Fall 2018, Math 320
Final Exam Cheat Sheet

You will receive a copy of this sheet with the midterm exam. **No other notes will be allowed.** Be sure to specify when you use one of the theorems lised here!

Theorem 1 (Division algorithm)**.** For any $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < b$ so that $a = qb + r$.

Theorem 2. Given $a, b, d \in \mathbb{Z}$, we have $(a, b) = d$ if and only if (i) $d \mid a$, (ii) $d \mid b$, and (iii) there exist $x, y \in \mathbb{Z}$ so that $d = ax + by$.

Theorem 3. For any $a, b, c \in \mathbb{Z}$, the following hold.

(a) If $c > 0$, then $c(a, b) = (ca, cb)$.

(b) For any $k \in \mathbb{Z}$, we have $(a, b) = (a, b + ka)$.

Theorem 4. An integer p is prime if and only if for every $a, b \in \mathbb{Z}$, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Theorem 5 (Fundamental theorem of arithmetic)**.** For any $n \in \mathbb{Z}$ with $n \neq 0, 1, -1$, there exist primes $p_1, \ldots, p_k$ with

$$n = p_1 p_2 \cdots p_k.$$

Moreover, this expression for n is unique: if $n = q_1 q_2 \cdots q_r$ for some primes $q_1, q_2, \ldots, q_r$, then $r = k$ and, after potentially reording $q_1, \ldots, q_r$, we have $p_i = q_i$ or $p_i = -q_i$ for every i.

Theorem 6. An integer is divisible by 9 if and only the sum of its digits is divisible by 9.

Theorem 7. Fix $n \geq 2$.

(a) The relation $a \equiv b \bmod n$ is an equivalence relation on $\mathbb{Z}$.

(b) For any $a, b \in \mathbb{Z}$, $[a]_n = [b]_n$ if and only if $a \equiv b \bmod n$.

(c) The set $\mathbb{Z}_n$ is a ring under the usual addition and multiplication of equivalence classes.

(d) If n is prime, then $\mathbb{Z}_n$ is a field. Otherwise, $\mathbb{Z}_n$ has zero-divisors.

Theorem 8. Suppose R is a ring and $S \subset R$ is a subset. Then $(S, +, \cdot)$ is a ring if and only if (i) S is closed under addition, (ii) S is closed under multiplication, (iii) $0_R \in S$, and (iv) for every $a \in S$, we have $-a \in S$.

Theorem 9. Suppose R is a ring.

(a) The additive identity $0_R \in R$ is unique.

(b) $0_R \cdot a = 0_R$ for all $a \in R$.

(c) Every element $a \in R$ has a unique additive inverse.

(d) If R has a multiplicative identity $1_R \in R$, then 1_R is the only multiplicative identity in R.

(e) If $a \in R$ is a unit, then a has a unique multiplicative inverse.

(f) If R is an integral domain and $a, b, c \in R$ satisfy $ab = ac$, then $b = c$.

(g) If $a \in R$ is a unit, then a is not a zero-divisor.

Theorem 10. If R and S are rings and $\phi : R \to S$ is a homomorphism, then the following hold.

(a) $\phi(0_R) = 0_S$.

(b) $\phi(-a) = -\phi(a)$ for all $a \in R$.

(c) If R has a unity $1_R \in R$ and ϕ is surjective, then S has unity and $\phi(1_R) = 1_S$.

(d) If R has a unity $1_R \in R$ and ϕ is surjective, then $\phi(a^{-1}) = (\phi(a))^{-1}$ for all units $a \in R$.

Theorem 11 (Division algorithm)**.** Fix a field F. For any $a(x), b(x) \in F[x]$ with $\deg b(x) > 0$, there exist unique $q(x), r(x) \in F[x]$ with $\deg r(x) < \deg b(x)$ so that $a(x) = q(x)b(x) + r(x)$.

Theorem 12. Fix a field F. Given $a(x), b(x), d(x) \in F[x]$, we have $\gcd(a(x), b(x)) = d(x)$ if and only if (i) $d(x) \mid a(x)$, (ii) $d(x) \mid b(x$, and (iii) there exist $u(x), v(x) \in F[x]$ so that $d(x) = a(x)u(x) + b(x)v(x)$.

Theorem 13. Fix a field F. For any $a(x) \in F[x]$ with $\deg a(x) > 0$, there exist irreducible polynomials $g_1(x), \dots, g_k(x) \in F[x]$ such that

$$a(x) = g_1(x)g_2(x)\cdots g_k(x).$$

Moreover, this expression for $a(x)$ is unique: if $a(x) = h_1(x)h_2(x)\cdots h_r(x)$ for some irreducible polynomials $h_1(x), h_2(x), \dots, h_r(x) \in F[x]$, then $r = k$ and, after potentially reording $h_1(x), \dots, h_r(x)$, we have, for each i, $g_i(x) = ch_i(x)$ for some constant $c \in F$.

Theorem 14 (Root Theorem)**.** Fix a field F, an element $r \in F$, and a polynomial $a(x) \in F[x]$. We have $(x - r) \mid a(x)$ if and only if r is a root of $a(x)$.

Theorem 15. Fix a ring R and elements $r_1, \dots, r_k \in R$. The set

$$\langle r_1, \dots, r_k \rangle = \{t_1 r_1 + t_2 r_2 + \cdots + t_k r_k : t_1, \dots, t_k \in R\}$$

is an ideal in R. Note: as a special case, $\langle r \rangle = \{tr : t \in R\}$ is an ideal of R.

Theorem 16. Fix a ring R and an ideal $I \subset R$.

(a) The relation $r \equiv t \bmod I$ is an equivalence relation on R.

(b) For any $r, t \in R$, $[r] = [t]$ in R/I if and only if $r \equiv t \bmod I$.

(c) The set R/I is a ring under the usual addition and multiplication of equivalence classes.

Theorem 17. Fix a field F and a polynomial $p(x) \in F[x]$ with $\deg p(x) \geq 1$. If $p(x)$ is irreducible, then $F[x]/\langle p(x) \rangle$ is a field. Otherwise, $F[x]/\langle p(x) \rangle$ has zero-divisors.

Theorem 18. If R and S are rings and $\varphi : R \to S$ is a homomorphism, then the kernel $\ker(\varphi)$ is an ideal of R.

Theorem 19 (First Isomorphism Theorem)**.** If R and S are rings and $\varphi : R \to S$ is a surjective homomorphism, then $R/\ker(\varphi) \cong S$.

Theorem 20. Every permutation can be written as a product of disjoint cycles, and as a product of (not necessarily disjoint) 2-cycles.

Theorem 21. Every finite group G with $|G| = n$ is isomorphic to a subgroup of S_n.