Math 7751, Fall 2018. Final exam. Due Tuesday, Dec 18th, by noon

Directions: Each problem is worth 15 points. The best 5 out of 6 scores will be counted with 100% weight, and the lowest score will be counted with $33\frac{1}{3}\%$ weight, so the maximal possible total is 80 points. Provide complete arguments (do not skip steps). State clearly any result you are referring to. Partial credit for incorrect solutions, containing steps in the right direction, may be given.

Rules: You are not allowed to discuss midterm problems with each other. You may ask me any questions about the problems (e.g. if the formulation is unclear), but as a rule I will only provide minor hints. You may freely use your class notes, previous homework assignments and the book by Dummit and Foote. The use of other books is allowed, but not encouraged. If you happen to run across a problem very similar or identical to one on the midterm which is solved in another book, do not consult that solution. The use of any online resources (except the class webpage) is absolutely prohibited.

Warning: Any exams turned in at 12:01pm on Dec 18 or later will not be accepted.

1. Let G be a group of order pqr where p, q, r are distinct primes and

(i) $p > q > r$

(ii) $gcd(q, p-1) = gcd(r, q-1) = gcd(r, p-1) = 1$.

(a) Prove that G has a normal subgroup P of order p.

(b) Prove that G has a normal subgroup S of order pq and that this subgroup S is cyclic.

(c) Finally prove that G itself is cyclic.

2. Let G be a finite abelian group and let p be a prime.

(a) Prove that the number of elements of order p in G is equal to the number of nontrivial homomorphisms from G to $\mathbb{Z}_p$. **Hint:** Calculate both numbers explicitly in terms of the EDF decomposition of G

(b) Use (a) to prove that the number of subgroups of order p in G is equal to the number of subgroups of index p in G

3.

(a) Find a monic irreducible polynomial of degree 4 in $\mathbb{F}_2[x]$. Then use it to construct a field F with $|F| = 16$ and **find explicitly** a generator of the multiplicative group $F^\times$ (recall that we proved in class that $F^\times$ is cyclic).

(b) Let $p > 3$ be a prime and $R = \mathbb{F}_p[x]/(x^3 - 1)$. Describe the multiplicative group $R^\times$ as a direct product of cyclic groups. **Hint:** There will be two different cases depending on whether $p \equiv 1$ or $2 \bmod 3$.

4. Let $\mathbb{R}$ denote the real numbers. The purpose of this problem is to show that the ring $A = \mathbb{R}[x, y]/(x^2+y^2-1)$ is not a UFD. For an element $f \in \mathbb{R}[x, y]$ we denote its image in A by $[f]$.

(a) Show that every element of A can be uniquely represented in the form $[f(x) + g(x)y]$ where $f(x), g(x) \in F[x]$.

(b) Show that A has an automorphism ϕ of order 2 such that $\phi([f(x)]) = [f(x)]$ for each $f(x) \in F[x]$ and $\phi([y]) = -[y]$.

(c) Use (a) and (b) to construct a function $N : A \to F[x]$ such that $N(uv) = N(u)N(v)$ for all $u, v \in A$.

(d) Use the function N from (c) to show that $[x]$ is an irreducible element of A and that the only invertible elements of A are (images of) nonzero constant polynomials. **Hint:** It is essential that you are working over $\mathbb{R}$, not over $\mathbb{C}$.

(e) Now show that A is not a UFD.

5. A commutative ring R with 1 is called *Artinian* if it satisfies the descending chain condition (DCC) on ideals, that is, if $I_1 \supseteq I_2 \supseteq \ldots$ is a descending chain of ideals, there exists $N \in \mathbb{N}$ such that $I_n = I_N$ for any $n \geq N$.

(a) Assume that R is Artinian, and let $\phi : R \to R$ be an injective homomorphism of additive groups such that $\operatorname{Im} \phi^n$ is an ideal for all $n \in \mathbb{N}$. Prove that ϕ is surjective.

(b) Give an example of an Artinian ring R with 1 and a ring homomorphism $\phi : R \to R$ which is injective and not surjective.

(c) Use (a) to prove that any Artinian domain must be a field. **Note:** The result should follow from (a) in a few lines. Do not use any other results about Artinian rings (including those established in DF, Chapter 16).

(d) (not directly related to (a)-(c)) Let R be a commutative ring with 1, and let $f \in R$ be such that the ideal (f) is maximal. Prove that if I is any ideal such that $(f) \supseteq I \supseteq (f^2)$, then $I = (f)$ or $I = (f^2)$.

6. Let F be a field and $R = F[x, y]$ the ring of polynomials over R in two (commuting) variables x and y. Let $I = xR$ be the principal ideal of R generated by x and $S = F + I = \{f + i : f \in F, i \in I\}$. Observe that S is a subring of R and I is an ideal of S (you need not justify these facts).

(a) Prove that I is not finitely generated as an ideal of S. **Hint:** Assume that I is finitely generated as an ideal of S and reach a contradiction by showing that there must exist a natural number m such that any polynomial $p(x, y) \in I$ contains no monomials of the form xy^n, with $n > m$.

(b) Prove that if R is a finitely generated commutative ring, then R is Noetherian (in class we proved this for commutative rings with 1). **Hint:** use the fact that any ring R can be embedded into a ring $\widetilde{R}$ with 1: define $\widetilde{R} = \mathbb{R} \times \mathbb{Z}$ as a set, with componentwise addition and multiplication given by

$$(r_1, n)(r_2, m) = (r_1 r_2 + n r_2 + m r_1, nm)$$

(note that $(0, 1)$ is the unity of $\widetilde{R}$).