Math 611 Final Exam, Wednesday 12/11/19 – Wednesday 12/18/19.

Instructions: This is a take home exam. Please note that collaboration with other students on the exam is not allowed. Justify all your answers carefully. If you use a result proved in the textbook, class notes, or homework solutions, state the result precisely. I will hold office hours on Monday 3-4PM and Tuesday 1-2PM in LGRT 1235H. Please turn in your exam either to my office LGRT 1235H or my mailbox in LGRT 1623D by 5PM on Wednesday 12/18/19.

(1) Let G be a finite group. Suppose there is a conjugacy class $C \subset G$ of size $|C| = 2$. Prove that G is not a simple group.

(2) Let G be a non-abelian group of order 117 containing an element of order 9.

   (a) Describe G explicitly (i) as a semidirect product and (ii) in terms of generators and relations. (You should in particular show that G is uniquely determined up to isomorphism by the above properties.)

   (b) Determine the center $Z(G)$ of G.

   (c) Determine the number of elements of G of order (i) 13 and (ii) 3.

(3) (a) Let R be a ring and $I \subset R$ an ideal. Describe a bijective correspondence between ideals of the quotient ring R/I and ideals of R containing I. (This may be stated without proof.)

   (b) Let n be a positive integer. Consider the quotient ring $S = \mathbb{R}[x]/(x^n)$.

      i. Determine a basis of S as an $\mathbb{R}$-vector space.

      ii. Find all the ideals of S and identify the prime ideals.

      iii. Determine the units of S.

(4) Let $\omega = \frac{1}{2}(-1+\sqrt{-3}) = e^{2\pi i/3} \in \mathbb{C}$, a primitive cube root of unity, and

$$R = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

the subring of $\mathbb{C}$ generated by ω. *Note that the ring R was studied in HW5Q2. You may use properties of R established in the homework solutions without proof.*

Let $p \in \mathbb{N}$ be a prime number. Show that the following conditions are equivalent.

(a) p is irreducible in R.

(b) The quotient ring $R/(p)$ is a field.

(c) The equation $x^2 + x + 1 = 0$ has no solutions modulo p.

(d) $p \equiv 2 \bmod 3$.

(5) Let M denote the abelian group $\mathbb{Z}^3$, and let $N \subset M$ be the subgroup generated by the elements

$$m_1 = \begin{pmatrix} 3 \\ 2 \\ -4 \end{pmatrix}, \; m_2 = \begin{pmatrix} 1 \\ -3 \\ 6 \end{pmatrix}, \; m_3 = \begin{pmatrix} -4 \\ 1 \\ -2 \end{pmatrix}.$$

(a) Determine the isomorphism type of the abelian groups N and M/N. (Identify each group with a direct product such that each factor is equal to $\mathbb{Z}$ or $\mathbb{Z}/p^\alpha\mathbb{Z}$ for some prime p and $\alpha \in \mathbb{N}$.)

(b) Does there exist a subgroup $L \subset M$ such that $M = L \times N$? Justify your answer carefully.

(6) Let R be a ring. We say an R-module M is *simple* if $M \neq \{0\}$ and the only submodules of M are $\{0\}$ and M.

(a) Show that M is simple if and only if M is isomorphic to R/I for some maximal ideal I of R.

(b) Using part (a) or otherwise, determine a matrix $A \in \mathrm{GL}_4(\mathbb{Q})$ with the following property: If $W \subset \mathbb{Q}^4$ is a $\mathbb{Q}$-vector subspace such that $A \cdot W \subset W$, then $W = \{0\}$ or $W = \mathbb{Q}^4$.

Hints:

1 What does it mean for a group to be simple? What is the orbit-stabilizer theorem? What are some sufficient conditions for a subgroup of a group to be normal?

2 (a) What are the Sylow therorems? How can we recognize a semi-direct product? What is the automorphism group of $\mathbb{Z}/p\mathbb{Z}$ and what can you say about it? (b) Compute explicitly using the generators and relations found in part (a). What is a convenient expression for an arbitrary element of the group in terms of the generators (compare the dihedral group)? Note that an element lies in the center if and only if it commutes with each generator. (c) Why is (b) relevant here?

3 (a) See DF 7.3. (b)(iii) Compute explicitly or use (ii).

4 What does ED $\Rightarrow$ PID $\Rightarrow$ UFD mean? What are the maximal ideals in a PID? What is the kernel of the homomorphism $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}[\omega]$ given by $\varphi(f(x)) = f(\omega)$? (What is the minimal polynomial of ω? What is the Gauss lemma (DF 9.3)?) What is the first isomorphism theorem? If $\alpha \in \mathbb{Z}/p\mathbb{Z}$ is a solution of $x^2+x+1 = 0 \bmod p$, what is the order of α in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of the field $\mathbb{Z}/p\mathbb{Z}$? What can you say about the group $(\mathbb{Z}/p\mathbb{Z})^\times$? Compare the description of the primes in the Gaussian integers $\mathbb{Z}[i]$ given in class and HW5Q13.

5 (a) An abelian group is the same thing as a $\mathbb{Z}$-module (why?). What is the Smith normal form of a matrix? (b) What can you say about a subgroup of a free abelian group?

6 (a) What are the submodules of the R-module $R = R^1$? Review Q3a. How can we describe the isomorphism type of a module that is generated by a single element? (What is the annihilator of an element of an R-module?). (b) For F a field, review the correspondence between $F[x]$-modules M and F-vector spaces V together with a linear transformation $T\colon V \to V$. What are the maximal ideals I of $F[x]$? What is a basis of $M = F[x]/I$ as an F-vector space? What is the matrix of the linear transformation T with respect to this basis?