MOCK QUALIFYING EXAMINATION, ALGEBRA, PART A, 2019

September n^4, 2019

Solve any four questions; indicate which ones are supposed to be graded. You must show all work and justify all statements either by referring to an appropriate theorem or by providing a full solution.

1. For a group G, let G' denote its commutator subgroup.

(a) Prove that G' is normal in G.

(b) Show that for any abelian group A, a homomorphism $G \to A$ must factor through the quotient G/G'.

(c) Let $G^{(1)} = G'$, $G^{(2)} = (G')'$, and in general $G^{(n)} = (G^{(n-1)})'$. Give an example of a group G such that $G^{(n)} \neq \langle e \rangle$ for any $n \in \mathbf{N}$.

(a) Recall that the commutator subgroup G' is *the normal subgroup generated by* elements of the form $aba^{-1}b^{-1}$ for all $a, b \in G$. To prove G' is a normal subgroup, take $x \in G'$, and note that for any $g \in G$, $gxg^{-1} = x\left(x^{-1}gxg^{-1}\right)$ is a product of two commutator elements, so it's in G'.

(b) Without loss of generality, suppose that $\varphi \colon G \twoheadrightarrow A$ is surjective. For any $g, h \in G$ we'll have $0 = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = \varphi(ghg^{-1}h^{-1})$, so the commutator subgroup G' is a subgroup of the kernel of φ. This scenario suggests the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & G' \arrow[r, hook] \arrow[d, hook] & G \arrow[r, two heads] \arrow[d, leftrightarrow, "\mathbf{1}"] & G/G' \arrow[r] & 0 \\
0 \arrow[r] & \operatorname{Ker}\varphi \arrow[r, hook] & G \arrow[r, two heads, "\varphi"'] & A \arrow[r] & 0
\end{tikzcd}$$

Then we need to build the map $G/G' \to A$, but this is just Question 2 on part B of this exam.

(c) The point here is to recognize that if $G^{(n)} = \langle e \rangle$ for some n that that means, by definition, G is solvable. So we just need to know an example of a non-solvable group. Consider A_5, the alternating group on 5 letters. Remember that A_5 is simple, which means its only subgroups are $\langle e \rangle$ and itself. So since we can find a nontrivial commutator element, $(1\,2)(2\,3)(1\,2)^{-1}(2\,3)^{-1} = (1\,3\,2)$, the commutator subgroup must be all of A_5.

2. Classify all groups of order 169.

Notice that $169 = 13^2$. Such a group G of order 169 will be a p group of order p^2. This means that G will have a nontrivial center by the class equation. If the center is all of G, then G is abelian. Otherwise if the center has order p, then G modulo the center will have order p too. This means the quotient is cyclic, which means G is abelian in this case too. So G must be abelian, so there are two options.

$$G \cong \mathbf{Z}_{169} \qquad \text{or} \qquad G \cong \mathbf{Z}_{13} \oplus \mathbf{Z}_{13}\,.$$

3. An integral domain R is integrally closed if for any monic polynomial f over R, every root of f in $\operatorname{Frac}(R)$ is actually in R.

(a) Prove that a unique factorization domain is integrally closed.

(b) Give an example of a ring that is *not* integrally closed.

(a) Take a monic polynomial $x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in R[x]$ with a root $\frac{a}{b} \in \operatorname{Frac}(R)$. So

$$\begin{aligned} & \left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0 \\ \implies \quad & a^n + \left(c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n\right) = 0 \end{aligned}$$

But then b divides $c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n$, and b divides zero, so b must divide a^n. (This is where we're using the fact that R is a UFD: a^n factors uniquely, and that factorization *must* contain b.) But since $\frac{a}{b} \in \operatorname{Frac}(R)$, (the fraction has to be "reduced" by construction), b must be a unit, so $\frac{a}{b} = ab^{-1} \in R$.

(b) The ring $\boldsymbol{k}[x^2, x^3]$ is not integrally closed. Note this ring is *not* a UFD because $x^6 = x^2x^2x^2 = x^3x^3$. Anyways, this is not integrally closed because x is a root of the polynomial $t^2 - x^2 \in \boldsymbol{k}[x^2, x^3][t]$, and x is in the fraction field of $\boldsymbol{k}[x^2, x^3]$ but not in $\boldsymbol{k}[x^2, x^3]$ itself.

4.

(a) Prove that a finite integral domain is a field. Is it true that a finite integral ring (non-commutative) is a division ring?

(b) Does there exist a field such that its additive group structure and its multiplicative group of units are isomorphic?

(c) (Challenge) Prove that every finite division ring is a field.

(a) Fix a finite integral domain $\boldsymbol{k}$, and pick some $a \in \boldsymbol{k}$. Consider the function $\boldsymbol{k} \to \boldsymbol{k}$ where $x \mapsto ax$. This function is injective since $ax = ay \implies x = y$, and so it's surjective since $\boldsymbol{k}$ is finite. In particular, some element has to map to 1. This'll be a^{-1}, so $\boldsymbol{k}$ is a field. And if $\boldsymbol{k}$ weren't commutative, it'd still be a division ring. If you consider the other map $x \mapsto xa$, then you similarly get a left inverse for a. And the left and right inverse must be the same since, if you had left inverse x and right inverse y so that $xa = 1$ and $ay = 1$, you get

$$x \;=\; x1 \;=\; xay \;=\; 1y \;=\; y$$

(b) Nope. If your field $\boldsymbol{k}$ is finite, then $\boldsymbol{k}$ and $\boldsymbol{k}^\times$ have different cardinalities, so there's no way that they're isomorphic. Now if $\boldsymbol{k}$ is infinite, for the sake of contradiction suppose you have a group isomorphism $\psi \colon \boldsymbol{k}^\times \xrightarrow{\sim} \boldsymbol{k}$. Note that -1 has order two in $\boldsymbol{k}^\times$, so in $\boldsymbol{k}$

$$0 \;=\; \psi(1) \;=\; \psi\big((-1)^2\big) \;=\; 2\psi(-1)\,.$$

We can't have both $\psi(1) = 0$ and $\psi(-1) = 0$, so $1 = -1$ and $\operatorname{char} \boldsymbol{k} = 2$. But this means $2x = 0$ for all $x \in \boldsymbol{k}$, which means $\psi(x)^2 = 1$ for all $x \in \boldsymbol{k}$. But

$$\psi(x)^2 = 1 \qquad \implies \qquad (\psi(x) - 1)^2 = 0\,,$$

which only has a single solution $\psi(x) \in \boldsymbol{k}^\times$.

(c) This is Wedderburn's little theorem.

5. For a set X let $\mathcal{P}(X)$ denote the set of a subsets of X. For $A, B \in \mathcal{P}(X)$ define the operations $AB := A \cap B$ and $A + B := (A \cup B) \setminus (A \cap B)$ (the *symmetric difference* of A and B).

(a) Prove that $\mathcal{P}(X)$ is a commutative unital ring under these operations.

(b) What is the characteristic of this ring? Prove that every ring R with the property that $AA = A$ for all $A \in R$ must have this characteristic.

(c) Prove that every finitely generated ideal of $\mathcal{P}(X)$ is principal.

(a) ◀

(b) ◀

(c) ◀

Attempt any four, all questions are worth 10 points.

1. (a) Prove that every quotient of a divisible group is divisible.

(b) Let B be an abelian group. Prove that for any subgroup A of B, a homomorphism A to $\mathbf{Q}/\mathbf{Z}$ must extend to a homomorphism B to $\mathbf{Q}/\mathbf{Z}$.

(a) If an abelian group G is divisible, this means that regarding G as an $\mathbf{Z}$-module, the module homomorphism $\varphi_n \colon G \to G$ given by $g \mapsto ng$ for an integer n is surjective for all $n \in \mathbf{Z}$. Suppose Q is a quotient of G, and let the quotient map be $\pi \colon G \twoheadrightarrow Q$. For an arbitrary $q \in Q$, since π and φ_n are surjective, there will be some $g \in G$ such that $\pi\varphi_n(g) = q$. But then considering the map $\widetilde{\varphi}_n \colon Q \to Q$, we have

$$\widetilde{\varphi}_n \colon \pi(g) \mapsto n\pi(g) = \pi(ng) = \pi\varphi_n(g) = q\,,$$

so $\widetilde{\varphi}_n$ is surjective and Q is divisible.

(b) First note that for any $r \in \mathbf{Q}$ and $n \in \mathbf{Z}$ we have $\frac{r}{n} \mapsto n\frac{r}{n} = r$. So $\mathbf{Q}$ is divisible, and so $\mathbf{Q}/\mathbf{Z}$ is divisible by part (a). Then a divisible abelian group is injective as an $\mathbf{Z}$-module, and you use the universal property to get the map $B \to \mathbf{Q}/\mathbf{Z}$.

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, hook] \arrow[d] & B \arrow[dl, dashed] \\
 & \mathbf{Q}/\mathbf{Z} &
\end{tikzcd}$$

2. For a ring R, consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r, tail, "i_1"] & C \arrow[r, two heads, "\pi_1"] \arrow[d, "h"] & A \arrow[r] & 0 \\
0 \arrow[r] & Y \arrow[r, tail, "i_2"'] & Z \arrow[r, two heads, "\pi_2"'] & X \arrow[r] & 0
\end{tikzcd}$$

in the category of R-modules such that the top and bottom rows are exact.

(a) Suppose that there is a map $g \in \mathrm{Hom}_R(B, Y)$ such that $hi_1 = i_2 g$. Prove that there exists a map $f \in \mathrm{Hom}_R(A, X)$ such that $f\pi_1 = \pi_2 h$.

(b) Now suppose that there exists some map $f \in \mathrm{Hom}_R(A, X)$ such that $f\pi_1 = \pi_2 h$. Does there necessarily exist a map $g \in \mathrm{Hom}_R(B, Y)$ such that $hi_1 = i_2 g$?

(a) Take some $a \in A$. Since π_1 is surjective, there exists some $c \in C$ such that $\pi_1(c) = a$. Let's tentatively define the map $f \colon A \to X$ such that $f(a) = \pi_2 h(c)$. Now we've made a *choice* of c here. To prove our function f is well-defined, we must prove that the value of $f(a)$ doesn't depend on our choice of c in the preimage of a. So suppose we have $c' \in C$ such that $\pi_1(c') = a$. Notice that since c and c' both map to a, $c - c'$ is in the kernel of π_1. Since the top row is exact, there is a unique $b \in B$ such that $i_1(b) = c - c'$. Following b down via g, since $hi_1 = i_2 g$ we get $i_2 g(b) = h(c - c')$. Then since the bottom row is exact, following π_2 we get $0 = \pi_2 i_2 g(b) = \pi_2 h(c - c') = \pi_2 h(c) - \pi_2 h(c')$, which means $\pi_2 h(c) = \pi_2 h(c')$, so our map f is well-defined.

(b) Take $b \in B$, and consider $i_1(b) \in C$. Since the top row is exact and $f\pi_1 = \pi_2 h$, we have $0 = \pi_2 i_1(b)$, and so $\pi_2 h i_1(b) = 0$. So since $hi_1(b)$ is in the kernel of π_2 and since the bottom row is exact, there exists $y \in Y$ such that $i_2(y) = hi_1(b)$, and this y is unique since i_2 is injective. Then we can define $g\colon B \to Y$ where $g(b) = y$. This map is well-defined, and $hi_1 = i_2 g$ by construction.

3. Let V be a finite dimensional vector space over $\mathbf{C}$, and take φ in $\mathrm{End}_{\mathbf{C}}(V)$.

(a) Prove that φ defines a left $\mathbf{C}[x]$-module structure on V where, for $f \in \mathbf{C}[x]$ and $\boldsymbol{v} \in V$, $f(\varphi) \in \mathrm{End}_{\mathbf{C}}(V)$ and $f.\boldsymbol{v} := \big(f(\varphi)\big)(\boldsymbol{v})$.

(b) We say a subspace $W \subset V$ is *φ-invariant* if $\varphi(W) \subset W$. Prove that W is φ-invariant if and only if W is a $\mathbf{C}[x]$-submodule of V under the action inducted by φ. Furthermore prove that $V_\varphi(\boldsymbol{v})$, the smallest φ-invariant subspace of V containing $\boldsymbol{v}$, is the cyclic submodule $\mathbf{C}[x]\boldsymbol{v}$.

(a) To make the notation cleaner, let f_φ denote $f(\varphi)$. To verify that this does give us a $\mathbf{C}[x]$-module structure, we need to verify that for $f, g \in \mathbf{C}[x]$ and $\boldsymbol{v}, \boldsymbol{w} \in V$:

- $(f+g).\boldsymbol{v} = (f+g)_\varphi(\boldsymbol{v}) = f_\varphi(\boldsymbol{v}) + g_\varphi(\boldsymbol{v}) = f.\boldsymbol{v} + g.\boldsymbol{v}$.
- $(fg).\boldsymbol{v} = (fg)_\varphi(\boldsymbol{v}) = (f_\varphi(\boldsymbol{v}))(g_\varphi(\boldsymbol{v})) = (f.\boldsymbol{v})(g.\boldsymbol{v})$.
- $f.(\boldsymbol{v} + \boldsymbol{w}) = f_\varphi(\boldsymbol{v} + \boldsymbol{w}) = f_\varphi(\boldsymbol{v}) + f_\varphi(\boldsymbol{w}) = f.\boldsymbol{v} + f.\boldsymbol{w}$.

(b) If W is a $\mathbf{C}[x]$-submodule of V under the action induced by φ, then for any $\boldsymbol{w} \in W$ we can take the polynomial $x \in \mathbf{C}[x]$ and see that $x.\boldsymbol{w} = x_\varphi(\boldsymbol{w}) = \varphi(\boldsymbol{w})$ must be in W.

Conversely, if $\varphi(\boldsymbol{w}) \in W$ for all $\boldsymbol{w} \in W$, then inductively $\varphi^n(\boldsymbol{w}) \in W$ for any positive integer n. Furthermore since W is a vector subspace of V, then it is closed under addition and scalar multiplication by elements of $\mathbf{C}$. This means that for any polynomial $z_n x^n + \cdots + z_1 x + z_0 \in \mathbf{C}[x]$, the vector $z_n \varphi^n(\boldsymbol{w}) + \cdots + z_1 \varphi(\boldsymbol{w}) + z_0 \boldsymbol{w} \in W$, so W is closed under the action of $\mathbf{C}[x]$ and will be a $\mathbf{C}[x]$-submodule of V.

4. Consider the matrices

$$M = \begin{pmatrix} 0 & 0 & 0 & 5 \\ 0 & 0 & 2 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \qquad N = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 5 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

(a) What are the invariant factor and elementary divisor decompositions of the $\mathbf{Q}[x]$-module corresponding to M? What are these decompositions if you consider the corresponding $\mathbf{C}[x]$-module instead? What about the decomposition as a $\boldsymbol{F}_5[x]$-module where $\boldsymbol{F}_5$ is the field with five elements?

(b) What is the Jordan canonical form of M considered as a matrix over $\mathbf{C}$? What is the Jordan canonical form over $\overline{\boldsymbol{F}_5}$, the algebraic closure of $\boldsymbol{F}_5$?

(c) Determine, with proof, whether or not the matrices M and N are equivalent over $\mathbf{C}$. Are M and N similar over $\mathbf{C}$? Are M and N similar over $\boldsymbol{F}_5$?

(a) Calculating the characteristic polynomial of M,

$$\det\begin{pmatrix}-\lambda & 0 & 0 & 5\\ 0 & -\lambda & 2 & 0\\ 0 & 2 & -\lambda & 0\\ 1 & 0 & 0 & -\lambda\end{pmatrix} = -\lambda\big(-\lambda(\lambda^2-4)\big) - 1\big(5(\lambda^2-4)\big) = (\lambda^2-5)(\lambda^2-4)$$

$$= (\lambda^2-5)(\lambda+2)(\lambda-2)$$

Since these irreducible factors of the characteristic polynomial are distinct, M will have just a single invariant factor over $\mathbf{Q}$, $f = (\lambda^2-5)(\lambda+2)(\lambda-2)$, and M will have three elementary divisors (λ^2-5), $(\lambda+2)$, and $(\lambda-2)$. This corresponds to the decomposition as a $\mathbf{Q}[x]$-module

$$\mathbf{Q}^4 \cong \mathbf{Q}[x]/(f) \cong \mathbf{Q}[x]/(x^2-5) \oplus \mathbf{Q}[x]/(x+2) \oplus \mathbf{Q}[x]/(x-2)\ .$$

As a $\mathbf{C}[x]$-module, that (x^2-5) elementary divisor will factor as $\left(x+\sqrt{5}\right)\left(x-\sqrt{5}\right)$, but these factors are distinct, so you still have a single invariant factor f, but now you have four elementary divisors

$$\mathbf{C}^4 \cong \mathbf{C}[x]/(x+\sqrt{5}) \oplus \mathbf{C}[x]/(x-\sqrt{5}) \oplus \mathbf{C}[x]/(x+2) \oplus \mathbf{C}[x]/(x-2)\ .$$

Now over $\boldsymbol{F}_5$, $5=0$, and our characteristic polynomial is now $x^2(x+2)(x-2)$. Now we have duplicate factors and we have to ask, is x and elementary divisor twice, or is the elementary divisor x^2? Ie. does x^2 divide the minimal polynomial? (remember the minimal polynomial is the highest invariant factor) To figure this out, we can manually compute the minimal polynomial of M over $\boldsymbol{F}_5$ to see if it's $x^2(x+2)(x-2)$ or $x(x+2)(x-2)$. Doing so, we find that $x^2(x+2)(x-2)$ is the minimal polynomial. So we still have a single invariant factor, but now there are three elementary divisors.

$$\boldsymbol{F}_5^4 \cong \boldsymbol{F}_5[x]/(x)^2 \oplus \boldsymbol{F}_5[x]/(x+2) \oplus \boldsymbol{F}_5[x]/(x-2)\ .$$

(b) Looking at its $\mathbf{C}[x]$-module decomposition, the Jordan canonical form of M over $\mathbf{C}$ will be

$$M \sim \begin{pmatrix}\sqrt{5} & 0 & 0 & 0\\ 0 & -\sqrt{5} & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & -2\end{pmatrix}.$$

Next looking at $\boldsymbol{F}_5[x]$-module decomposition of M, luckily the characteristic polynomial factored completely over $\boldsymbol{F}_5[x]$, and we can see that the Jordan canonical form will be

$$M \sim \begin{pmatrix}0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & -2\end{pmatrix}.$$

(c) Note that for an educated choice of invertible P and Q we have

$$PMQ = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 5 \\ 0 & 0 & 2 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 5 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = N\,,$$

so yes, M and N are equivalent over $\mathbf{C}$. They are certainly not similar though. Doing a brisk computation we see that the characteristic polynomial of N is $(x^2-2)(x^2-10)$; similar matrices must have the same characteristic polynomial. And M and N are similarly not similar over $\boldsymbol{F}_5$, having characteristic polynomials $x^2(x^2+1)$ and $x^2(x^2+3)$ respectively.

6. Recall that a functor is exact if it takes short exact sequences to short exact sequences.

(a) Prove that if F is a finite dimensional free R-module, then $-\otimes_R F$ is an exact functor.

(b) Prove that if P is a finitely generated projective R-module, then $-\otimes_R P$ is an exact functor.

(c) (Challenge) Prove that if R is a ring $\mathcal{P}(X)$ like in Question 5, Part A of this exam, then the functor $-\otimes_R M$ is exact for *any* R-module M.

(a) ◄

(b) ◄

(c) ◄

Mock Algebra Qualifier 2019 - Part C

Do 4 out of the 5 problems.

(1) Let F/k be a normal extension of fields and let K_0 be the maximal separable subextension of k. Show that K_0/k is normal.

Solution by Derek Lowenberg:

To show the extension K_0/k is normal, consider a polynomial $f(x) \in k[x]$ which is irreducible over k and suppose that it has a root $a \in K_0$ but that it does not split into linear factors in K_0. Since K/k is normal, there is some $b \in K$ that is a root of $f(x)$ where $b \notin K_0$ hence b is inseparable. That is, the minimal polynomial $g(x) \in k[x]$ of b has a multiple root. Now $g(x)$ divides $f(x)$, which contradicts the irreducibility of $f(x)$ unless $f(x) = ug(x)$ for some $u \in k$, hence $f(x)$ also has a multiple root. Let $h(x) \in k[x]$ be the minimal polynomial of $a \in K_0$. Then $h(x)$ is separable, that is, has no multiple roots. However, since $f(x)$ is irreducible and $h(x)$ divides it, we conclude that $f(x) = vh(x)$ for some $v \in k$ and hence $f(x)$ also has no multiple roots. Thus we arrive at a contradiction, showing that no such $f(x)$ exists. That is, every polynomial irreducible over k either has no roots in K_0 or it has all its roots in K_0.

(2) Let F be a field and $p(x) \in F[x]$ an irreducible polynomial.
   (a) Prove that there exists a field extension K of F in which $p(x)$ has a root.
   (b) Determine the dimension of K as a vector space over F and exhibit a vector space basis for K.
   (c) If $\theta \in K$ denotes a root of $p(x)$, express θ^{-1} in terms of the basis found in part (b).
   (d) Suppose $p(x) = x^3 + 9x + 6$. Show $p(x)$ is irreducible over $\mathbf{Q}$. If θ is a root of $p(x)$, compute the inverse of $(1 + \theta) \in \mathbf{Q}(\theta)$.

If $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is irreducible, then $K = F[x]/(p)$ will contain a root of p. Namely, that root of p will be the image of x under the quotient map $F[x] \to F[x]/(p)$.

Now what $K = F[x]/(p)$ a polynomial ring with a relation slapped on it. Initially $F[x]$ has basis $\{1, x, x^2, \ldots, x^n, \ldots\}$ as an infinite dimensional vector space over F. But when you mod out by p you are declaring that $x^n = -a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$. Ie, that any polynomial with terms of degree n or higher can be rewritten in $F[x]/(p)$ with terms of degree less than n. So a possible basis of $F[x]/(p)$ as a F vector space is $\{1, x, \ldots, x^{n-1}\}$.

Now if θ is a root of p we have $p(\theta) = \theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_0 = 0$. We can rearrange this equation to get an inverse for θ:

$$\begin{aligned} & \theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_0 = 0 \\ \implies \quad & \theta\big(\theta^{n-1} + a_{n-1}\theta^{n-2} + \cdots + a_1\big) = -a_0 \\ \implies \quad & \theta\left(-\frac{1}{a_0}\theta^{n-1} - \frac{a_{n-1}}{a_0}\theta^{n-2} + \cdots - \frac{a_1}{a_0}\right) = 1 \end{aligned}$$

If we specify $p(x) = x^3 + 9x + 6$ over $\mathbf{Q}$, we can see that p is irreducible by the Schönemann–Eisenstein theorem considering the prime 3. Finding an inverse for $(1+\theta)$ in K is a bit cumbersome, but do-able. Since $\{1, x, x^2\}$ will be a basis for K over F, the inverse $(1+\theta)$ must look like $(a\theta^2 + b\theta + c)$ for some $a, b, c \in \mathbf{Q}$ (remember that x IS θ). Writing out $(1+\theta)(a\theta^2 + b\theta + c) = 1$, multiplying those two polynomials together, and remembering that $\theta^3 = -9\theta - 6$, we arrive at a system of equations

$$\begin{cases} -6b + c = 1 \\ -9a + b + c = 0 \\ a + b = 0 \end{cases}$$

which we may solve to find $a = -b = \frac{1}{4}$, and $c = \frac{5}{2}$. So our inverse to $(1+\theta)$ is $\frac{1}{4}\theta^2 - \frac{1}{4}\theta + \frac{5}{2}$.

(3) Let $f = x^5 - 45x^3 + 35x^2 + 15$ and $g = x^{11} - 11$, both considered as polynomials in $\mathbf{Q}[x]$. Suppose $\alpha \in \mathbf{C}$ is a root of f. Prove or disprove: $\mathbf{Q}(\alpha)$ contains a root of g.

◀

(4) Given a tower of fields $F \to E \to K$, prove or disprove by providing a counterexample:
 (a) If K is normal over F, then K is normal over E.
 (b) If K is normal over E and E is normal over F, then K is normal over F.

(c) If K is separable over F, then K is separable over E and E is separable over F.

(a) ◀

(b) ◀

(c) ◀

(5) Let p be a prime number and $K = \boldsymbol{F}_{p^6}$ be a field with p^6 elements.

(a) Given an element of K, what are the possible degrees of it's minimal polynomial over $\boldsymbol{F}_p$?

(b) For each possible degree, how many elements in K have a minimal polynomial with that degree?

(a) ◀

(b) ◀