Algebra Qualifying Exam
August 27, 2021 (1pm–5pm)

For *page arrangement*, follow these general instructions closely throughout the test.

- Write in a legible fashion.
- For each sheet, write only on a single side and leave a 1×1 square inch area blank at the upper left corner – for staples.
- Start with a new sheet for each question.
- Absolutely no cell phones of any kind during the entire test.
- Arrange all papers by the order of the questions before submission.

The following instructions are given in "Algebra Qualifying Exam August 2021 Guidelines" under "Exam Format". It is the student's responsibility to read and follow these instructions carefully.

- Do seven problems out of eight. The exam is 70 points. Each problem is worth 10 points.
- If you attempt solutions to all eight problems, then only the **first seven** submitted problems will be graded.
- No calculators or other electronic devices are allowed.
- Write in a legible fashion. Give proper mathematical justification of all your statements. Your solutions must be detailed enough to get full credit.
- Start with a new sheet for each problem. Clearly write the problem number and your name before beginning your solution. For each sheet, write only on a single side. Arrange all papers by the order of the questions before submission.
- All your submitted written responses will be graded. If you write any statements (correct or incorrect) which are not used in your solution, you will be penalized. Please make sure to erase clearly the responses you don't want to be graded.
- If multiple version of solutions are provided, then all versions will be graded and then the average credits is taken as the final score.
- No questions may be asked during the exam. If a problem appears ambiguous to you, interpret it in a way that makes sense to you but not in a way that makes it trivial.
- Throughout the exam, if a question has multiple parts, you may assume any previous part as a true statement in order to answer the consecutive parts whenever needed.

Exam grade: In order to pass the algebra qualifying exam, you must satisfy the following two criteria:

(a) Receive the full score from at least three questions.

(b) Receive a passing score 70% or better; equivalently, 49 points or more out of the total 70 points.

Notation. Throughout the exam, we use the following notation:
$\mathbb{Z}$ is the ring of integers;
$\mathbb{Q}$ is the field of rational numbers;
$\mathbb{R}$ is the field of real numbers;
$\mathbb{C}$ is the field of complex numbers;
$\mathbb{F}_q$ is the field with q elements, where $q = p^k$ for some prime p and $k \geq 1$;
S_n is the symmetric group on a set of n elements.

1. Assume that n is an integer greater than or equal to 2. We consider the symmetric group S_n on a set of n elements.

[3 points] (a) Prove that S_n is generated by transpositions; i.e., two-cycles.

[2 points] (b) Prove that S_n is generated by $\{(1\ \ i) \,|\, 2 \leq i \leq n\}$.

[2 points] (c) Prove that S_n is generated by $\{(i\ \ i+1) \,|\, 1 \leq i \leq n-1\}$.

[3 points] (d) Prove that S_n is generated by $(1\ \ 2)$ and $(1\ \ 2\ \ \cdots\ \ n)$.

2. Let G be a group acting on a set S. We say that $a \in S$ is a fixed point if $g \cdot a = ga$ for all $g \in G$. Assume that p is a prime. A finite group with order equal to a power of p is said to be a p-group.

[4 points] (a) Let G be a p-group acting on a finite set S. Let F denote the set of all fixed points under this action. Prove that
$$|S| \equiv |F| \bmod p.$$

[3 points] (b) Let G be a finite group and H a p-subgroup of G. Prove that
$$[G : H] \equiv [N(H) : H] \bmod p$$
where $N(H)$ is the normalizer of H in G. (*Hint:* Consider the action of H on G/H by left multiplication.)

[3 points] (c) Let G be a p-group and let $H \leq G$ be such that $[G : H] = p$. Prove that $H \trianglelefteq G$.

[4 points] 3. (a) Solve the following simultaneous system of congruences over $\mathbb{Z}$:
$$x \equiv 1 \bmod 4$$
$$x \equiv 2 \bmod 11$$
$$x \equiv 3 \bmod 27.$$

[3 points] (b) In the polynomial ring $\mathbb{R}[x]$, are the two polynomials $f(x) = x^4 + x^3 + x^2 + x + 1$ and $g(x) = x^2 + x + 1$ relatively prime? (You must justify the answer.)

[3 points] (c) Determine whether or not the following congruent system is solvable in $\mathbb{R}[x]$:
$$F \equiv 1 \bmod f$$
$$F \equiv 2 \bmod g.$$

If yes, find F. Otherwise, justify the answer.

4. Let R and S be commutative rings. Assume that $f\colon R \longrightarrow S$ is a ring homomorphism.

[4 points] (a) Let I be an ideal in S. Prove that the preimage of I is an ideal in R.

[3 points] (b) Let $\mathfrak{p}$ be a prime ideal in S. Is the preimage of $\mathfrak{p}$ a prime ideal in R? Prove or provide a counterexample that is not a trivial homomorphism.

[3 points] (c) Let $\mathfrak{m}$ be a maximal ideal of S. Is the preimage of $\mathfrak{m}$ a maximal ideal in R? Prove or provide a counterexample that is not a trivial homomorphism.

[3 points] 5. (a) Show that $3x^4 - 4x^2 + 3x + 5$ is irreducible in $\mathbb{Z}[x]$. (*Hint:* Consider the polynomial modulo the ideal in $\mathbb{Z}$ generated by 2.)

[2 points] (b) Show that $x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. (Recall $\mathbb{F}_2$ from the notation list in the previous page.)

[2 points] (c) Let E be the splitting field of of x^3+x+1 over $\mathbb{F}_2$. Assume that r is a root of x^3+x+1 in E. Prove that r^2 is also a root of $x^3 + x + 1$.

[3 points] (d) Let E be as in the previous part. Determine the degree of E as an extension field over $\mathbb{F}_2$.

[4 points] 6. (a) Let $f(x)$ be a polynomial in $\mathbb{Q}[x]$ with the splitting field $K \subseteq \mathbb{C}$. Let G denote the Galois group of $f(x)$ over $\mathbb{Q}$. Prove that the complex conjugation defines an element of G; i.e., if $\sigma\colon \mathbb{C} \longrightarrow \mathbb{C}$ is given by $\sigma(z) = \overline{z}$, then the restriction of σ on K is an element of G.

[6 points] (b) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p, where p is a prime. Assume that $f(x)$ has all but two roots in $\mathbb{R}$. Prove that the Galois group of $f(x)$ over $\mathbb{Q}$ is isomorphic to S_p. (Note: You can use the following result: a subgroup of S_p containing any p-cycle and any transposition is S_p.)

7. Let R be a ring, let M, M', and N be R-modules, and let $f\colon M \longrightarrow N$, $g\colon M' \longrightarrow N$ be R-module homomorphisms. Define the *fiber product* (or *pull back*) of f and g as

$$X = \big\{(a,b) \,|\, a \in M,\ b \in M',\ \text{such that } f(a) = g(b)\big\},$$

and define the projections $\pi_1(a,b) = a$ and $\pi_2(a,b) = b$.

[3 points] (a) Show that X is an R-submodule of $M \oplus M'$ and that the following diagram commutes; that is, $f \circ \pi_1 = g \circ \pi_2$ in

$$\begin{array}{ccc} X & \xrightarrow{\ \pi_2\ } & M' \\ {\scriptstyle \pi_1}\big\downarrow & & \big\downarrow{\scriptstyle g} \\ M & \xrightarrow[\ f\ ]{} & N \end{array}$$

[1 point] (b) Show that if f is injective then π_2 is injective.

[1 point] (c) Show that if f is surjective then π_2 is surjective.

[2 points] (d) Now suppose $0 \longrightarrow L \xrightarrow{h} M \xrightarrow{f} N \longrightarrow 0$ is a short exact sequence and define $h' \colon L \longrightarrow X$ by $h'(n) = \big(h(n), 0\big)$. Show that the following diagram is commutative with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L & \xrightarrow{h'} & X & \xrightarrow{\pi_2} & M' & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \mathrm{id}_L} & & \Big\downarrow{\scriptstyle \pi_1} & & \Big\downarrow{\scriptstyle g} & & \\
0 & \longrightarrow & L & \xrightarrow[h]{} & M & \xrightarrow[f]{} & N & \longrightarrow & 0
\end{array}$$

[3 points] (e) Let $0 \longrightarrow K \longrightarrow P \xrightarrow{\varphi} M \longrightarrow 0$ and $0 \longrightarrow K' \longrightarrow P' \xrightarrow{\varphi'} M \longrightarrow 0$ be two short exact sequences of R-modules, where P and P' are projective. Show that $P \oplus K' \cong P' \oplus K$.

8. Let β be a linear transformation on a vector space $M = \mathbb{Q}^3$ over $\mathbb{Q}$. We view M as a module over a polynomial ring in one variable $\mathbb{Q}[t]$ via β; namely

$$t \cdot v = \beta(v) = \begin{pmatrix} 3 & -4 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot v,$$

for any $v = (a, b, c)^\top \in M$ where $^\top$ means transpose.

[4 points] (a) Knowing that $\mathbb{Q}[t]$ is a principal ideal domain (P.I.D.), decompose M as a product of cyclic modules.

[6 points] (b) Find a generator for each cyclic module in the above decomposition.