Math 206B: Algebra
Midterm 1: Things to Know

This document builds on something I wrote up at the end of Math 206A. I will give a list of key definitions to know followed by some important results to know.

1 Ring Theory Basics

1.1 Definitions

1. Ring;
2. Field;
3. Division Ring/Skew Field;
4. Zero Divisor;
5. Unit;
6. Integral Domain;
7. Commutative Ring;
8. Unital Ring (Ring with Identity);
9. Subring;
10. Quotient Ring;
11. Left Ideal, Right Ideal, (Two-Sided) Ideal;
12. Ring Homomorphism;
13. Kernel and Image of a Ring Homomorphism;
14. The sum and product of ideals;
15. Ideal Generated by a Set;
16. Principal Ideal;
17. Maximal Ideal;
18. Prime Ideal;
19. Ring of Fractions;
20. Field of Fractions;

21. The Subfield Generated by a Subset;
22. Comaximal Ideals;
23. Norm;
24. Euclidean Domain;
25. Discrete Valuation;
26. Greatest Common Divisor;
27. Principal Ideal Domain;
28. Irreducible Element;
29. Prime Element;
30. Unique Factorization Domain;
31. Associates;
32. Ascending Chain Condition on Ideals;
33. Noetherian Ring.

1.2 Examples

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
2. $\mathbb{Z}/n\mathbb{Z}$;
3. Rings of Functions;
4. Real (Hamilton) Quaternions;
5. Quadratic Fields $\mathbb{Q}(\sqrt{D})$ and Quadratic Integer Rings. Norms in Quadratic Fields and Quadratic Integer Rings.
6. Polynomial Rings $R[x], R[x_1, \ldots, x_n],\ R[x_1, x_2, \ldots]$;
7. Matrix Rings $M_n(R)$;
8. Example of an ideal that is not principal;
9. Example of an ideal that is not finitely generated;
10. Example of a prime ideal that is not maximal;
11. Example of an irreducible element that is not prime;
12. Example of an integral domain that is not a UFD;
13. Examples of Rings of Fractions, $\mathbb{Z} \to \mathbb{Q},\ \mathbb{Z}[x] \to \mathbb{Q}(x)$;
14. Examples of Euclidean Domains, $\mathbb{Z},\ F[x],\ \mathbb{Z}[i]$.

1.3 Theorems

1. Let $a, b, c \in R$ with a not a zero divisor. If $ab = ac$ either $a = 0$ or $b = c$. If R is an integral domain, then $ab = ac$ implies $a = 0$ or $b = c$.

2. A finite integral domain is a field.

3. The units in $R[x]$ are the units of R. R is an integral domain if and only if $R[x]$ is an integral domain.

4. If R is a ring and I is an ideal of R, then the quotient group R/I is a ring with multiplication operation $(r + I) \cdot (s + I) = rs + I$. Conversely, if I is an additive subgroup of R such that the operation above is well-defined, then I is an ideal of R.

5. The kernel of a ring homomorphism is an ideal. Every ideal I is the kernel of the natural projection homomorphism from R to R/I.

6. Isomorphism Theorems for Rings (1st, 2nd, 3rd, 4th).

7. A commutative ring R with identity $1 \neq 0$ if a field if and only if R has no nonzero proper ideals.

8. In a commutative ring R with identity $1 \neq 0$, every proper ideal is contained in a maximal ideal. (Proof used Zorn's lemma.)

9. In a commutative ring R with identity $1 \neq 0$, if M is an ideal of R then M is maximal if and only if R/M is a field.

10. In a commutative ring R with identity $1 \neq 0$, if P is an ideal of R then P is prime if and only if R/P is an integral domain.

11. In a commutative ring R with identity $1 \neq 0$, every maximal ideal is prime.

12. Theorem 15 in Section 7.5 (on the existence of the rings of fractions);

13. The Chinese Remainder Theorem and its consequences for the ring $\mathbb{Z}/n\mathbb{Z}$.

14. Every Euclidean Domain is a PID.

15. Greatest common divisors in a Euclidean domain can be computed algorithmically (Theorem 4 in Section 8.1).

16. Every nonzero prime ideal in a PID is maximal.

17. If R is a commutative ring such that $R[x]$ is a PID then R is a field.

18. In an integral domain, a prime element is always irreducible.

19. In a PID a nonzero element is prime if and only if it is irreducible.

20. In a UFD a nonzero element is prime if and only if it is irreducible. (This implies the previous result.)

21. Given two elements of a UFD that are factored into products of irreducible elements, it is easy to compute their gcd (Proposition 13 Sec. 8.3).

22. Every ideal of R is finitely generated if and only if R satisfies the Ascending Chain Condition on Ideals.

23. Every PID is a UFD.

24. Fermat's Theorem on the sum of two squares and the description of irreducible elements in $\mathbb{Z}[i]$ (Proposition 18 Sec. 8.3).

25. The description of positive integers that can be written as a sum of two squares.
The number of ways that such an integer can be written as a sum of two squares. (Corollary 19 Sec. 8.3).

26. The comparison of $R[x]/(I)$ and $(R/I)[x]$, 'Reducing the coefficients modulo I'. (Proposition 2 Sec. 9.1)