9. Which finite simple unital rings R have the property that $Th(R)$ has quantifier elimination?

Proposition: For a finite simple unital ring, R, $Th(R)$ has quantifier elimination if and only if $R \cong M_n(\mathbb{F}_{p^k})$ for p prime with $n = 1$ or ($n = 2$ and $k = 1$).

Claim 1: If R is a finite simple unital ring then $R \cong M_n(\mathbb{F}_q)$ for some natural number n and some prime power q.

Proof: By the Artin-Wedderburn Theorem a semisimple ring, R, is isomorphic to a product of $n_i \times n_i$ matrix rings over a division ring, D for $1 \leq i \leq m$ for some $n_1, \ldots, n_m, m \in \mathbb{N}$. Hence if R is simple, R is isomorphic to a single $n \times n$ matrix ring over a division ring. Since R is finite the division ring, D, is necessarily a finite division ring. Since D is a division ring, D is a domain (i.e. D has no zero divisors). By Wedderburn's Little Theorem, every finite domain is a field. Therefore D is a finite field, and so $D = \mathbb{F}_q$ for some prime power q and so R is an $n \times n$ matrix ring over $\mathbb{F}_q$ for some natural number R and some prime power q.

Claim 2: The theory of a finite field has elimination of quantifiers.

Proof: Let $q = p^k$ for some prime p and some positive integer k. Suppose that K and L are isomorphic unital subrings of $\mathbb{F}_q$, the field with q elements, with isomorphism α. Then $|K| = |L| = p^m$ for some $0 < m \leq k$. For any $a \in K \setminus \{0\}$, $a^{p^m-1} = 1$ and so K is closed under inverses. Hence K is a subfield of $\mathbb{F}_q$, and so too is L. Since $|K| = |L|$, $K = L = \{a \in \mathbb{F}_q | a^{p^m} = a\}$. Hence α is a power of the Frobenius map, $x \mapsto x^p$ since the Frobenius map is a generator for the automorphism group on a finite field. So $\alpha : K \to K$, $x \mapsto x^{p^s}$ for some s. This map extends to a map $\widehat{\alpha} : \mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto x^{p^s}$ which is an isomorphism of $\mathbb{F}_q$. Hence for any prime power, q, $\mathbb{F}_q$ is ultrahomogeneous and so by problem 4 on this assignment, $\mathbb{F}_{\text{ıı}}$ has elimination of quantifiers.

Claim 3: For $n \geq 3$, $R := M_n(\mathbb{F}_q)$, $Th(R)$ does not have elimination of quantifiers for any prime power, q.

Proof: Let e_i be the matrix in $R := M_n(\mathbb{F}_q)$ with a 1 in the (i,i)-position and zeros elsewhere for $1 \leq i \leq n$. Consider the unital subrings S and T of R where $S = \{ae_1 + b(1 - e_1) | a, b \in \mathbb{F}_q\}$ and $S = \{a(e_1 + e_2) + b(1 - e_1 - e_2) | a, b \in \mathbb{F}_q\}$. Then S and T are isomorphic via the isomorphism $f : S \to T$. $ae_1 + b(1 - e_1) \mapsto a(e_1 + e_2) + b(1 - e_1 - e_2)$ for $a, b \in \mathbb{F}_q$. Suppose that R has quantifier elimination. Then by problem 4 in this assignment, R is ultrahomogeneous and so f extends to an automorphism, $\widehat{f}$, of R. By the Skolem-Noether Theorem, since R is a finite simple unital ring, every automorphism of R is inner (i.e. given by conjugation). Hence there exists a unit $c \in R$ such that $\widehat{f}(x) = c^{-1}xc$ for all $x \in R$. In particular, since $\widehat{f}$ extends f, $\widehat{f}(e_1) = f(e_1) = e_1 + e_2 = c^{-1}e_1c$. However, there is no such $c \in R$ so that $c^{-1}e_1c = e_1 + e_2$ since the rank of $c^{-1}e_1c$ equals the rank of e_1, which is 1 while the rank of $e_1 + e_2$ is 2. Hence f does not extend to an automorphism of R and so R is not ultrahomogeneous. So by problem 4, $Th(R)$ does not have elimination of quantifiers.

Claim 4: If $q = p^k$ for some prime p and some $k > 1$ then for $R := M_2(\mathbb{F}_q)$, $Th(R)$ does not have quantifier elimination.

Proof: Consider $f : \mathbb{F}_q \to R$, $x \mapsto \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$ and $g : \mathbb{F}_q \to R$, $x \mapsto \begin{bmatrix} x & 0 \\ 0 & \alpha(x) \end{bmatrix}$ where $\alpha : \mathbb{F}_q \to \mathbb{F}_q$ is the Frobenius map, $x \mapsto x^p$.

Since f and g are both clearly injective unital ring homomorphisms, for $S = im(f)$ and $T = im(g)$, we have that $S \cong T$ via isomorphism $h := g \circ f^{-1}$. Suppose there exists an automorphism, $\widehat{h} : R \to R$ extending h. Then as above, by the Skolem-Noether Theorem, there exists a unit $c \in R$ such that $\widehat{h}(z) = c^{-1}zc$ for all $z \in R$. Since $\widehat{h}$ extends h, we have that $c^{-1}f(x)c = g(x)$ for every $x \in \mathbb{F}_q$. However, since $f(x)$ is a diagonal matrix for each x, $f(x)$ commutes with c for each x and so $c^{-1}f(x)c = f(x) = g(x)$. In particular, this implies that $\alpha(x) = x^p = x$ for all $x \in \mathbb{F}_q$. However, since $\mathbb{F}_q$ is a field of order $q = p^k$ for $k > 1$, there exists $y \in \mathbb{F}_q$ such that $y^p \neq y$. Therefore h is an isomorphism of unital subrings of R that does not extend to an automorphism of R, and so R is not ultrahomogeneous. By problem 4, $Th(R)$ does not have quantifier elimination.

Claim 5: If p is prime then for $R := M_2(\mathbb{F}_p)$, $Th(R)$ has quantifier elimination.

Proof: Let S and T be isomorphic unital subrings of R via isomorphism f. Then S and T are vector spaces over the field of prime order $\mathbb{F}_p$.

Case $\dim_{\mathbb{F}_p} S = 1$: In this case f is the identity and $S = T$ since f maps 1 to 1. So clearly f extends to an automorphism of R.

Case $\dim_{\mathbb{F}_p} S = 2$: Since S is unital, S is the $\mathbb{F}_p$-span of the identity matrix, I, and another matrix, A. Since $f : S \to T$ is an isomorphism, T is the span of I and $B := f(A)$. Now A and B satisfy the same minimal polynomial as follows. Since f maps the identity to itself and since $\mathbb{F}_p$ is a prime field, f maps αI to itself for each $\alpha \in \mathbb{F}_p$. This makes f an $\mathbb{F}_p$-algebra homomorphism. Hence $f(\sum_{i=0}^{k} \alpha_i A^i) = \sum_{i=0}^{k} \alpha_i (f(A))^i = \sum_{i=0}^{k} \alpha_i B^i$ and so f preserves minimal polynomials. Note that if $\mathbb{F}_q$ is not a prime field then f need not be an $\mathbb{F}_q$-algebra homomorphism and so f may not preserve minimal polynomials. Since A and B are 2×2 matrices with the same minimal polynomial, they must have the same Jordan form. Therefore A and B are conjugate and f is an isomorphism given by conjugation, which extends to an automorphism of R.

Case $\dim_{\mathbb{F}_p} S = 3$: Let S act on $V = \mathbb{F}_p^2$, the $\mathbb{F}_p$ vector space of 2×1 column vectors, in the usual way. Since R acts faithfully on V and $S \leq R$, S acts faithfully on V. This makes V an S-module. Assume for a contradiction that V is a simple S-module. By the Wedderburn-Artin Theorem, since S is an Artinian ring with semi-simple module, V, S is simple. However, this cannot happen as follows. S is a simple ring with an isomorphic copy of $\mathbb{F}_p$ in its center. Therefore S is isomorphic to a matrix ring over a field extension of $\mathbb{F}_p$. Since $\dim_{\mathbb{F}_p}(S) = 3$, this field extension cannot be dimension 2 over $\mathbb{F}_p$ otherwise S has even dimension. Clearly this extension cannot be dimension larger than 3 over $\mathbb{F}_p$. Hence S is isomorphic to $\mathbb{F}_{p^3}$. However, $\mathbb{F}_{p^3}$ is not a subring of $R = M_2(\mathbb{F}_p)$ since every element of R satisfies a degree 2 polynomial over $\mathbb{F}_p$ while there are elements of $\mathbb{F}_{p^3}$ which satisfy a degree 3 polynomial and no degree 2 polynomial over $\mathbb{F}_p$. Therefore S is not simple and so V is not a simple S-module.

Since V is not simple and $\dim_{\mathbb{F}_p}(V) = 2$, V must have a submodule, U, with $\dim_{\mathbb{F}_p}(U) = 1$. Let $0 \neq x \in U$. Let $\{x, y\}$ be a basis for V for some y. Then elements of S map x to a multiple of x and so with respect to this basis, elements of S are upper triangular. Since S has dimension 3 over $\mathbb{F}_p$, S must be the ring of upper triangular matrices. Similarly, with respect to some other basis, T is the ring of upper triangular matrices. But change of basis is given by conjugation, and so S and T are conjugate subrings. Hence $f : S \to T$ is given by conjugation and so f

extends to an automorphism of $R = M_2(\mathbb{F}_p)$.

Case $\dim_{\mathbb{F}_p} S = 4$: In this case, $S = R$ and so f is an automorphism of R.

Therefore any isomorphism between unital subrings of $R = M_2(\mathbb{F}_p)$ extends to an automorphism of R and so R is ultrahomogeneous. By problem 4, since R is finite, $Th(R)$ has quantifier elimination.

So, for a finite simple unital ring, R, $Th(R)$ has quantifier elimination if and only if $R \cong M_n(\mathbb{F}_{p^k})$ for p prime with $n = 1$ or ($n = 2$ and $k = 1$).