Math 412. Definitions and Theorems.
Professor Karen E. Smith[1]

These are the main definitions and theorems for Math 412 that you must **memorize** *to be successful in the class. Please be aware that there are some slight differences with the textbook. I will point out when this happens with a footnote.* **For full credit on Exams, Homework, and Quizzes, you must state the definitions exactly as in this document.**

1. Chapter 1

THEOREM 1.1: THE DIVISION ALGORITHM IN $\mathbb{Z}$. *Let $n, d \in \mathbb{Z}$, with $d > 0$. Then there exist* **unique** *integers q, r such that $n = qd + r$ where $0 \leq r < d$.*

DEFINITION: Let $n, d \in \mathbb{Z}$. We say d **divides** n and write $d|n$ if there exists an integer k such that $n = kd$.

DEFINITION: The **greatest common divisor** or **gcd** of two integers a, b (not both zero) is the largest integer d such that $d|a$ and $d|b$.

DEFINITION: Two integers a and b are **relatively prime** if their greatest common divisor is 1.

THEOREM 1.2: Let a and b be integers, not both zero, and let d be their greatest common divisor. Then there exist $r, s \in \mathbb{Z}$ such that $ra + sb = d$. (Indeed, d is the *smallest* positive integer which is a $\mathbb{Z}$-linear combination of a and b.)

ANOTHER IMPORTANT TECHNIQUE: You should know the **Euclidean algorithm**, which is a method to find the gcd of two integers. It can also be used to find a specific pair of numbers r, s such that $ra + sb$ is $\gcd(a, b)$. This is helpful for finding the multiplicative inverse of $[d]$ in $\mathbb{Z}_n$. There is also a Euclidean algorithm for polynomials (Chapter 4).

DEFINITION: A integer $p \pm 1$ is **prime** if its only divisors are ± 1 and $\pm p$.

THEOREM 1.5: Let p be a prime integer, and $a, b \in \mathbb{Z}$ arbitrary. If $p|(ab)$, then $p|a$ or $p|b$.

Conversely, suppose an integer $p \neq 1$ has the property that *whenever $p|(ab)$, then $p|a$ or $p|b$.* Then p is prime.

THEOREM 1.8. THE FUNDAMENTAL THEOREM OF ARITHMETIC: An integer $n \neq 0, \pm 1$ can be written as a product of primes; Moreover, if

$$p_1 \cdots p_s \text{ and } q_1 \cdots q_t$$

are two factorizations of n into primes, then, $s = t$ and there exists a reordering of the $\{q_j\}$ such that $q_i = \pm p_i$ for all i.

[1]With the Assistance of Graham Bader, proofreader extraordinaire.

2. CHAPTER 2

DEFINITION: Fix a non-zero integer N. We say that $a, b \in \mathbb{Z}$ are **congruent modulo** N if $N|(a-b)$. We write $a \equiv b \mod N$.

This definition is equivalent to "a is congruent to b modulo I" where $I \subset \mathbb{Z}$ is the ideal generated by (N). See Chapter 6.

THEOREM 2.2: Fix a non-zero integer N. For $a, b, c, d \in \mathbb{Z}$,

(1) If $a \equiv b \mod N$ and $c \equiv d \mod N$, then $(a+c) \equiv (b+d) \mod N$.
(2) If $a \equiv b \mod N$ and $c \equiv d \mod N$, then $(a \cdot c) \equiv (b \cdot d) \mod N$.

DEFINITION: Fix a non-zero integer N. For $a \in \mathbb{Z}$, the **congruence class of** a **modulo** N is the subset of $\mathbb{Z}$ consisting of all integers congruent to a modulo N; That is, the **congruence class of** a **modulo** N is

$$[a]_N := \{b \in \mathbb{Z} \mid b \equiv a \mod N\} = \{a + Nk \mid k \in \mathbb{Z}\}.$$

Note here that $[a]_N$ is the **notation** for this congruence class— in particular, $[a]_N$ stands for a *subset of* $\mathbb{Z}$, not a number.

DEFINITION: The notation $\mathbb{Z}_n$ denotes the **ring** of **congruence classes modulo** n. The addition and multiplication are defined by

$$[a]_n + [b]_n = [a+b]_n \qquad [a]_n \cdot [b]_n = [a \cdot b]_n$$

The addition and multiplication in $\mathbb{Z}_n$ are well-defined because of Theorem 2.2.

Another way to express Theorem 2.2 is

THEOREM: Fix a non-zero integer N. The canonical mapping

$$\mathbb{Z} \to \mathbb{Z}_N \qquad x \mapsto [x]_N$$

is a **ring homomorphism.**

COROLLARY 2.5: Fix a non-zero integer N. Two integers a and b are in the same congruence class modulo N if and only if they have the same remainder after dividing by N. So there are exactly N elements in $\mathbb{Z}_N$:

$$[0]_N, [1]_N, \ldots, [N-1]_N,$$

one for each remainder.

THEOREM: 2.8 The ring $\mathbb{Z}_n$ is a field if and only if n is prime. The ring $\mathbb{Z}_n$ is a domain if and only if n is prime.

THEOREM 2.10: The element $[d]$ is a unit in the ring $\mathbb{Z}_n$ if and only if the gcd of d and n is 1.

3. CHAPTER 3

DEFINITION: A *ring* is a non-empty set R with two binary operations, denoted "$+$" and "$\times$," such that

- $+$ and $\times$ are both associative,
- $+$ is commutative,
- $+$ has an identity, which we denote 0_R; this means $r + 0_R = x$ for all $r \in R$.
- Every element of R has an inverse for the operation $+$; this means that for all $r \in R$, there exists $s \in R$ such that $r + s = 0_R$.
- $\times$ has an identity,[2] denoted 1_R;
- The two operations are related by the *distributive properties*: $a \times (b+c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$.

NOTATION: For any element $r \in R$, we write $-r$ for the additive inverse of r.

DEFINITION: In any ring R, we define subtraction $s - r$ by $s + (-r)$ for all $r, s \in R$.

DEFINITION: Let R be a ring. An element $r \in R$ is a **unit** if it has a multiplicative inverse; that is r is a unit if there exists an element $s \in R$ such that $rs = 1_R$ and $sr = 1_R$.
NOTATION: We write r^{-1} for the multiplicative inverse of r *when it exists.*

DEFINITION: A **subring**[3] of a ring R is a subset S which contains 1_R, and is closed under $+$, $\times$, and $-$. Equivalently, a subring is a subset which is itself a ring with the same 1 (using the binary operations $+$ and $\times$ from R).[4]

DEFINITION: An **integral domain** (or just **domain**) is a commutative ring R with $1_R \neq 0_R$ which satisfies the additional axiom: *if* $xy = 0$*, then* x *or* $y = 0$ *for all* $x, y \in R$.

DEFINITION: A **field** is a commutative ring with $1_R \neq 0_R$ such that every non-zero element has a multiplicative inverse.

DEFINITION: A map of rings $R \xrightarrow{\phi} S$ is a **homomorphism** if it satisfies the following three conditions:

(1) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ for all $r_1, r_2 \in R$;
(2) $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$ for all $r_1, r_2 \in R$; and
(3) $\phi(1_R) = 1_S$.[5]

We showed on a previous worksheet that these conditions imply also that $\phi(0_R) = 0_S$ as well.

DEFINITION: A **ring isomorphism** is a bijective ring homomorphism. We say that two rings R and S are **isomorphic** if there is an isomorphism $R \xrightarrow{\phi} S$ between them.

You should think of a ring isomorphism as a renaming of the elements of a ring, so that two isomorphic rings are "the same ring" if you just change the names of the elements. An important feature of ring isomorphisms is that all the ring structure is preserved: the units must correspond to the units, the nilpotents to the nilpotents, and so on.

---

[2]This axiom is omitted in the book's definition. They use the term "ring with identity" for what we call "ring".

[3]This is different from the book, since the book does not require the existence of a multiplicative identity.

[4]Although it is not obvious, you can check a subset of R is a subring by checking only that it contains 1_R, and is closed under $\times$ and $-$. Try to prove it! If you get stuck, look at Theorem 3.6 in the book.

[5]The book leaves out this third condition because they leave out the 1 in the definition of ring.

4. CHAPTER 4

THEOREM 4.3: Let R be any ring. The polynomial ring $R[x]$ is a domain if and only if R is a domain.

THEOREM 4.5: For any domain R, the **units** in $R[x]$ are the units in the subring R of constant polynomials. In particular, if $\mathbb{F}$ is a field, then the units in $\mathbb{F}[x]$ are the non-zero constant polynomials.

THEOREM 4.6: THE DIVISION ALGORITHM FOR POLYNOMIALS. Fix a field $\mathbb{F}$. Let $f, d \in \mathbb{F}[x]$, where $d \neq 0$. There there exist **unique** polynomials $q, r \in \mathbb{F}[x]$ such that

$$f = qd + r \quad \text{where } r = 0 \text{ or } \deg(r) < \deg(d).$$

DEFINITION: Fix a field $\mathbb{F}$. Fix $f, g \in \mathbb{F}[x]$. We say "f divides g" and write $f|g$ if there exists $h \in \mathbb{F}[x]$ such that $g = fh$.

Saying $f|g$ is the same as saying $g \in (f)$, the ideal of $\mathbb{F}[x]$ generated by (f). See Chapter 6.

DEFINITION: Fix a field $\mathbb{F}$. A polynomial $f \in \mathbb{F}[x]$ is **irreducible** if it can not be factored into polynomials of *lower degree*.[6] **Caution:** We can always factor $f = (\lambda f)(\frac{1}{\lambda})$ where $\lambda \in \mathbb{F} \setminus \{0\}$, so the lower degree of the factors is important.

DEFINITION: Fix $f, g \in \mathbb{F}[x]$. The **greatest common divisor** of f and g is the *monic* polynomial of *largest degree* which divides both f and g.

THEOREM 4.8: Let $\mathbb{F}$ be a field. In $\mathbb{F}[x]$, the greatest common divisor of two polynomials f and g is an $\mathbb{F}[x]$-linear combination of f and g. In fact, it is the *monic polynomial of smallest degree* which is an $\mathbb{F}[x]$-linear combination of f and g.

THEOREM 4.12 Let $\mathbb{F}$ be a field. In $\mathbb{F}[x]$, a polynomial $p(x)$ is irreducible if and only if it satisfies the following property: whenever $p|(fg)$ for some $f, g \in \mathbb{F}[x]$, we have $p|f$ or $p|g$.

THEOREM 4.14: ANALOG OF FUNDAMENTAL THEOREM FOR POLYNOMIALS RINGS:
Let $\mathbb{F}$ be a field. Every $f \in \mathbb{F}[x]$ can be factored as

$$f = p_1 p_2 \cdots p_t$$

where each p_i is an irreducible polynomial in $\mathbb{F}[x]$. Moreover, this expression is unique up to re-ordering and multiplication by units (non-zero constants).

THEOREM 4.15: THE REMAINDER THEOREM: Let $\mathbb{F}$ be a field. Let $f \in \mathbb{F}[x]$ be an arbitrary polynomial. The remainder when f is divided by $(x - a)$ is the constant polynomial $f(a)$.

COROLLARY 4.16: THE FACTOR THEOREM: Let $\mathbb{F}$ be a field. Let $f \in \mathbb{F}[x]$ be an arbitrary polynomial. Then $(x - a)$ is a factor of f if and only if $f(a) = 0$.

COROLLARY 4.19: Let $\mathbb{F}$ be a field. A polynomial $f \in \mathbb{F}[x]$ of degree 2 or 3 is irreducible if and only if it has no roots in $\mathbb{F}$.

[6] The book defined irreducible polynomial in a different but equivalent way; see page 101. The proof that our definition is equivalent to theirs is Theorem 4.11 on page 101.

5. CHAPTER 5

DEFINITION: Let $\mathbb{F}$ be a field. Fix a non-zero polynomial $f \in \mathbb{F}[x]$. We say that $g, h \in \mathbb{F}[x]$ are **congruent modulo** f if $f|(g-h)$. We write $g \equiv h \mod f$.

This definition is equivalent to "g is congruent to h modulo I" where $I \subset \mathbb{F}[x]$ is the ideal generated by (f). See Chapter 6.

THEOREM 5.2: Let $\mathbb{F}[x]$ be a field. Fix a polynomial $f \in \mathbb{F}[x]$. For $g_1, h_1, g_2, h_2 \in \mathbb{F}[x]$,

(1) If $g_1 \equiv h_1 \mod f$ and $g_2 \equiv h_2 \mod f$, then $(g_1 + g_2) \equiv (h_1 + h_2) \mod f$.
(2) If $g_1 \equiv h_1 \mod f$ and $g_2 \equiv h_2 \mod f$, then $(g_1 \cdot g_2) \equiv (h_1 \cdot h_2) \mod f$.

DEFINITION: Let $\mathbb{F}[x]$ be a field. Fix a polynomial $f \in \mathbb{F}[x]$. For a polynomial $g \in \mathbb{F}[x]$, the **congruence class of** g **modulo** f is the subset of $\mathbb{F}[x]$ consisting of all polynomials congruent to g modulo f; That is, the **congruence class of** g **modulo** f is

$$[g]_f := \{b \in \mathbb{F}[x] \mid b \equiv g \mod f\} = \{g + hf \mid h \in \mathbb{F}[x]\}.$$

Note here that $[g]_f$ is the **notation** for this congruence class. Another notation is $g + (f)$.

These congruence classes are the same as the congruence classes of g modulo I where $I \subset \mathbb{F}[x]$ is the ideal generated by f. See Chapter 6.

DEFINITION: The notation $\mathbb{F}[x]/(f)$ denotes the **ring** of **congruence classes modulo** f. The addition and multiplication are defined by

$$[g_1]_f + [g_2]_f = [g_1 + g_2]_f \qquad [g_1]_f \cdot [g_2]_f = [g_1 \cdot g_2]_f$$

The addition and multiplication in $\mathbb{F}[x]/(f)$ are well-defined because of Theorem 2.2.

Another way to express Theorem 5.2 is

THEOREM: Let $\mathbb{F}$ be a field. Fix a polynomial $f \in \mathbb{F}[x]$. The canonical mapping

$$\mathbb{F}[x] \to \mathbb{F}[x]/(f) \qquad g \mapsto [g]_f$$

is a **ring homomorphism.**

COROLLARY 5.5: Let $\mathbb{F}$ be a field. Fix a polynomial $f \in \mathbb{F}[x]$. Two polynomials g and h are in the same congruence class modulo f if and only if they have the same remainder after dividing by f.

COROLLARY: Let $\mathbb{F}$ be a field. Fix a polynomial $f \in \mathbb{F}[x]$ of degree d. Then each congruence class modulo f contains exactly one polynomial of degree $\leq d$.

Put differently, we can represent the elements of $\mathbb{F}[x]/(f)$ by

$$[a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}]_f$$

where $a_i \in \mathbb{F}$ and $d = \deg f$.

THEOREM 5.9: Let $\mathbb{F}$ be a field. Fix a polynomial $f \in \mathbb{F}[x]$. Then the congruence class $[g(x)]_f$ is a unit in $\mathbb{F}[x]/(f)$ if and only if $gcd(f, g) = 1$.

THEOREM 5.10: Let $\mathbb{F}$ be a field. Fix a non-constant polynomial $f \in \mathbb{F}[x]$. Then $\mathbb{F}[x]/(f)$ is a field if and only if f is irreducible. Also, $\mathbb{F}[x]/(f)$ is a domain if and only if f is irreducible.

6. CHAPTER 6

DEFINITION: An **ideal** of a ring R is a non-empty subset I satisfying[7]

(1) If $x_1, x_2 \in I$, then $x_1 + x_2 \in I$;
(2) If $x \in I$ and $r \in R$, then $rx \in I$ and $xr \in I$.

DEFINITION: Let I be an ideal in a ring R. A non-empty subset $\mathcal{S}$ of I is said to **generate** I if the ideal I is exactly the set of all R-linear combinations of the elements of S. In this case, the elements of S are said to be **generators** for I.

DEFINITION: An ideal I of a ring R is **principal** if it can be generated by one element.

NOTATION: We write $(s_1, \ldots, s_t)$ for the ideal of R generated by the set $\{s_1, \ldots, s_t\}$.

DEFINITION: Let I be an ideal of a ring R. We say that $x, y \in R$ are **congruent modulo** I if $x - y \in I$. Write $x \equiv y \mod I$.

AN ACCEPTABLE ABUSE OF NOTATION: If $I = (d)$ is a principal ideal of R, we also say "x and y are congruent modulo d." This is used in Chapter 2 (for $\mathbb{Z}$) and Chapter 5 (for $\mathbb{F}[x]$).

DEFINITION: Let I be an ideal of a ring R. The **congruence class of** y **modulo** I is the set

$$y + I := \{x \in R \,|\, x - y \in I\}$$

consisting of all elements of R that are congruent modulo I to y. [It would be natural to use the notation $[y]_I$ but no one does this.]

THEOREM 6.5: Let I be an ideal of a ring R. If $r_1 \equiv r_2 \mod I$ and $s_1 \equiv s_2 \mod I$, then

(1) $(r_1 + s_1) \equiv (r_2 + s_2) \mod I$.
(2) $(r_1 \cdot s_1) \equiv (r_2 \cdot s_2) \mod I$.

DEFINITION: Let I be an ideal of a ring R. The **Quotient Ring** of R by I is the set R/I consisting of all congruence classes modulo I in R, together with binary operations $+$ and $\cdot$ defined by

$$(x + I) + (y + I) := (x + y) + I \qquad (x + I) \cdot (y + I) := (x \cdot y) + I.$$

The addition and multiplication in R/I are well-defined because of Theorem 6.5.

Another way to express Theorem 6.5 is

THEOREM: Let R be any ring and any I any ideal of R. The canonical[8] mapping

$$R \to R/I \qquad r \mapsto r + I$$

is a **ring homomorphism.** It is **surjective** with kernel I.

DEFINITION: Let $R \xrightarrow{\phi} S$ be any ring homomorphism. The **kernel** of ϕ is the set

$$\ker \phi := \{r \in R \,|\, \phi(r) = 0\}.$$

[7] CAUTION: When reading the text, you will see an ideal defined as a certain kind of "subring". DO NOT USE THIS DEFINITION! Remember that for us, a subring always contains 1, because all rings contain 1. But most ideals do not contain 1.

[8] The book calls this the "natural homomorphism." Both terms are in use.

THEOREM 6.10: The kernel of a ring homomorphism is an ideal (of the source ring).

THEOREM 6.11: A ring homomorphism $R \xrightarrow{\phi} S$ is injective if and only if $\ker \phi = 0$.

THEOREM 6.13: NOETHER'S FIRST ISOMORPHISM THEOREM: *Let $R \xrightarrow{\phi} S$ be a surjective homomorphism of rings. Let I be the kernel of ϕ. Then R/I is isomorphic to S.*

In reading the definitions from the first half of the course, observe that there is some repetition. There is less to memorize than it would appear, if you take the time to understand.

One theme is the similarity of the ring $\mathbb{Z}$ and the ring $\mathbb{F}[x]$ where $\mathbb{F}$ is a field.

You should compare and contrast the definitions and theorems in Chapter 1 (divisibility, the division algorithm, factorization in $\mathbb{Z}$) with the definitions and theorems in Chapter 4 (divisibility, the division algorithm, factorization in $\mathbb{F}[x]$). Try to "match up" the definitions and theorems exactly.

Also compare and contrast the definitions and theorems in Chapter 2 (congruence and modular arithmetic $\mathbb{Z}$) with the definitions and theorems in Chapter 5 (congruence and modular arithmetic in $\mathbb{F}[x]$). How is $\mathbb{F}[x]/(f)$ "the same" as $\mathbb{Z}_n$? Try to match up all the theorems and definitions between Chapter 2 and Chapter 5. Try to compare computations in each setting. For example, in what sense is finding the units in $\mathbb{F}[x]/(f)$ "the same" as finding the units in $\mathbb{Z}_n$?

Finally, those four chapters on $\mathbb{Z}$ (and its quotient rings) and $\mathbb{F}[x]$ (and its quotient rings) are special cases of the General Ring theory covered in Chapters 3 and 6. For example, both the construction of $\mathbb{Z}_n$ and $\mathbb{F}[x]/(f)$ are special cases of the quotient ring construction R/I in Chapter 6. Compare the Theorems and see which ones in Chapters 1, 2, 4, or 5 are special cases of more general Theorems in Chapters 3 and 6.

However: not every theorem about $\mathbb{Z}$ and $\mathbb{F}[x]$ works in an arbitrary ring R. There are several special features of $\mathbb{Z}$ and $\mathbb{F}[x]$ which we may not have in general, such as commutativity. Crucially, both $\mathbb{Z}$ and $\mathbb{F}[x]$ have a **division algorithm** which allows us to develop a Euclidean algorithm, prove that all ideals are principal, and prove "essentially unique" factorization. None of these things hold in, say the ring $M_2(\mathbb{R})$ or $\mathcal{C}^0$.

7. CHAPTER 7

DEFINITION: An **group** is a non-empty set G with binary operation, denoted "$\circ$," which satisfies the axioms

- For all $g_1, g_2, g_3 \in G$, we have $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ (composition is associative).
- There exists an element $e \in G$ such that for all $g \in G$, we have $g \circ e = e \circ g = g$ (there exists an identity)
- For all $g \in G$, there exists $h \in G$ such that $g \circ h = h \circ g = e$ (every element has an inverse under $\circ$)

DEFINITION: An **abelian group** is a group G with one additional axiom

- For all $g_1, g_2 \in G$, we have $(g_1 \circ g_2) = (g_2 \circ g_1)$ ($\circ$ is commutative).

DEFINITION: A **subgroup** of a group $(G, \circ)$ is a subset H which is itself a group under $\circ$.

In practice, it is usually easier to prove a given subset is a subgroup using:

THEOREM: A subset H of a group $(G, \circ)$ is a subgroup H if it satisfies the following three properties:

(1) H is non-empty (usually it is easiest to check that $e_G \in H$.)
(2) If $h_1, h_2 \in H$, then $h_1 \circ h_2 \in H$.
(3) If $h \in H$, then $h^{-1} \in H$.

DEFINITION: A **group homomorphism** is a map $G \xrightarrow{\phi} H$ between groups that satisfies $\phi(g_1 \circ g_2) = \phi(g_1) \circ \phi(g_2)$.

REMARK: If $G \xrightarrow{\phi} H$ is a group homomorphism, then *it follows that* $\phi(e_G) = e_H$. [Prove it!.] Likewise, for a ring homomorphism $R \xrightarrow{\psi} S$, it follows from the fact that ring homomorphisms preserve addition that $\psi(0_R) = 0_S$. This jives with the fact that both R and S are groups under addition, and ψ is a group homomorphism from $(R, +)$ to $(S, +)$. HOWEVER: It does **not** follow from the definition of a ring homomorphism that $\psi(1_R) = 1_S$. This must be assumed as part of the definition.[9]

DEFINITION: An **isomorphism** of groups is a bijective homomorphism.

DEFINITION: The **kernel** of a group homomorphism $G \xrightarrow{\phi} H$ is the subset

$$\ker \phi := \{g \in G \mid \phi(g) = e_H\}.$$

THEOREM: A homomorphism of groups is injective if and only if its kernel is $\{e_G\}$.

8. GROUP ACTIONS

DEFINITION: Let X be any set and let G be any group. We say that the group G **acts on** X if there is a map

$$G \times X \to X \qquad (g, x) \mapsto g \cdot x,$$

satisfying the following two axioms:

(1) $h \cdot (g \cdot x) = (h \circ g) \cdot x$ for all $g, h \in G$ and all $x \in X$; and
(2) $e_G \cdot x = x$ for all $x \in X$.

Fix an action of a group G on a set X. Consider a point $x \in X$.

DEFINITION: The **orbit** of x is the subset of X

$$O(x) := \{g \cdot x \,|\, g \in G\} \subset X.$$

DEFINITION: The **stabilizer** of x is the subset of G

$$Stab(x) = \{g \in G \mid g(x) = x\}.$$

THE ORBIT-STABILIZER THEOREM: *If a finite group G acts on a set X, then for every $x \in X$, we have*

$$|G| = |O(x)| \times |Stab(x)|.$$

[9]The reason is that that prove that the identity is preserved uses the existence of inverses for each element; we have this for the additive structure, but not the multiplicative structure of rings.