdot \sqrt{3} + 3 \cdot \sqrt{3} + 0 \cdot \sqrt{15}. \end{aligned}$$

As we saw in class, this yields the matrix equation

$$A \cdot \begin{bmatrix} 1 \\ \sqrt{3} \\ \sqrt{5} \\ \sqrt{15} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

where $A = \begin{bmatrix} -\beta & 1 & 1 & 0 \\ 3 & -\beta & 0 & 1 \\ 5 & 0 & -\beta & 1 \\ 0 & 5 & 3 & -\beta \end{bmatrix}$. The determinant of A equals zero, so $\beta^4 - 16\beta^2 + 4 = 0$, i.e., β is a root of $f(x) = x^4 - 16x^2 + 4$. If we show that $f(x)$ is irreducible over $\mathbb{Q}$, then it will be the minimal polynomial of β over $\mathbb{Q}$. One way to do this is as follows: We set $y = x^2$ and define a ring homomorphism $\phi : \mathbb{Q}[x] \to \mathbb{Q}[y]$, by $\phi(g(x)) = g(y) = g(x^2)$, for all $g(x)$ in $\mathbb{Q}[x]$. It is straightforward to check that ϕ is an isomorphism of rings. It follows that for $g(x) \in \mathbb{Q}[x]$, $g(x)$ is irreducible over $\mathbb{Q}$ if and only if $\phi(g(x))$ is irreducible over $\mathbb{Q}$. Since $y^2 - 16y + 4$ is irreducible over $\mathbb{Q}$, it follows that $f(x)$ is irreducible over $\mathbb{Q}$, which is what we want. Alternately, we can use Gauss's Lemma as in the previous problem (since $f(x)$ is a primitive polynomial). Suppose $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$. If one of $g(x), h(x)$ has degree one, then $f(x)$ has a root in $\mathbb{Q}$, but the Rational Root Test fails for $f(x)$, so such a factorization fails for $f(x)$. Suppose $g(x) = x^2 + a_1x + a_0$ and $h(x) = x^2 + b_1x + b_0$ belong to $\mathbb{Z}[x]$. Then the equation $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$ yields the following system of equations over $\mathbb{Z}$:

$$\begin{aligned} a_1 + b_1 &= 0 \\ a_1b_1 + a_0 + b_0 &= -16 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_0 &= 4. \end{aligned}$$

I leave it to you to check that this system has no solutions over $\mathbb{Z}$. Thus $f(x)$ is irreducible over $\mathbb{Z}$, and so $f(x)$ is the minimal polynomial of $\sqrt{3}+\sqrt{5}$ over $\mathbb{Q}$. Thus $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ has degree 4 over $\mathbb{Q}$ and since $\mathbb{Q}(\sqrt{3}+\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3},\sqrt{5})$ these fields must be equal.

7. Prove the following generalization of Part (iv) in Proposition 2.1. Let $\sigma : F \to F_0$ be an isomorphism of fields. Let $F \subseteq K$ and $F_0 \subseteq K_0$ be field extensions. Let $f(x) \in F[x]$ be irreducible over F, so that $f_0(x) := f^\sigma(x)$ is irreducible over F_0. Here $f^\sigma(x)$ denotes the polynomial in $F_0[x]$ obtained by applying σ to the coefficients of $f(x)$. Finally, let $\alpha \in K$ be a root of $f(x)$ and $\alpha_0 \in K_0$ be a root of $f_0(x)$. Prove that there exists $\tau : F(\alpha) \to F_0(\alpha_0)$ an isomorphism of fields extending σ. We will see that this is a key method in calculating the Galois group of a finite extension.

Solution. The proof is quite similar to the proof given in Proposition 2.1. The point is that the field structure of $F(\alpha)$ is determined by the arithmetic in $F[x]$ upon division by $f(x)$, while the field structure of $F_0(\alpha_0)$ is determined by the arithmetic in $F_0[x]$ upon division by $f_0(x)$, and since the rings $F[x]$ and $F_0[x]$ are isomorphic and $f_0(x)$ corresponds to $f(x)$ under this isomorphism, we expect the fields $F(\alpha)$ and $F_0(\alpha)$ to be isomorphic.

Let us continue to use $h^\sigma(x)$ to denote the polynomial in $F_0[x]$ obtained by applying σ to the coefficients of $h(x)$, for any $h(x) \in F[x]$. I leave it to you to check that $\phi : F[x] \to F_0[x]$ defined by $\phi(h(x)) = h^\sigma(x)$ is an isomorphism of rings. Assume that $f(x)$ and $f_0(x)$ each have degree d. For $A \in F(\alpha), A = a_0 + \cdots + a_{d-1}\alpha^{d-1}$, we define

$$\tau(A) := \sigma(a_0) + \cdots + \sigma(a_{d-1})\alpha_0^{d-1}.$$

As before, we let $A(x)$ be the polynomial in $F[x]$ corresponding to A, so that $A = A(\alpha)$. Similarly, for $B = b_0 + \cdots + b_{d-1}\alpha^{d-1}$ in $F(\alpha)$, we let $B(x)$ denote the corresponding polynomial in $F[x]$, so that $B = B(\alpha)$. Now,

$$\begin{aligned}
\tau(A+B) &= \tau((a_0+b_0) + \cdots + (a_{d-1}+b_{d-1})\alpha^{d-1}) \\
&= \sigma(a_0+b_0) + \cdots + \sigma(a_{d-1}+b_{d-1})\alpha_0^{d-1} \\
&= \sigma(a_0) + \sigma(b_0) + \cdots + (\sigma(a_{d-1}) + \sigma(b_{d-1}))\alpha_0^{d-1} \\
&= \{\sigma(a_0) + \cdots + \sigma(a_{d-1})\alpha_0^{d-1}\} + \{\sigma(b_0) + \cdots + \sigma(b_{d-1})\alpha_0^{d-1}\} \\
&= \tau(A) + \tau(B).
\end{aligned}$$

Now suppose $A(x)B(x) = f(x)h(x) + r(x)$, where $r(x)$ has degree less than d. Then, applying the ring isomorphism ϕ to this equation yields $A^\sigma(x)B^\sigma(x) = f_0(x)h^\sigma(x) + r^\sigma(x)$. So, in $F(\alpha)$, we have $A \cdot B = r(\alpha)$, from which it follows that $\tau(A \cdot B) = r^\sigma(\alpha_0)$. On the other hand, $\tau(A) = A^\sigma(\alpha_0)$ and $\tau(B) = B^\sigma(\alpha_0)$. Since $A^\sigma(x)B^\sigma(x) = f_0(x)h^\sigma(x) + r^\sigma(x)$, it follows that $\tau(A) \cdot \tau(B) = r^\sigma(\alpha_0)$, so $\tau(A \cdot B) = \tau(A) \cdot \tau(B)$. Thus, τ is a field homomorphism. Since field homomorphisms are always one-to-one, and ϕ is surjective, it is easy to see that τ is also surjective, and thus τ is an isomorphism from $F(\alpha)$ to $F(\alpha_0)$ extending σ.

8. Let F be a field and $f(x) \in F[x]$. Write $f'(x)$ for the formal derivative of $f(x)$ and assume $f'(x) \neq 0$.
   (i) Prove that $f(x)$ has a repeated root (possibly in a larger field) if and only if $f'(x) = 0$ or $f(x)$ and $f'(x)$ have a common factor in $F[x]$. Recall α is a repeated root of $f(x)$ iff $(x-\alpha)^2$ is a factor of $f(x)$ over the splitting field of $f(x)$. Hint: $f'(x) = 0$ can only occur if F has characteristic $p > 0$.
   (ii) Prove that if $f'(x) = 0$, then every root is a repeated root.

Solution. For part (i), suppose $f(x)$ has a repeated root (possibly in $\overline{F}$). Then $f(x) = (x-a)^2 g(x)$, for some $a \in \overline{F}$ and $g(x) \in \overline{F}[x]$. This gives $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x)$, so $f'(a) = 0$. Suppose $f'(x) \neq 0$. If $f(x)$ and $f'(x)$ have no common factor in $F[x]$, then we may write $1 = g(x)f(x) + h(x)f'(x)$, with $g(x), h(x) \in F[x]$. Setting $x = a$ yields $0 = 1$, a contradiction Thus, $f(x)$ and $f'(x)$ have a common factor.

Conversely, suppose $f'(x) = 0$. Write $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ over $\overline{F}$. Then

$$0 = f'(x) = \Pi_{i \neq 1}(x-\alpha_i) + \cdots + \Pi_{i \neq n}(x-\alpha_i).$$

All of the terms $\Pi_{i \neq j}(x-\alpha_i)$ with $j \neq 1$ in the sum above are divisible by $x-\alpha_1$, so the first terms is divisible by $x-\alpha_1$. By the UFD property of $F[x]$, we must have $x-\alpha_1 = x-\alpha_i$, for some $i \neq 1$. Thus, $\alpha_1 = \alpha_i$, so

that $f(x)$ has repeated root. Now suppose $f'(x) \neq 0$ and $f(x)$ and $f'(x)$ have a common factor. Then, they have a common irreducible factor $p(x) \in F[x]$. Write $f(x) = p(x)g(x)$. Then $f'(x) = p'(x)g(x) + p(x)g'(x)$. If $p'(x) \neq 0$, then, since $p(x)$ divides $f'(x)$, it divides $p'(x)g(x)$. Therefore, $p(x)$ must divide $g(x)$. We can now write $f(x) = p(x)^2 g_0(x)$, for some $g_0(x) \in F[x]$. Thus, any root of $p(x)$ is a repeated root of $f(x)$. If $p'(x) = 0$, then as we have just seen, $p(x)$ has a repeated root, and therefore $f(x)$ also has a repeated root.

For part (ii), suppose $f'(x) = 0$ and $\alpha \in \overline{F}$ is a root of $f(x)$. Then we can write $f(x) = (x - \alpha)g(x)$ as elements of $\overline{F}[x]$. We then have

$$0 = f'(x) = g(x) + (x - \alpha)g'(x).$$

If we set $x = \alpha$, it follows that $g(\alpha) = 0$, which shows that α is a repeated root of $f(x)$.

9. Let $f(x)$ be an irreducible polynomial with coefficients in $\mathbb{Q}$. Prove that $f(x)$ has distinct roots in its splitting field over $\mathbb{Q}$. Does the same conclusion hold if $f(x)$ is an irreducible polynomial with coefficients in $\mathbb{Z}_p$, $p > 0$, a prime? Prove this, or give a counter-example.

Solution. If $f(x) \in \mathbb{Q}[x]$, then $f'(x) \neq 0$, and moreover, if $f(x)$ is irreducible, then $f(x)$ and $f'(x)$ cannot have a common factor. Thus, by the previous problem, $f(x)$ has distinct roots. Now suppose $f(x) \in \mathbb{Z}_p[x]$ is irreducible. If $f'(x) \neq 0$, then since $f(x)$ is irreducible, $f(x)$ and $f'(x)$ have no common factor, and thus, by the previous problem, $f(x)$ has distinct roots. Suppose $f'(x) = 0$. Then, when we write $f(x) = \sum_{i=0}^{d} a_i x^i$, with $a_i \in \mathbb{Z}_p$, $a_i \neq 0$ if and only if p divides i. So, we can rewrite $f(x)$ as $\sum_{j=0}^{r} a_{pj} x^{pj}$, where $d = pr$. Now, by Euler's theorem, $a_{jp} = a_{jp}^p$, for all j, so that

$$f(x) = \sum_{j=0}^{r} a_{pj} x^{pj} = \sum_{j=0}^{r} a_{pj}^p x^{pj} = (\sum_{j=0}^{r} a_{pj} x^j)^p,$$

which contradicts the irreducibility of $f(x)$. Therefore, when $F = \mathbb{Z}_p$, we cannot have $f'(x) = 0$, when $f(x)$ is irreducible over F. Thus, $f(x)$ has distinct roots. Consequently, every finite extension of $\mathbb{Z}_p$ is a separable extension.

10. Let F be a field and $F(x)$ the rational function field in one variable over F, i.e., the field consisting of all fractions $f(x)/g(x)$, with $f(x), g(x) \in F[x]$, $g(x) \neq 0$. Let K be a field satisfying $F \subset K \subseteq F(x)$ and assume $K = F(f/g)$, for some $f/g \in F(x) \backslash F$, with $f(x)$ and $g(x)$ relatively prime. Show that $[F(x) : K]$ is the maximum of the degrees of $f(x)$ and $g(x)$. Conclude that $[F(x) : K] < \infty$, for any $F \subset K \subseteq F(x)$.

Solution. Let t be an indeterminate over K (so that x, t are independent variables over F). If $f(x)$ has degree greater than the degree of $g(x)$, set $h(t) := f(t) - (f(x)/g(x))g(t)$, so that $h(t) \in K[t]$ and the degree of $h(t)$ equals the degree of $f(x)$. Since we may assume that $f(x)$ is monic, as replacing $f(x)$ by the polynomial obtained by dividing $f(x)$ by its leading coefficient does not change K, $h(t)$ is a monic polynomial in $K[t]$ whose degree is the maximum of the degrees of $f(x)$ and $g(x)$. Suppose the degree of $g(x)$ is greater than or equal to the degree of $f(x)$. If $f(x)$ and $g(x)$ have the same degree, the division algorithm gives $f(x) = g(x) + r(x)$, where $r(x)$ has degree less than the degree of $g(x)$. But then, $f(x)/g(x) = 1 + r(x)/g(x)$ and $K = F(r(x)/g(x))$, so we may relabel $r(x)$ as $f(x)$ and assume the degree of $g(x)$ is strictly greater than the degree of $f(x)$. In this case we take, $h(t) = g(t) - (g(x)/f(x))f(t)$, and assume that $g(x)$ is monic, so that again, $h(t)$ is a monic polynomial in $K[t]$ whose degree is the maximum of the degrees of $f(x)$ and $g(x)$. Without loss of generality, we assume that we are in the first case. Then, we have that $h(x) = 0$, so that x is algebraic over K. Since $F(x) = K(x)$, this shows that $[F(x) : K] < \infty$. To see that $[F(x) : K]$ equals the maximum of the degrees of $f(x)$ and $g(x)$, namely, the degree of $f(x)$, it suffices to show that $h(t)$ is irreducible as an element of $K[t]$.

Since $f(x)/g(x)$ is not algebraic over F, we can think of $f(x)/g(x)$ as a variable over F, so for ease of notation, we set $u := f(x)/g(x)$. Therefore, $h(t) \in F(u)[t]$, where $F(u)$ is the rational function field in u over F, i.e., the quotient field of the polynomial ring $F[u]$. In this new notation, $h(t) = f(t) - ug(t)$, which also belongs to the polynomial ring $F[u, t]$ in two variables over F. Now, as a polynomial in t, with coefficients in $F[u]$, $h(t)$ is a primitive polynomial, so by Gauss's lemma, it is irreducible as an element of $F(u)[t]$, if it is irreducible as an element of $F[t, u]$. We can also regard $h(t)$ as a polynomial in u with coefficients in $F[t]$. Since $f(t), g(t)$ have no common factor, $h(t)$ is irreducible as as element of $F[t, u]$, since it has degree one as a polynomial in u, which gives what we want.