Modern Algebra 1 — Exam 1
MAT 514/614, Spring 2025 — D. Ivanšić

Name:____________________________

Show all your work!

Do all the theory problems. Then do five problems, at least two of which are of type B (one if you are an undergraduate student). If you do more than five, best five will be counted.

Theory 1. (3pts) Define a ring, while condensing all the conditions that only involve addition into one simple condition that "$(R, +)$ is an a____ g____."

Theory 2. (3pts) State Cauchy's theorem on abelian groups.

Theory 3. (3pts) Define the characteristic of a ring.

Type A problems (5pts each)

A1. Show that the subgroup of even permutations $A_n \leq S_n$ is normal.

A2. List all possible abelian groups of order 1400.

A3. Give an example of a ring where elements do not all have the same additive order.

A4. Determine whether the set $S = \left\{ \begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} \mid a, b \in \mathbf{R} \right\}$ is a subring of $M_2(\mathbf{R})$.

A5. Show that the polynomial $2x + 3$ is a unit in the polynomial ring $\mathbf{Z}_4[x]$.

A6. Let R be an integral domain with characteristic 3. Show that $(x + y)^4 = x^4 + y^4$ if and only if $x = 0$, $y = 0$ or $x^2 + y^2 = 0$.

Type B problems (8pts each)

B1. Let $GL(2, \mathbf{Z})$ be the group of all invertible 2×2 matrices with integer entries whose inverse is in $GL(2, \mathbf{Z})$. Let $SL(2, \mathbf{Z}) = \{A \in M_2(\mathbf{Z}) \mid \det A = 1\}$.
a) What can you say about $\det A$ if $A \in GL(2, \mathbf{Z})$?
b) Show that $SL(2, \mathbf{Z})$ is a normal subgroup of $GL(2, \mathbf{Z})$.
c) Find the index of $SL(2, \mathbf{Z})$ in $GL(2, \mathbf{Z})$ and determine $GL(2, \mathbf{Z})/SL(2, \mathbf{Z})$. (First isomorphism theorem will help.)

B2. Let G be a finite abelian group such that pq divides $|G|$, where p and q are distinct primes. Use the fundamental theorem of finite abelian groups or other method to show that G has an element of order pq.

B3. Let $\phi : G \to \overline{G}$ be a surjective homomorphism, let $\overline{H}$ be a subgroup of $\overline{G}$ finite index and let $H = \phi^{-1}(\overline{H})$. Show that the index of H in G is the same as the index of $\overline{H}$ in $\overline{G}$.

B4. Show that $\mathbf{Z} \times \mathbf{Z} / \langle (3, 5) \rangle \approx \mathbf{Z}$. (Cook up a surjective homomorphism $\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ that sends $(3, 5)$ to 0 and apply the first isomorphism theorem.)

B5. Determine the smallest subring of $\mathbf{Q}$ that contains $\frac{2}{3}$.

Modern Algebra 1 — Exam 2 MAT 514/614, Spring 2025 — D. Ivanšić	Name: ______________________________ *Show all your work!*

Do all the theory problems. Then do five problems, at least two of which are of type B (one if you are an undergraduate student). If you do more than five, best five will be counted.

Theory 1. (3pts) If R, S are rings, define a ring homomorphism $f : R \to S$.

Theory 2. (3pts) Let $f \in R[x]$ be a polynomial. State the theorem on the connection between a being a zero of f and divisibility of f by a certain polynomial.

Theory 3. (3pts) State the theorem that helps you tell when $f \in \mathbf{Z}[x]$ is irreducible over $\mathbf{Q}$ by connecting it to an $\overline{f} \in \mathbf{Z}_p[x]$.

Type A problems (5pts each)

A1. Let R be a commutative ring with unity and A a maximal ideal of R. Show that A is a prime ideal.

A2. Let $S = \{a + bi \mid a, b \in \mathbf{Z}, 3|b\}$. Show that S is a subring of $\mathbf{Z}[i]$, but not an ideal.

A3. Show that one of the homomorphisms with the stated properties exists, and the other does not. For the one that exists, write the table of values.

a) $\phi : \mathbf{Z}_5 \to \mathbf{Z}_{20}$, $\phi(1) = 16$

b) $\phi : \mathbf{Z}_{21} \to \mathbf{Z}_{15}$, $\phi(1) = 5$

A4. Let $A \subseteq \mathbf{Q}[x]$ be the set $A = \{f \in \mathbf{Q}[x] \mid a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \cdots + a_1 \cdot 2 + a_0 = 0\}$. Show that A is an ideal by finding its generator.

A5. Show that the polynomials are irreducible over $\mathbf{Q}$: a) $x^5+5x^2+20x-5$ b) x^3-x^2+3x+1

Type B problems (8pts each)

B1. Determine the number of elements in $\mathbf{Z}[i]/\langle 1 + i\rangle$ and state the characteristic of this quotient ring.

B2. Show that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

B3. If F is a field (and therefore and integral domain), show that the field of quotients of F is isomorphic to F.

B4. Let $A \subseteq \mathbf{Q}[x]$ be the set $A = \{f \in \mathbf{Q}[x] \mid f(2) = 0, f(4) = 0, f(-1) = 0\}$. Show that A is an ideal and find its generator.

B5. Show that $x^4 + 5$ is irreducible over $\mathbf{Q}$, but is reducible over $\mathbf{R}$.

B6. Let $f, g \in \mathbf{Z}[x]$, where the leading coefficient of g is 1. Use induction to show that the division algorithm is true in this case, that is, there exist unique polynomials $q, r \in \mathbf{Z}[x]$ such that $f = gq + r$, where $\deg r < \deg f$ or $r = 0$.

Modern Algebra 1 — Exam 3
MAT 514/614, Spring 2025 — D. Ivanšić

Name: ______________________________

Show all your work!

Do all the theory problems. Then do five problems, at least two of which are of type B (one if you are an undergraduate student). If you do more than five, best five will be counted.

Theory 1. (3pts) Define the Galois group $\mathrm{Gal}(E/F)$ of a field E over F.

Theory 2. (3pts) State the theorem that guarantees the existence in some way of a zero of any polynomial $f \in F[x]$.

Theory 3. (3pts) Define a solvable group.

Type A problems (5pts each)

A1. Show that $\mathbf{Q}(2+\sqrt{5}) = \mathbf{Q}(\sqrt{5})$.

A2. Determine the splitting field of $x^4 - 1$ over $\mathbf{Q}$.

A3. Show that $x^2 + x + 1$ is irreducible in $\mathbf{Z}_2[x]$. How many elements are in $\mathbf{Z}_2(\alpha) \approx \mathbf{Z}_2[x]/\langle x^2 + x + 1\rangle$? Write the table of multiplication for its nonzero elements.

A4. Are $\mathbf{Q}(\sqrt{3})$ and $\mathbf{Q}(\sqrt{3}i)$ ring isomorphic?

A5. Show that the dihedral group D_n is solvable.

A6. Suppose E is the splitting field of some polynomial over a field F of characteristic zero, so that $\mathrm{Gal}(E/F)$ is abelian and has order 21. Draw the subfield lattice for fields between E and F.

Type B problems (8pts each)

B1. Show that $x^3 + 2x + 2$ is irreducible in $\mathbf{Z}_3[x]$, so it has a zero β in some extension of $\mathbf{Z}_3$. Factor $x^3 + 2x + 2$ into linear factors in $\mathbf{Z}_3(\beta)[x]$.

B2. What is the order of the splitting field of the polynomial $(x^2+x+1)(x^3+x+1) \in \mathbf{Z}_2[x]$ over $\mathbf{Z}_2$?

B3. Factor $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbf{Z}_2[x]$ into irreducible factors by showing first f has no zeroes in $\mathbf{Z}_2$. This leaves two possibilities: $f = pq$, where $\deg p = 2$ or 3. Try some p's, keeping in mind that p cannot have any zeros in $\mathbf{Z}_2$, and checking if p divides f.

B4. Let E be the splitting field of $f(x) = x^5 - 1$ over $\mathbf{Q}$. Thinking of it as $\mathbf{Q}(\omega)$, where ω is the primitive 5-th root of 1, identify the group that $\mathrm{Gal}(E/\mathbf{Q})$ is isomorphic to, and show that $\mathbf{Q}(\omega+\omega^4)$ is fixed by a subgroup of $\mathrm{Gal}(E/\mathbf{Q})$. (Since $\omega + \omega^4 \notin \mathbf{Q}$, $\mathbf{Q}(\omega+\omega^4) \neq \mathbf{Q}$. It turns out to be $\mathbf{Q}(\sqrt{5})$, but you don't have to show this.)

B5. Let E be the splitting field of $f(x) = (x^2-2)(x^2-3)$ over $\mathbf{Q}$. Describe $\mathrm{Gal}(E/\mathbf{Q})$ and determine the lattice of subgroups of $\mathrm{Gal}(E/\mathbf{Q})$. For the automorphism that keeps no roots of f fixed, determine the fixed field.

Type C problems (12pts each)

C1. Show A_5 is not solvable by showing it has no nontrival normal subgroups. To do this, assume $H \neq \{\varepsilon\}$ is a normal subgroup of A_5. Then show:
1) If $f = (a_1, \ldots, a_k)$ is a 5-cycle or a 3-cycle, show that by conjugating it with a 2-cycle we can get any consecutive a_i and a_{i+1} to trade places and, in the case of a 3-cycle, we can swap any a_i with a number outside of $\{a_1, a_2, a_3\}$.
2) Show this implies that by conjugating several times, we can turn a fixed k-cycle into any k-cycle, $k = 3, 5$.
3) Argue that 2) implies that if H contains any 5-cycle or 3-cycle, it has to contain all of them.
4) Similarly to 1), show that we can conjugate any product of two 2-cycles to any other product of two 2-cycles, so if H contains any product of two 2-cycles, it has to contain all of them.
5) Finish the argument by considering what is possible for order of H and the numbers of 3- and 5-cycles and products of two 2-cycles in A_5.