ABSTRACT ALGEBRA DEFINITIONS

PAUL L. BAILEY

1. Set Theory Definitions

Definition 1. Let a and b be elements. The *ordered pair* (a, b) is the set

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Definition 2. Let A and B be sets. The *cartesian product* of A and B is

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Definition 3. Let A and B be sets. A *function* from A to B is a subset of $A \times B$, $f \subset A \times B$, such that

$$\text{for every } a \in A \text{ there exists a unique } b \in B \text{ such that } (a, b) \in f.$$

We write $f(a)$ to denote the unique element $b \in B$ such that $(a, b) \in f$, so $f(a) = b$.

The notation $f : A \to B$ means that f is a function from A to B.

The notation $f : a \mapsto b$ means that $f(a) = b$.

Definition 4. Let A and B be sets and let $f : A \to B$.

We say that f is *injective* if

$$f(a_1) = f(a_2) \text{ implies } a_1 = a_2$$

for all $a_1, a_2 \in A$.

We say that f is *surjective* if

$$\text{for every } b \in B \text{ there exists } a \in A \text{ such that } f(a) = b.$$

We say that f is *bijective* if f is injective and surjective.

Definition 5. Let A and B be sets and let $f : A \to B$.

Let $C \subset A$. The *image* of C under f is

$$f(C) = \{b \in B \mid b = f(c) \text{ for some } c \in C\}.$$

Let $D \subset B$. The *preimage* of D under f is

$$f^{-1}(D) = \{a \in A \mid f(a) \in D\}.$$

Definition 6. Let A be a set. A *relation* on A is a subset of $A \times A$, $R \subset A \times A$. We write $a_1 R a_2$ to mean $(a_1, a_2) \in R$.

Definition 7. Let $\sim$ be a relation on a set A. We say that $\sim$ is an *equivalence relation* if

- **(a)** $a \sim a$, for all $a \in A$ (reflexivity);
- **(b)** $a \sim b$ implies $b \sim a$, for all $a, b \in A$ (symmetry);
- **(c)** $a \sim b$ and $b \sim c$ implies $a \sim c$, for all $a, b, c \in A$ (transitivity).

Date: April 30, 2007.

Definition 8. Let X be a set. The *power set* of X, denoted $\mathcal{P}(X)$, is the set of all subsets of X:

$$\mathcal{P}(X) = \{A \mid A \subset X\}.$$

Definition 9. Let A be a set. A *partition* of A is a collection of subsets of A, $\mathcal{C} \subset \mathcal{P}(A)$, such that

- **(a)** $\cup\mathcal{C} = A$;
- **(b)** $C_1 = C_2$ or $C_1 \cap C_2 = \varnothing$, for all $C_1, C_2 \in \mathcal{C}$.

2. Number Theory Definitions

Definition 10. Let $m, n \in \mathbb{Z}$. We say that m *divides* n, and write $m \mid n$, if there exists $x \in \mathbb{Z}$ such that $mx = n$.

Definition 11. Let $m, n \in \mathbb{Z}$ be positive. The *greatest common divisor* of m and n is the unique $d \in \mathbb{Z}$, $d \geq 1$, such that

- **(a)** $d \mid m$ and $d \mid n$;
- **(b)** $e \mid m$ and $e \mid n$ implies $d \mid e$.

Definition 12. Let $m, n \in \mathbb{Z}$ be positive. The *least common multiple* of m and n is the unique $l \in \mathbb{Z}$, $l \geq 1$, such that

- **(a)** $m \mid l$ and $n \mid l$;
- **(b)** $m \mid k$ and $n \mid k$ implies $l \mid k$.

Definition 13. Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$. We say that a *is congruent to* b *modulo* n, and write $a \equiv b \pmod{n}$, if n divides $a - b$:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid (a - b).$$

3. Group Theory Definitions

Definition 14. Let A be a set. A *binary operation* $*$ on A is a function

$$* : A \times A \to A.$$

We write $a * b$ to mean $*(a, b)$.

Definition 15. A *group* is a set G together with a binary operation

$$\cdot : G \times G \to G$$

such that

- **(G1)** $g_1(g_2g_3) = (g_1g_2)g_3$ for all $g_1, g_2, g_3 \in G$ (associativity);
- **(G2)** $\exists 1 \in G$ such that $1 \cdot g = g \cdot 1 = g$ for all $g \in G$ (existence of an identity);
- **(G3)** $\forall g \in G\, \exists g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1$ (existence of inverses).

Let G be group. We say that G is *abelian* if

- **(G4)** $g_1g_2 = g_2g_1$ for all $g_1, g_2 \in G$ (commutativity).

Definition 16. Let G be a group. The *order* of G is $|G|$.

Definition 17. Let G be a group and let $H \subset G$.

We say that H is a *subgroup* of G, and write $H \leq G$, if

- **(S0)** H is nonempty;
- **(S1)** $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$;
- **(S2)** $h \in H \Rightarrow h^{-1} \in H$.

Definition 18. Let G be a group. We say that G is *cyclic* if there exists $g \in G$ such that $G = \{g^n \mid n \in \mathbb{Z}\}$. We call g a *generator* for G.

Definition 19. Let $g \in G$. The *order of* g, denoted $\mathrm{ord}(g)$, is the smallest positive integer $n \in \mathbb{Z}$ such that $g^n = 1$, if such an integer exists; otherwise, $\mathrm{ord}(g) = \infty$.

Definition 20. Let G and H be a groups. A *group homomorphism* from G to H is a function $\phi : G \to H$ such that

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \text{ for any } g_1, g_2 \in G.$$

A *monomorphism* is an injective homomorphism.
An *epimorphism* is a surjective homomorphism.
An *isomorphism* is a bijective homomorphism.
An *endomorphism* is a homomorphism $\phi : G \to G$.
An *automorphism* is an isomorphism $\phi : G \to G$.

Definition 21. Let $\phi : G \to H$ be a homomorphism.
The *kernel* of ϕ is the subset of G denoted by $\ker(\phi)$ and defined by

$$\ker(\phi) = \{g \in G \mid \phi(g) = 1_H\}.$$

Definition 22. Let G be a group and $H \leq G$. Let $g \in G$.
The *left coset* at g of H in G is the set

$$gH = \{gh \mid h \in H\}.$$

The *right coset* at g of H in G is the set

$$Hg = \{hg \mid h \in H\}.$$

The collection of left cosets of H in G, denoted G/H, is called the *left coset space* of H in G.

The collection of right cosets of H in G, denoted $G\backslash H$, is called the *right coset space* of H in G.

The *index* of H is G, denoted by $[G : H]$, is the cardinality of the left coset space of H in G:

$$[G : H] = |G/H|.$$

Definition 23. Let G be a group and $H \leq G$. We say that H is a *normal* subgroup, and write $H \triangleleft G$, if $gH = Hg$ for every $g \in G$.

4. Ring Theory Definitions

Definition 24. A *ring* is a set R together with a pair of binary operations

$$+ : R \times R \to R \quad \text{and} \quad \cdot : R \times R \to R,$$

called *addition* and *multiplication*, such that

(R1) $a + b = b + a$ for every $a, b \in R$;
(R2) $(a + b) + c = a + (b + c)$ for every $a, b, c \in R$;
(R3) there exists $0 \in R$ such that $a + 0 = a$ for every $a \in R$;
(R4) for every $a \in R$ there exists $-a \in R$ such that $a + (-a) = 0$;
(R5) $(ab)c = a(bc)$ for every $a, b, c \in R$;
(R6) there exists $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for every $a \in R$;
(R7) $a(b + c) = ab + ac$ for every $a, b, c \in R$;
(R8) $(a + b)c = ac + bc$ for every $a, b, c \in R$.

A *commutative ring* is a ring R satisfying

(R9) $ab = ba$ for every $a, b \in R$.

Definition 25. Let R be a commutative ring and let $a \in R$.
We say that a is *entire* if $ab = 0 \Rightarrow b = 0$ for every $b \in R$.
We say that a is *cancelable* if $ab = ac \Rightarrow b = c$ for every $b, c \in R$.
We say that a is *invertible* if there exists an element $a^{-1} \in R$ such that $aa^{-1} = 1$.
We say that a is a *zero divisor* if $a \neq 0$ and there exists $b \in R \smallsetminus \{0\}$ such that $ab = 0$.

Definition 26. Let R be a nonzero commutative ring.
We say that R is an *integral domain* if every nonzero element of R is entire.
We say that R is a *field* if every nonzero element of R is invertible.

Definition 27. Let R be a ring. A *subring* of R is a subset $S \subset R$ such that
(S0) $1 \in S$;
(S1) $a, b \in S \Rightarrow a + b \in S$;
(S2) $a \in S \Rightarrow -a \in S$;
(S3) $a, b \in S \Rightarrow ab \in S$.
If S is a subring of R, we write $S \leq R$.

Definition 28. Let R and S be rings. A *ring homomorphism* from R to S is a function $\phi : R \to S$ such that
(H0) $\phi(1_R) = 1_S$;
(H1) $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$;
(H2) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.
A bijective ring homomorphism is called a *ring isomorphism*. If there exists a ring isomorphism from R to S we say that R and S are *isomorphic*, and write $R \cong S$.
An isomorphism from a ring onto itself is called a *ring automorphism*.

Definition 29. Let R be a ring. An *ideal* of R is a subset $I \subset R$ such that
(I1) $a, b \in I \Rightarrow a + b \in I$;
(I2) $a \in I$ and $r \in R \Rightarrow ra, ar \in I$.
If I is an ideal of R, we write $I \triangleleft R$.

Department of Mathematics and CSCI, Southern Arkansas University
E-mail address: `plbailey@saumag.edu`