Introduction. This document provides complete solutions to some problems in Algebra prelims in the Mathematics department at the University of Minnesota. The solutions are meant to be as explanatory as possible. All proofs of results that can be assumed to be true in the context of the prelims can be found in either of [1],[3],[2]. A brief commentary of the problem precedes the solution (analogue to commentary previous to a soccer match!). Many of the solutions are not checked for accuracy by anyone other than the author.

1. Describe all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_9)$, where $\zeta_9$ is a primitive ninth root of unity.

Commentary. This is a standard Galois extension problem, with the twist that it may be difficult to compute explicitly a primitive ninth root of unity in terms of rational powers of elements in $\mathbb{Q}$. Recall that

$$\zeta_9 = e^{\pi i/9} = \cos(\pi/9) + \sin(\pi/9)i,$$

and in the test environment it may be difficult to come up with the correct formula for the cosine or sine of 40 degrees, so that it may be difficult to come up with the correct explicit (as elements in $\mathbb{C}$) generators of the intermediate fields. But, as will be seen in the solution below, it is not necessary that one explicitly characterizes the intermediate fields in that way. This also makes sense: We shouldn’t need to know anything about $\mathbb{C}$ to solve the problem as stated.

We quickly show that $\mathbb{Q}(\zeta_9)$ must be a degree 6 Galois extension, but this does not immediately determine the Galois group since there are two isomorphism classes of Galois groups of order 6, namely, $\mathbb{Z}/6$ and $S_3$. The idea then is to manufacture two distinct intermediate fields which are Galois over $\mathbb{Q}$. By the Sylow Theorem we know
there will be exactly one field extension of degree 2 over \( \mathbb{Q} \), but a priori there may be several field extensions of degree 3 over \( \mathbb{Q} \). But, the field extension of degree 3 over \( \mathbb{Q} \) that we will produce will be Galois, and this fact will allow us to immediately determine the Galois group, and thus finally finish the field diagram.

**Solution.** Primitive ninth roots of unity are exactly all the roots of the ninth cyclotomic polynomial. This polynomial is obtained by "dividing out" all other ninth roots of unity from the polynomial \( x^9 - 1 \). Since

\[
x^9 - 1 = (x^3)^3 - 1 = (x^3 - 1)(x^6 + x^3 + 1),
\]

it follows the ninth cyclotomic polynomial is

\[
p(x) := x^6 + x^3 + 1.
\]

This polynomial is irreducible over \( \mathbb{Q} \) (we can take as a known fact that all the cyclotomic polynomials are irreducible, this fact has no quick proof by the way). Moreover, \( \zeta_9 \) will generate all other roots of \( p(x) \) (which are, for completeness, \( \zeta_9^2, \zeta_9^4, \zeta_9^5, \zeta_9^7, \zeta_9^8 \)). It follows that \( \mathbb{Q}(\zeta_9) \) splits \( p(x) \). On the other hand, a splitting field of \( p(x) \) must contain \( \zeta_9 \) since \( \zeta_9 \) is a root of \( p(x) \). Thus, \( \mathbb{Q}(\zeta_9) \) is the splitting field for the separable (since irreducible over the perfect field \( \mathbb{Q} \)) polynomial \( p(x) \), so that

\[
\mathbb{Q}(\zeta_9) \cong \mathbb{Q}[x]/(x^6 + x^3 + 1),
\]

and \( \mathbb{Q}(\zeta_9) \) is a Galois extension over \( \mathbb{Q} \). Since \( \deg p(x) = 6 \), we have

\[
[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6,
\]

so that we also have

\[
|\text{Gal } (\mathbb{Q}(\zeta_9)/\mathbb{Q})| = 6.
\]

Denote \( G := \text{Gal } (\mathbb{Q}(\zeta_9)/\mathbb{Q}) \).

From (1) we see that third roots of unity lie in \( \mathbb{Q}(\zeta_9) \) (or verify this directly too). Let \( \beta \) be a third root of unity. Then

\[
\mathbb{Q}(\beta) \cong \mathbb{Q}[x]/(x^2 + x + 1),
\]

which implies \( \mathbb{Q}(\beta) \) is a Galois extension over \( \mathbb{Q} \) of degree 2 (recall \( x^2 + x + 1 \) is the third cyclotomic polynomial), and clearly \( \mathbb{Q}(\beta) \) is a subfield of \( \mathbb{Q}(\zeta_9) \), with

\[
[\mathbb{Q}(\zeta_9) : \mathbb{Q}(\beta)] = 3.
\]

Thus there corresponds a normal subgroup of order 3 in \( G \). If we want a more explicit characterization of \( \mathbb{Q}(\beta) \), note that we can take

\[
\beta = e^{\pi i/3} = \cos(\pi/3) + \sin(\pi/3)i,
\]
and from this observation we see that \( \beta \in \mathbb{Q}(i\sqrt{3}) \). Since
\[
\mathbb{Q}(i\sqrt{3}) \cong \mathbb{Q}[x]/(x^2 + 3),
\]
then \([\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2\), and this proves \(\mathbb{Q}(\beta) \cong \mathbb{Q}(i\sqrt{3})\). We emphasize that this explicit characterization is not necessary to solve the problem.

Next, since \(\zeta_9^9 = 1\), we have \(\zeta_9^6 = \zeta_9^{-3}\), so
\[
0 = p(\zeta_9^0) = \zeta_9^6 + \zeta_9^3 + 1 = (\zeta_9 + \zeta_9^{-1})^3 - 3(\zeta_9 + \zeta_9^{-1}) + 1. \tag{2}
\]

The above calculation shows that \(\mathbb{Q}(\zeta_9)\) splits the polynomial
\[
q(x) := x^3 - 3x + 1.
\]
Moreover, \(q(x)\) is irreducible over \(\mathbb{Q}\). This is gleaned as follows: if it were reducible, it must have a linear factor, hence a root in \(\mathbb{Q}\). But since \(q(x)\) is a polynomial with integer coefficients, its roots in \(\mathbb{Q}\) actually lie in \(\mathbb{Z}\), and furthermore, by the Rational Roots Theorem, any root of \(q(x)\) would need to divide 1. But through straightforward computation it is seen that neither 1 or \(-1\) are roots of \(q(x)\). Hence \(q(x)\) has no roots in \(\mathbb{Q}\), and so it is irreducible.

By (2), we see that \(\zeta_9 + \zeta_9^{-1}\) is a root of the irreducible polynomial \(q(x)\). It follows that
\[
\mathbb{Q}(\zeta_9 + \zeta_9^{-1}) \cong \mathbb{Q}[x]/(x^3 - 3x + 1),
\]
the field extension \(\mathbb{Q}(\zeta_9 + \zeta_9^{-1})\) is Galois over \(\mathbb{Q}\), and
\[
[\mathbb{Q}(\zeta_9) : \mathbb{Q}(\zeta_9 + \zeta_9^{-1})] = 2.
\]
Since 2, 3 are relatively prime, there is no danger that \(\mathbb{Q}(\zeta_9 + \zeta_9^{-1})\) is contained (or contains) \(\mathbb{Q}(\beta)\). All of this implies there is a normal subgroup of order 2 in \(G\). Thus there are two normal subgroups of \(G\) of order 2 and 3 respectively which intersect at the identity; it follows that \(G\) is isomorphic to the direct product of these two subgroups, so
\[
G \cong \mathbb{Z}/2 \times \mathbb{Z}/3.
\]
By the Sylow theorems, the normality of the subgroups of order 2, 3 in \(G\) implies that there can be no more proper subgroups of \(G\) other than these two and the identity subgroup. Hence the field diagram is complete. \(\square\)

2. Show that every rational number is expressible as a sum of fractions \(\frac{c}{p^n}\) with denominators which are prime powers (and \(c \in \mathbb{Z}\)).
Commentary. A possible solution method is to use induction, and just work out the calculation. However, the following solution is in our opinion much more elegant. The Chinese Remainder Theorem is begging for attention here, and we will give it its due. Specifically, (3) gives us what we want: it intuitively says that remainders modulo an integer are in 1-1 correspondence with remainders modulo the prime power factors of said integer. Then, the magical trick of multiplication by 1 yields us the result very quickly.

Solution. Fix $b \in \mathbb{Z} \setminus \{0, 1\}$. It is enough to show the desired result for arbitrary $a/b$ where $a \in \mathbb{Z}/(b)$ and $b > 0$, since all other rational numbers can be written as sums of integers with fractions of the aforementioned manner, and integers have a trivial denominator of $1 = p^0$ for any prime $p$. Thus, factor $b$ into its prime powers: there exist a list $(p_1, \ldots, p_n)$ of distinct primes and a list $(\ell_1, \ldots, \ell_n)$ of positive integers such that

$$b = \prod_{i=1}^{n} p_i^{\ell_i}.$$  

For $i \neq j$, it is clear that $(p_i, p_j) = 1$, and so for all $i \neq j$, the ideals $(p_i^{\ell_i}), (p_j^{\ell_j})$ are comaximal in $\mathbb{Z}$. Therefore the Chinese Remainder Theorem gives

$$\mathbb{Z}/(b) = \mathbb{Z}/\left(\prod_{i=1}^{n} p_i^{\ell_i}\right) \cong \mathbb{Z}/(p_1^{\ell_1}) \times \cdots \times \mathbb{Z}/(p_n^{\ell_n}) =: L. \tag{3}$$

This is basically what we want. More precisely, the map $\phi : L \to \mathbb{Z}/(b)$ given by

$$\phi(c_1, \ldots, c_n) = \sum_{i=1}^{n} c_i \prod_{j \neq i} p_j^{\ell_j}$$

is a ring isomorphism: It is easy to see that it is a ring homomorphism and that it is well-defined. Moreover, its kernel is trivial, for if $\phi(c_1, \ldots, c_n) = 0$ then

$$\sum_{i=1}^{n} c_i \prod_{j \neq i} p_j^{\ell_j} \in (b).$$

For each $k = 1, \ldots, n$, multiply the above element by $\prod_{j \neq k} p_j^{\ell_j}$. This implies that

$$c_k \prod_{j \neq k} p_j^{2\ell_j} \in (b)$$

but this can only occur if $c_k \in (p_k)$, so that for each $k$, $c_k = 0$. So $\phi$ is indeed a ring isomorphism.
Consider the sets
\[ A := \left\{ \sum_{i=1}^{n} \frac{c_i}{p_i^{\ell_i}} \mid c_i \in \mathbb{Z}/(p_i^{\ell_i}) \right\}, \]
\[ S := \left\{ \frac{c}{b} \mid c \in \mathbb{Z}/(b) \right\}. \]

Actually, we can write
\[ A = \left\{ \frac{1}{b} \sum_{i=1}^{n} c_i \prod_{j \neq i} p_j^{\ell_j} \mid c_i \in \mathbb{Z}/(p_i^{\ell_i}) \right\}, \]
by simply multiplying and dividing through by \( \prod_{j \neq i} p_j^{\ell_j} \) on each term in the summand. Then,
\[ A = \left\{ \frac{1}{b} \phi(c_1, \ldots, c_n) \mid c_i \in \mathbb{Z}/(p_i^{\ell_i}) \right\}, \]
so that \( A \subset S \) and \(|A| = |L|\). But by (3), \(|S| = |L|\) too, which implies \( A = S \). This is exactly the desired result. □

3. Let \( G \) be the group of invertible 2 by 2 matrices over the field \( \mathbb{F}_7 \) of 7 elements. Find a 3–Sylow subgroup of \( G \).

Commentary. We will quickly note that a 3–Sylow subgroup must have order 9. Unfortunately there are no elements in \( \mathbb{F}_7 \) that have order 9. But, if we can find two subgroups \( H_1 \) and \( H_2 \) of order 3 in \( G \) such that at least one of them is normal in \( G \), then we win. Playing around for a little time should yield the desired subgroups.

Solution. First recall the formula
\[ |GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}), \]
from which we compute that 9 is the highest power of 3 dividing \(|G|\). So it suffices to find a group of order 9. We realize \( 2 \in \mathbb{F}_7 \) has order 3, so that the matrix \( 2I \) (\( I \) the identity matrix in \( G \)) has order 3, and so \( \langle 2I \rangle \) is a cyclic subgroup of order 3. Also note that the matrix
\[ A := \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} \]
has order 3, so \( \langle A \rangle \) is a subgroup of order 3. We note \( \langle 2I \rangle \cap \langle A \rangle = I \), and that \( \langle 2I \rangle \) is a normal subgroup. This is clear: if \( g \in G \), then
\[ g(2I)g^{-1} = 2gIg^{-1} = 2gg^{-1} = 2I. \]
This calculation shows that in fact $\langle 2I \rangle$ is a subgroup of the center of $G$. In any case, it follows that the semi-direct product $(2I) \rtimes \langle A \rangle$ is well-defined (here we take the automorphism $\phi : \langle A \rangle \to \text{Aut}(\langle 2I \rangle)$ induced by the $G$–multiplication; that is, $\phi$ maps $a \in \langle A \rangle$ to the automorphism of left conjugation by $a$ on $\langle 2I \rangle$), has order $3 \cdot 3 = 9$, and

$$\langle 2I, A \rangle = \langle 2I \rangle \langle A \rangle \cong \langle 2I \rangle \rtimes \langle A \rangle.$$ 

So $\langle 2I, A \rangle$ is a $3$–Sylow subgroup. A straightforward alternative to the argument in the last paragraph is to just write out $\langle 2I, A \rangle$ and verify that indeed it has order 9.  

4. Count the conjugacy classes in the group $GL_2(\mathbb{F}_4)$ of multiplicatively invertible 2 by 2 matrices over the field of 4 elements.

**Commentary.** The Fundamental Structure Theorem of Finitely Generated Modules over a Principal Ideal Domain. That is what it boils down to, really. In practice, though, we know about rational canonical forms, and that is all that is needed. A good source here is Chapter 3 Section 10 of [3]. Make sure to read the remark following the solution too.

**Solution.** For a matrix $A \in G := GL_2(\mathbb{F}_4)$, the conjugacy class that $A$ resides in is the set

$$\{XAX^{-1} \mid X \in G\} \subset G,$$

and we do remark that one of the representatives of the conjugacy class of $A$ is the rational canonical form of $A$ (recall the fact that a matrix is similar to its rational canonical form, and similarity is exactly the condition of being in the same conjugacy class). Since $A$ was arbitrary in $G$, it follows that the number of conjugacy classes in $G$ is exactly the number of different invertible rational canonical forms possible in $G$.

Recall that rational canonical forms are simply the gluing together of different companion matrices for the monic polynomials which are invariant factors (in the sense of the Smith normal form) for some matrix $xI - A$, $A \in G$. The invertible matrices of $M_2(\mathbb{F}_4)$ are exactly those matrices whose determinants are not 0. Therefore, all the invertible rational canonical forms in $G$ are exactly

$$\begin{pmatrix} 0 & -a \\ 1 & -b \end{pmatrix}, a \in \mathbb{F}_4^\times, b \in \mathbb{F}_4, \quad \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}, c \in \mathbb{F}_4^\times.$$ 

Counting these, it is clear we have $3 \times 4 + 3 = 15$ conjugacy classes in $G$.  

**Remark.** The Fundamental Structure Theorem of Finitely Generated Modules over a Principal Ideal Domain is implicitly used in our solution above the moment we invoke
rational canonical forms. Since rational canonical forms arise as the matrix representations of linear transformations on a basis for the vector space which is explicitly given by the invariant factor decomposition of the vector space seen as an $F[x]$-module ($F$ the underlying field), what has been done in our solution is actually the *exact same thing* as counting the possible invariant factor decompositions of $F_4[x]$ modulo monic quadratic (since the dimension of our space is 2) polynomials over $F_4$ *that yield invertible transformations*. All module isomorphism classes for $V$ (the two-dimensional vector space over $F_4$) are

$$F_4[x]/(x^2 + ax + b), \quad F_4[x]/(x - c) \oplus F_4[x]/(x - c), a, b, c \in F_4,$$

but these isomorphism classes include ones whose corresponding linear operator is *not* invertible. Namely, this will be the case if and only if $b = 0$ or $c = 0$. This can be seen by resorting to companion matrices, or a few other ultimately equivalent ways.

**References**

