Algebra QE I Exam
August 2023

Name . . . .

KSU Email . . . .

Instructions:

Do not write your name or any other identifying information on any page except this cover page.

Use the space below the statement of a problem as well as the back of the page and the next page for the solution. If more space is needed, use the blank pages at the end.

All pages must be submitted. If there is work you want ignored, cross it out (or otherwise indicate its status) or tape a clean sheet over it to create more space to be used, being careful not to cover the code at the top.

You have three hours to work on these problems. Attempt all problems. Four complete solutions will earn a pass. Credit for completed parts of separate problems may combine to result in a pass.

No references are to be used during the exam.

All rings are assumed to be unitary (i.e., with 1) and all ring homomorphisms are assumed to send 1 to 1. A ring is assumed to be possibly noncommutative unless stated explicitly.

1. **(10 pts)** Let G be a group of order $56 = 2^3 \cdot 7$. Show that G is not simple.

2. **(10 pts)** Prove Cayley's theorem: Any group of order n is isomorphic to a subgroup of the permutation group S_n.

3. **(10 pts)** Let x^2+x+1 be an element in the polynomial ring $\mathbb{Z}[x]$ and consider the quotient ring

$$R := \mathbb{Z}[x]/(2, x^2+x+1).$$

(a) List all elements of R and write the addition table of additive group $(R, +)$.

(b) Write the multiplication table of nonzero elements $R^\times = R \setminus \{0\}$ in R and prove that the set $R^\times$ with multiplication is a cyclic group of order 3. Deduce that R is a field.

4. **(10 pts)** Let R be a ring, M a left R-module, and $N \subseteq M$ an R-submodule. Denote by $\pi : M \to M/N$ the quotient map. Let M_1 and M_2 be two R-submodules of M, such that $M_1 \subseteq M_2$. Show that $M_1 = M_2$ if and only if $M_1 \cap N = M_2 \cap N$ and $\pi(M_1) = \pi(M_2)$.

   Give an example to show that, without the assumption $M_1 \subseteq M_2$, $M_1 \cap N = M_2 \cap N$ and $\pi(M_1) = \pi(M_2)$ do not imply $M_1 = M_2$.

5. **(10 pts)** Let V be a vector space over a field k and $\phi : V \to V$ be a linear transformation. Show that, for $\lambda \in \mathsf{k}$, the set

$$V_\lambda(\phi) = \{v \in V \mid (\phi - \lambda)^m v = 0 \ \ \textit{for some } m > 0\}$$

is a vector subspace of V and that $\phi(V_\lambda(\phi)) \subseteq V_\lambda(\phi)$. Furthermore, show that $V_\lambda(\phi) \neq 0$ if and only if λ is an eigenvalue of ϕ.

6. **(10 pts)** It is given as a fact that $|\mathsf{Aut}(E/F)| \leq [E : F]$ for any finite extension of fields $F \subseteq E$. Let p be a prime, $F = \mathbb{Z}/p\mathbb{Z}$ be the finite field with p elements, and K be a finite field with p^n elements with n being a positive integer. It is known that K contains a subfield isomorphic to F (the subfield generated by 1). Prove that $\mathsf{Aut}(K/F)$ is a cyclic group of order n, generated by $\tau : K \to K$, defined as $\tau(\alpha) = \alpha^p$ for all $\alpha \in K$. Then prove that $F \subseteq K$ is a Galois extension.

   Note that $\mathsf{Aut}(E/F) = \{\sigma \in \mathsf{Aut}(E) \mid \sigma(\alpha) = \alpha \ (\forall \alpha \in F)\}$.