21-373 Final exam theorem list

- Two out of eight questions on the final exam will ask you to prove results that we proved in class. This document is about them.
- In proving the results you can use only results that precede it in the book/lectures. [For example, you cannot use the classification of finite abelian groups to prove Application 1 on page 61.]
- You must clearly state all the results that you use in your proof
- You can give any valid proof. You do not have to give the same proof as in the book or lectures.
- The proofs must contain all the details, including those that were left as exercises in the book or lecture.
- Below is a complete list of possible results that might appear on the final

1. (Lemma 2.3.1) Let G be a group. Then
   (a) The identity element of G is unique.
   (b) Every $a \in G$ has a unique inverse in G.
   (c) For every $a \in G$, we have $(a^{-1})^{-1} = a$.
   (d) For all $a, b \in G$, we have $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.
2. (Lemma 2.3.2) Let G be a group, and $a, b \in G$. Then the equation $a \cdot x = b$ has a unique solution in G.
3. (Lemma 2.4.1) A nonempty subset of the group G is a subgroup if and only if
   (a) $a, b \in H$ implies that $ab \in H$,
   (b) $a \in H$ implies that $a^{-1} \in H$.
4. (Lemma 2.4.2) If H is a nonempty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.
5. (Lemma 2.4.5 and Theorem 2.4.1) Let H be a subgroup of a group G.
   (a) There is a bijection between any two right cosets of H in G.
   (b) If G is a finite, then $o(H)$ divides $o(G)$.
6. (Corollary 1 on page 43) If G is a finite group and $a \in G$, then $o(a) \mid o(G)$.

7. (Corollary 5 on page 44) If G is a finite group whose order is a prime number p, then G is a cyclic group.

8. (Lemma 2.5.1) Let H, K be subgroups of a group G. Then HK is a subgroup G if and only if $HK = KH$.

9. (Theorem 2.5.1) Let H, K be fintie subgroups of a group G of orders $o(H)$ and $o(K)$. Then $o(HK) = \frac{o(H)o(K)}{o(H \cap K)}$.

10. (Lemma 2.6.2) The subgroup N of G is a normal subgroup of G if and only if every left coset of N in G is a right coset of N in G.

11. (Lemma 2.7.3) Let $G, \overline{G}$ be groups. If ϕ is a homomorphism of G into $\overline{G}$ with kernel K, then K is a normal subgroup of G.

12. (Theorem 2.7.1) Let $G, \overline{G}$ be groups. Let ϕ be a surjective homomorphism from G to $\overline{G}$ with kernel K. Then $G/K \approx \overline{G}$.

13. (Application 1 on page 61) Suppose G is a finite abelian group and $p \mid o(G)$, where p is a prime number. Then there is an element $a \neq e$ such that $a^p = e$.

14. (Lemma 2.8.2) $\mathcal{I}(G) \approx G/Z$, where $\mathcal{I}$ is the group of inner automorphisms of G, and Z is the center of G

15. (Theorem 2.9.1) Every group is isomorphic to a subgroup of $A(S)$ for some appropriate S.

16. (Pages 78-80)

    (a) Give a definition of an *even permutation*

    (b) Prove that the set of even permutations in S_n is an index-2 subgroup.

17. (Theorem 2.11.2) If G is a group, and $o(G) = p^n$ where p is a prime number, then $Z(G) \neq (e)$.

18. (Page 86) If $o(G) = p^2$ where p is a prime number, then G is abelian.

19. (Slightly easier form of Theorem 2.12.1) If G is a group, p is a prime number and $p^\alpha \mid o(G)$ and $p^{\alpha+1} \nmid o(G)$, then G has a subgroup of order p^α.

20. (The "only if" direction of Theorem 2.14.2) Let p be a prime number. Let G, G' be abelian groups of order p^n and $G = A_1 \times \cdots \times A_k$ and $G' = B_1 \times \cdots \times B_S$, where each A_i and B_i are cyclic of orders $o(A_i) = p^{n_i}$ and $o(B_i) = p^{H_i}$ satisfying $n_1 \geq \cdots \geq n_k > 0$ and $h_1 \geq \cdots \geq h_s > 0$. Then G and G' are isomorphic only if $k = s$ and for each i, $n_i = h_i$.

21. (Lemma 3.2.1 for rings with 1) If R is a ring with 1, then for all $a, b \in R$

    (a) $a0 = 0a = 0$

    (b) $a(-b) = (-a)b = -(ab)$

    (c) $(-a)(-b) = ab$

    (d) $(-1)a = -a$

22. (Fixed Lemma 3.2.2) Let R be a finite integral domain with at least two elements. Then R is a field.

23. (Part of Theorem 3.4.1) Let R and R' be rings and $\phi\colon R \to R'$ be a surjective ring homomorphism with kernel U. Then R' is isomorphic to R/U.
24. Let R be a commutative ring with unit element whose only ideals are (0) and R itself. Then R is a field.
25. (Theorem 3.7.1 + its corollary on page 144) Prove that every Euclidean ring is a principal ideal domain.
26. (Theorem 3.8.1) $J[i]$ is a Euclidean ring.
27. (Lemma 3.8.1.) Let p be a prime integer and suppose that for some integer c relatively prime to p we can find integers x and y such that $x^2 + y^2 = cp$. Then there exist integers a and b such that $p = a^2 + b^2$.
28. (Lemma 3.9.2) Let F be a field. Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$, then there exist two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.
29. (Lemma 3.10.1) If $f, g \in J[x]$ are both primitive polynomials, then fg is a primitive polynomial too.
30. (Lemma 3.11.4) Let R be a unique factorization domain, let F be its field of quotients. If $f \in R[x]$ is both primitive and irreducible as an element of $R[x]$, then it is irreducible as an element of $F[x]$. Conversely, if the primitive element of $f \in R[x]$ is irreducible as an element of $F[x]$, it is also irreducible as an element of $R[x]$.
31. (Theorem 5.1.1) Let K, L, F be fields. If L is a finite extension of K and if K is a finite extension of F, then $[L : F] = [L : K][K : F]$.
32. (Theorem 5.1.2) Let F be a subfield of K. Then $a \in K$ is algebraic over F if and only if $F(a)$ is a finite extension of F.
33. (Special case of Theorem 5.1.4) Let F be a subfield of K. If $a, b \in K$ are algebraic over F, then $a + b$ is algebraic over F.
34. (Theorem 5.1.5) If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.
35. (Problem 1 on page 219) Prove that e (the base of the natural logarithms) is irrational.
36. (Lemma 5.3.2) Let F be a field. A nonzero polynomial $f \in F[x]$ of degree n can have at most n roots in any extension of F.
37. (Simplified Theorem 5.3.1) Let F be a field. If $p(x)$ is a polynomial in $F[x]$ of degree $n \geq 1$ and is irreducible over F, then there exists an extension E of F in which $p(x)$ has a root.
38. (Theorem 5.3.2) Let F be a field, and $f(x) \in F[x]$ be of degree $n \geq 1$. Then there is an extension E of F of degree at most $n!$ in which $f(x)$ splits into linear factors.
39. (Lemma 5.5.2) Let F be a field. The polynomial $f(x) \in F[x]$ has a multiple root if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree.
40. (Theorem 5.5.1) If F is a field of characteristic 0 and if a, b are algebraic over F, then there exists an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.