Midterm I review sheet: Math 412, Winter 2014

Principle of Mathematical Induction: Let $\{P(n)\}_{n\in\mathbb{N}}$ be a family of mathematical statements indexed by the natural numbers $\mathbb{N}$. If $P(0)$ is true and $P(k+1)$ is true whenever $P(k)$ is true, then $P(n)$ is true for all $n \in \mathbb{N}$.

Well-ordering axiom: Every non-empty subset of the set of non-negative integers contains a smallest element.

The Division algorithm: Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$. (q is the **quotient** and r is the **remainder**.)

Definition: Let a and b be integers with $b \neq 0$, we say that b **divides** a, and write $b \mid a$ if $a = bc$ for some integer c.

Defiinition: If a and b are integers, not both 0, then the **greatest common divisor** of a and b, written (a, b), is the largest integer which divides both a and b, i.e. $d = (a, b)$ if

(1) $d \mid a$ and $d \mid b$, and
(2) if $c \mid a$ and $c \mid b$, then $c \leq d$.

Theorem 1.2: If a and b are integers, not both zero, then there exist integers u and v so that $(a, b) = au + bv$.

Corollary 1.3: If a and b are integers, not both zero, and d is a positive integer, then $d = (a, b)$ if and only if

(1) $d \mid a$ and $d \mid b$, and
(2) if $c \mid a$ and $c \mid b$, then $c \mid d$.

Corollary 1.4: If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Definition: An integer p is **prime** if $p \neq 0, \pm 1$ and its only divisors are ± 1 and $\pm p$.

Theorem 1.5: Suppose that p is a integer with $p \neq 0, \pm 1$. Then p is prime if and only if whenever $p \mid bc$ then $p \mid b$ or $p \mid c$.

Corollary 1.6: If p is prime and $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some a_i.

Theorem 1.8: Every integer n, except $0, \pm 1$, can be written as a product of primes. Moreover, if

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

where each p_i and each q_j is prime, then $r = s$ and, after re-ordering, $p_i = \pm q_i$ for all $i \in \{1, \ldots, r\}$.

Definition: If $a, b, n \in \mathbb{Z}$ and $n > 1$, then we say a is **congruent to** b (modulo n), and write $a \equiv b (mod\ n)$, if $n \mid b - a$.

Theorem 2.1: If $a, b, c, n \in \mathbb{Z}$ and $n > 1$, then

(1) $a \equiv a (mod\ n)$,
(2) if $a \equiv b (mod\ n)$, then $b \equiv a (mod\ n)$, and
(3) if $a \equiv b (mod\ n)$ and $b \equiv c (mod\ n)$, then $a \equiv c (mod\ n)$.

Definition: If $a, n \in \mathbb{Z}$ and $n > 1$, then the **congruence class of** a **modulo** n is the set of all integers that are congruent to a modulo n, i.e.

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a (mod\ n)\}.$$

Theorem 2.3: $a \equiv c (mod\ n)$ if and only if $[a] = [c]$.

Corollary 2.4: Two congruence classes modulo n are either disjoint or identical.

Corollary 2.5: Suppose that $n > 1$ is an integer and consider congruence classes modulo n. Then

(1) If a is an integer and r is its remainder when divided by n, then $[a] = [r]$.
(2) There are exactly n congruence classes, namely $[0], [1], \ldots, [n-1]$.

Definition: If $n > 1$ is an integer, let $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ and define the operations $[a] \oplus [b] = [a \oplus b]$ and $[a] \odot [b] = [ab]$.

Definition: A **ring** is a non-empty set with two operations satisfying the following 8 axioms for all $a, b, c \in R$.

(1) $a + b \in R$
(2) $a + (b + c) = (a + b) + c$
(3) $a + b = b + a$
(4) There exists $0_R \in R$ so that $a + 0_R = a = 0_R + a$ for all $a \in R$.
(5) For each $a \in R$, the equation $a + x = 0_R$ has a solution in R.
(6) $ab \in R$
(7) $a(bc) = (ab)c$
(8) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Defiintions: A **commutative ring** is a ring such that

(9) $ab = ba$ for all $a, b \in R$.

Definition: A **ring with identity** is a ring such that there exists $1_R \in R$ so that

(10) $a1_R = a = 1_R a$ for all $a \in R$.

Theorem 2.7: If $n > 1$ is an integer, then $\mathbb{Z}_n$ is a commutative ring with identity.

Definition: If R and S are rings and $R \times S = \{(r, s) \mid r \in R,\ s \in S\}$ then we define two operations on $R \times S$ by $(r, s) + (r', s') = (r + s, r' + s')$ and $(r, s)(r', s') = (rr', ss')$ for all $(r, s), (r', s') \in R \times S$.

Theorem 3.1: If R and S are rings, then $R \times S$ is a ring. If both R and S are commutative, then $R \times S$ is commutative and if both R and S have identities then $(1_R, 1_S)$ is an identity for $R \times S$.

Theorem 3.3: If $a \in R$ and R is a ring, then $a + x = 0_R$ has a unique solution.

Definition: If $a \in R$, we define $-a$ to be the unique solution of $a + x = 0_R$ and, if $a, b \in R$, we define $a - b = a + (-b)$.

Theorem 3.4: If $a, b, c \in R$, R is a ring and $a + b = a + c$, then $b = c$.

Theorem 3.5: If $a, b \in R$ and R is a ring, then

(1) $a0_R = 0_R = 0_R a$. In particular, $0_R 0_R = 0_R$.
(2) $a(-b) = -ab = (-a)b$
(3) $-(-a) = a$
(4) $-(a + b) = (-a) + (-b)$
(5) $-(a - b) = -a + b$
(6) $(-a)(-b) = ab$
(7) If R has an identity, $(-1_R)a = -a$.

Definition: A non-empty subset S of a ring R is a **subring** if S is a ring (with the restrictions of the operations of R.)

Theorem 3.2: Suppose that R is a ring and S is a subset of R, then S is a subring of R if the following four conditions hold:

(1) S is closed under addition (i.e. if $a, b \in S$, then $a + b \in S$), and
(2) S is closed under multiplication (i.e. if $a, b \in S$, then $ab \in S$).
(3) $0_R \in S$, and
(4) If $a \in S$, then $a + x = 0_R$ has a solution in S.

Theorem: 3.6: A non-empty subset S of a ring R is a subring of R if

(1) S is closed under subtraction (i.e. if $a, b \in S$, then $a - b \in S$), and
(2) S is closed under multiplication (i.e. if $a, b \in S$, then $ab \in S$).

Definition: A commutative ring R with identity $1_R \neq 0_R$ is an **integral domain** if
(11) If $ac = 0_R$ in R, then $a = 0_R$ or $c = 0_R$.

Definition: A commutative ring R with identity $1_R \neq 0_R$ is a **field** if
(12) If $a \neq 0_R$ in R, then the equation $ax = 1_R$ has a solution in R.

Theorem 2.8: If $p > 1$ is an integer, then the following are equivalent:

(1) p is prime.
(2) $\mathbb{Z}_p$ is an integral domain.
(3) $\mathbb{Z}_p$ is a field.

Definition: A non-zero element a of a ring R is a **zero divisor** if there exists a non-zero element c of R so that $ac = 0_R$ or $ca = 0_R$.

Definition: An element a of a ring R is a **unit** if there exists $u \in R$ so that $au = 1_R = au$, in which case we write $u = a^{-1}$.

Theorem 2.9: If $n > 1$ is an integer, then $[a]$ is a unit in $\mathbb{Z}_n$ if and only if $(a, n) = 1$.

Theorem 3.7: If R is an integral domain, $a \neq 0_R$ and $ab = ac$ then $b = c$.

Theorem 3.8: Every field is an integral domain.

Theorem 3.9: Every finite integral domain is a field.

Definition: A function $f : R \to S$ between rings is an **isomorphism** if

(1) f is injective,
(2) f is surjective, and
(3) $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$.

Definition: A function $f : R \to S$ between rings is a **homomorphism** if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$.

Theorem 3.10: If $f : R \to S$ is an homomorphism of rings, then

(1) $f(0_R) = 0_S$,
(2) $f(-a) = -f(a)$ for all $a \in R$,
(3) $f(a - b) = f(a) - f(b)$ for all $a, b \in R$, and
If R is a ring with identity and f is surjective, then
(4) S is a ring with identity $f(1_R)$, and
(5) If u is a unit in R, then $f(u)$ is a unit in S and $f(u)^{-1} = f(u^{-1})$.

Corollary 3.11: If $f : R \to S$ is a homomorphism of rings, then the image of f is a subring of S. (The image $Im(f)$ of f is $Im(f) = \{s \in S \mid s = f(r) \text{ for some } r \in S\}$.)

Fact: If $f : R \to S$ is an isomorphism of rings, then $f^{-1} : S \to R$ is an isomorphism of rings.