PRACTICE Final Exam for Math 453
Due Tuesday, May 3, 2022, at 11:59pm

A mathematician is a device for turning coffee into theorems. –Paul Erdős

Take this practice exam on your own, giving yourself two hours, then go back and check your solutions. The instructions that will appear on the actual exam follow below.

- **Please do not begin until you are instructed to do so.**
- You are not allowed outside notes, calculators, phones, or internet access during the exam. Please leave your phone in your bag/purse/backpack and do not take it with you if you get up to use the restroom.
- Extra scratch paper is available at the front of the room. Turn in with your exam any work that you would like to have graded.
- You will have **2 hours (120 minutes)** to complete this exam. The approximate time remaining will be visible at the front of the room.
- On this exam:
  - PROBLEM 1 involves giving definitions of terms.
  - PROBLEM 2 involves stating theorems from the textbook.
  - PROBLEM 3 is TRUE/FALSE, and PROBLEM 4 involves proving/disproving statements from PROBLEM 3.
  - PROBLEMS 5–7 are calculations, of which PROBLEM 5 was previously an exercise from a workshop, and the others are new calculations.
  - PROBLEMS 8–10 are proofs, of which PROBLEM 8 was previously a homework problem, and the others are new proofs.
- Show your work on all problems (except TRUE/FALSE), including problems you have done before.
- If you have a question, please raise your hand.
- You may turn in your exam early if you finish early, **unless** there are fewer than 10 minutes remaining, in which case you should wait until time is called to avoid disturbing other students.
- Good luck!

Problem 1

Complete the definitions of the following terms. (Make sure you give the *defintion*, not another condition that we proved was equivalent.)

(a) [3 points] Let X be a set. A function $\pi : X \to X$ is a **permutation** if...

(b) [3 points] Let F be a field and E a field extension of F. Then E is **algebraic** over F if...

(c) [4 points] Let R be a ring and I be an ideal of R. The ideal I is a **maxiaml ideal** if...

PROBLEM 2

Complete the statements of the following theorems.

(a) [5 points] [**Lagrange's Theorem**] Let G be a finite group, and let H be a subgroup of G. Then...

In particular...

(b) [5 points] [**Second Isomorphism Theorem**] Let H be a subgroup of a group G and N a normal subgroup of G. Then...

PROBLEM 3

Determine whether each of the following statements are true or false. Write TRUE or FALSE.

(a) In the RSA algorithm with $n = pq$, the integers D and E are chosen so that the product $DE \equiv 1 \pmod{(p-1)(q-1)}$.

(b) Let $n \in \mathbb{N}$, and suppose $n = \prod_{j=1}^{k} p_j^{e_j}$ is the factorization of n into distinct prime powers. Let $e = \max_{1 \le j \le n} e_j$, that is, e is the largest of the exponents e_j. Up to isomorphism, the number of abelian groups of order n is equal to e.

(c) If G is a group of order n, $d \in \mathbb{N}$, and $d|n$, then G has a subgroup of order d.

(d) If R is an integral domain, then every ideal of R is a principal ideal.

(e) If E is an field extension of a field F and the degree of E over F is finite, then E is algebraic over F.

PROBLEM 4

(a) [5 points] Prove one of the true statements from Problem 3, excluding statment (a). (If the statement is a direct restatement of a theorem from the textbook, reprove that theorem rather than just citing it. Otherwise, you may use any theorem we covered in this course.)

(b) [5 points] Disprove one of the false statements from Problem 3, excluding statment (a). (You may do so by giving a counterexample, if appropriate.)

PROBLEM 5

Let $K = \mathbb{Q}(\sqrt{2})$. Let $\mathcal{B} = \{1, \sqrt{2}\}$. Let $\phi : \mathbb{Q}^2 \to K$ be the $\mathbb{Q}$-linear transformation

$$\phi\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = x + y\sqrt{2}.$$

Let $\alpha \in K$, and write $\alpha = a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. Define the $\mathbb{Q}$-linear transformation $T_\alpha : K \to K$ by $T_\alpha(\zeta) = \alpha\zeta$. **Find a matrix** M_α such that $(\phi^{-1} \circ T_\alpha \circ \phi)\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = M_\alpha \begin{bmatrix} x \\ y \end{bmatrix}$. (In other words, M_α should be the matrix that represents T_α in the basis $\mathcal{B}$.)

PROBLEM 6

Find integers r and s such that

$$97r + 42s = 1.$$

PROBLEM 7

Find the splitting field K of the polynomial $f(x) = x^4 - 4x^2 - 1$ over $\mathbb{Q}$, and find $[K : \mathbb{Q}]$.

Problem 8

If H and K are normal subgroups of a group G and $H \cap K = \{e\}$, prove that G is isomorphic to a subgroup of the direct product group $(G/H) \times (G/K)$.

PROBLEM 9

Prove **either one (and only one)** of the following two statements. Circle the letter for the statement you are proving.

(a) Let R and S be rings with identity $1 \in R$, $1 \in S$, and suppose that S is an integral domain. Let $\phi : R \to S$ be a ring homomorphism such that $\ker \phi \neq R$. Prove that $\phi(1) = 1$.

(b) An ideal M in a commutative ring R is **minimal** if $M \neq \{0\}$ and, for any ideal I,

$$\{0\} \subseteq I \subseteq M \implies I = \{0\} \text{ or } I = M.$$

If R is an integral domain that isn't a field, prove that R has no minimal ideals.

PROBLEM 10

Let $p \geq 3$ be a prime number. Prove that S_p contains exactly $(p-2)!$ distinct subgroups of order p, each of which is of the form $\langle \sigma \rangle$ where σ is an p-cycle.