Supplement. Dr. Bob's Modern Algebra Glossary

Based on Fraleigh's *A First Course on Abstract Algebra*, 7th Edition, Sections 0 through IV.23

Abelian Group. A group $\langle G, * \rangle$ (or just "G" for short) is *abelian* if its binary operation is commutative.

Alternating Group. The subgroup of S_n consisting of the even permutations of n letters is the *alternating group* A_n *on* n *letters*.

Associative. A binary operation $*$ on a set S is *associative* if $(a*b)*c = a*(b*c)$ for all $a, b, c \in S$.

Automorphism of a Group. An isomorphism $\phi : G \to G$ of a group with itself is an *automorphism* of G.

Binary Algebraic Structure. A *binary algebraic structure* is an ordered pair $\langle S, * \rangle$ where S is a set and $*$ is a binary operation on S.

Binary Operation. A *binary operation* $*$ on a set S is a function mapping $S \times S$ into S. For each (ordered pair) $(a, b) \in S \times S$, we denote the element $*((a, b)) \in S$ as $a * b$.

Cartesian Product. Let A and B be sets. The set $A \times B = \{(a, b) \mid a \in A, b \in B\}$ is the *Cartesian product* of A and B. The *Cartesian product* of sets $S_1, S_2, \ldots, S_n$ of the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_i \in S_i$ for $i = 1, 2, \ldots, n$. This is denoted

$$\prod_{i=1}^{n} S_i = S_1 \times S_2 \times \cdots \times S_n.$$

Cayley Digraph/Graph. For a group G with generating set $\{a_1, a_2, \ldots, a_n\}$, define a *digraph* with *vertex set* V with the same elements as the elements of G. For each pair of vertices v_1 and v_2 define an *arc* (v_1, v_2) *of color* a_i if $v_1 a_i = v_2$. The totality of all arcs form the *arc set* A of the digraph. The vertex set V and arc set A together form a *Cayley digraph* for group G with respect to generating set $\{a_1, a_2, \ldots, a_n\}$.

Center of a Group. For group G, define the *center* of G as

$$Z(G) = \{z \in g \mid zg = gz \text{ for all } g \in G\}.$$

Characteristic of a Ring. If for a ring R there is $n \in \mathbb{N}$ such that $n \cdot a = 0$ for all $a \in R$ (remember that "$n \cdot a$" represents repeated addition), then the least such natural number is the *characteristic* of the ring R. If no such n exists, then ring R is of *characteristic* 0.

Closed. Let $*$ be a binary operation on set S and let $H \in S$. Then H is *closed* under $*$ if for all $a, b \in H$, we also have $a * b \in H$.

Commutator Subgroup. For group G, consider the set

$$C = \{aba^{-1}b^{-1} \mid a, b \in G\}.$$

C is the *commutator subgroup* of G.

Commutative Binary Operation. A binary operation $*$ on a set S is *commutative* if $a * b = b * a$ for all $a, b \in S$.

Commutative Ring. A ring in which multiplication is commutative (i.e., $ab = ba$ for all $a, b \in R$) is a *commutative ring*.

Complex Numbers. The *complex numbers* are $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i\sqrt{-1}\}$.

Cosets. Let H be a subgroup of a group G. The subset $aH = \{ah \mid h \in H\}$ of G is the *left coset* of H containing a. The subset $Ha = \{ha \mid h \in H\}$ is the *right coset* of H containing a.

Cycle. A permutation $\sigma \in S_n$ is a *cycle* if it has at most one orbit containing more than one element. The *length* of the cycle is the number of elements in its largest orbit.

Cyclic Notation. Let $\sigma \in S_n$ be a cycle of length m where $1 < m \leq n$. Then the *cyclic notation* for σ is

$$(a, \sigma(a), \sigma^2(a), \ldots \sigma^{m-1}(a))$$

where a is any element in the orbit of length m which results when $\{1, 2, \ldots, n\}$ is partitioned into orbits by σ.

Cyclic Subgroup Generated by an Element. Let G be a group and let $a \in G$. Then the subgroup $H = \{a^n \mid n \in \mathbb{Z}\}$ of G (of Theorem 5.17) is the *cyclic subgroup of G generated by a*, denoted $\langle a \rangle$.

Cyclotomic Polynomial. The polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-1} + \cdots + x^2 + x + 1$$

for prime p is the *pth cyclotomic polynomial*.

Decomposable Group. A group G is *decomposable* if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is *indecomposable*.

Dihedral Group. The nth *dihedral group D_n* is the group of symmetries of a regular n-gon. In fact, $|D_n| = 2n$.

Division Ring. Let R be a ring with unity $1 \neq 0$. An element $u \in R$ is a *unit* of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a *division ring* (or *skew field*).

Divisors of Zero. If a and b are two nonzero elements of a ring R such that $ab = 0$ then a and b are *divisors of* 0.

Equivalence Relation. An *equivalence relation* $\mathcal{R}$ on a set S is a relation on S such that for all $x, y, z \in S$, we have

(1) $\mathcal{R}$ is *reflexive*: $x \,\mathcal{R}\, x$,

(2) $\mathcal{R}$ is *symmetric*: If $x \,\mathcal{R}\, y$ then $y \,\mathcal{R}\, x$, and

(3) $\mathcal{R}$ is *transitive*: If $x \,\mathcal{R}\, y$ and $y \,\mathcal{R}\, z$, then $x \,\mathcal{R}\, x$.

Euler Phi-Function. For $n \in \mathbb{N}$, define $\phi(n)$ as the number of natural numbers less than or equal to n which are relatively prime to n. ϕ is the *Euler phi-function*.

Even and Odd Permutations. A permutation of a finite set is *even* or *odd* according to whether it can be expressed as a product of an even number of transpositions or the product of an odd number of transpositions.

Factor Group (Quotient Group). Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH) \cdot (bH) = (ab)H$ called the the *factor group* (or *quotient group*) of G by H.

Field. A *field* is a commutative division ring.

Function. A *function* ϕ mapping set X into set Y is a relation between X and Y such that each $x \in X$ appears as the first member of exactly one ordered pair $(x, y) \in \phi$. We write $\phi : X \to Y$ and for $(x, y) \in \phi$ we write $\phi(x) = y$. The *domain* of ϕ is the set X and the *codomain* of ϕ is Y. The *range* of ϕ is the set $\phi[X] = \{\phi(x) \mid x \in X\}$.

Generator of a Group. An element a of a group G *generates* G if $\langle a \rangle = G$. A group is *cyclic* if there is $a \in G$ such that $\langle a \rangle = G$.

Generating Set of a Group. Let G be a group and let $a_i \in G$ for $i \in I$. The smallest of G containing $\{a_i \mid i \in I\}$ is the *subgroup generated by the set* $\{a_i \mid i \in I\}$. This subgroup is defined as the intersection of all subgroups of G containing $\{a_i \mid i \in I\}$: $H = \cap_{i \in J} H_j$ where the set of all subgroups of G containing $\{a_i \mid i \in I\}$ is $\{H_j \mid j \in J\}$. If this subgroup is all of G, then the *set* $\{a_i \in i \in I\}$ *generates* G and the a_i are *generators* of G. If there is a finite set $\{a_i \mid i \in I\}$ that generates G, then G is *finitely generated*.

Greatest Common Divisor. Let $r, s \in \mathbb{N}$. The positive generator d of the cyclic group $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$ under addition is the *greatest common divisor* of r and s, denoted $\gcd(r, s)$.

Group. A *group* $\langle G, * \rangle$ is a set G and a binary operation on G such that G is closed under $*$ and

$\mathcal{G}_1$ For all $a, b, c \in G$, $*$ is *associative*:

$$(a * b) * c = a * (b * c).$$

$\mathcal{G}_2$ There is $e \in G$ called the *identity* such that for all $x \in G$:

$$e * x = x * e = x.$$

$\mathcal{G}_3$ For all $a \in G$, there is an *inverse* $a' \in G$ such that:

$$a * a' = a' * a = e.$$

Homomorphism of Groups. A map ϕ of a group G into a group G' is a *homomorphism* if for all $a, b \in G$ we have $\phi(ab) = \phi(a)\phi(b)$.

Homomorphism of Rings. For rings R and R', a map $\phi : R \to R'$ is a *homomorphism* if for all $a, b \in R$ we have:

1. $\phi(a + b) = \phi(a) + \phi(b)$, and

2. $\phi(ab) = \phi(a)\phi(b)$.

Identity Element. Let $\langle S, * \rangle$ be a binary structure. An element e of S is an *identity element* of $*$ if $e * s = s * e = e$ for all $s \in S$.

Image. Let $f : A \to B$ for sets A and B. Let $H \subset A$. The *image of set* H under f is $\{f(h) \mid h \in H\}$, denoted $f[H]$. The *inverse image* of B in A is $f^{-1}[B] = \{a \in A \mid f(a) \in B\}$.

Index of a Subgroup. Let H be a subgroup of group G. The number of left cosets of H in G (technically, the cardinality of the set of left cosets) is the *index* of H in G, denoted $(G : H)$.

Integers. The *integers* are $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Integral Domain. An *integral domain* D is a commutative ring with unity $1 \neq 0$ and containing no divisors of 0.

Isomorphism of Binary Algebraic Structures. Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary algebraic structures. An *isomorphism* of S with S' is a *one-to-one* function ϕ mapping S *onto* S' such that

$$\phi(x * y) = \phi(x) *' \phi(y) \text{ for all } x, y \in S.$$

We then say S and S' are *isomorphic* binary structures, denoted $S \simeq S'$.

Isomorphism of Rings. A *isomorphism* $\phi : R \to R'$ from ring R to ring R' is a homomorphism which is one to one and onto R'.

Kernel of a Homomorphism. Let $\phi : G \to G'$ be a homomorphism. The subgroup $\phi^{-1}(\{e'\}) = \{x \in G \mid \phi(x) = e'\}$ (where e' is the identity in G) is the *kernel* of ϕ, denoted $\mathrm{Ker}(\phi)$.

Least Common Multiple. For $r_1, r_2, \ldots, r_n \in \mathbb{N}$, the smallest element of $\mathbb{N}$ that is a multiple of each r_i for $i = 1, 2, \ldots, n$, is the *least common multiple* of the r_i, denoted $\mathrm{lcm}(r_1, r_2, \ldots, r_n)$.

Maximal Normal Subgroup. A *maximal normal subgroup* of a group G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M.

Modulus. For $z = a + bi \in \mathbb{C}$, define the *modulus* or *absolute value* of z as $|z| = \sqrt{a^2 + b^2}$.

Natural Numbers. The *natural numbers* are $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Normal Subgroup. A subgroup H of a group G is *normal* if its left and right cosets coincide. That is if $gH = Hg$ for all $g \in G$. Fraleigh simply says "H is a normal subgroup of G," but a common notation is $H \triangleleft G$.

Order of an Element. Let G be a group and $a \in G$. If G is cyclic and $G = \langle a \rangle$, then (1) if G is finite of order n, then *element a is of order n*, and (2) if G is infinite then *element a is of infinite order.*

Order of a Group. If G is a group, then the *order* $|G|$ of G is the number of elements in G.

One to One. A function $\phi : X \to Y$ is *one to one* (or an *injection*) if $\phi(x_1) = \phi(x_2)$ implies $x_1 = x_2$.

One-to-One Correspondence. A function that is both one to one and onto is called a *one-to-one correspondence* (or a *bijection*) between the domain and codomain.

Onto. The function ϕ is *onto* Y (or a *surjection*) if the range of ϕ is Y.

Partition. A *partition* of a set S is a collection of nonempty subsets of S such that every element of S is in exactly one of the subsets.

Permutation. A *permutation* of a set A is a function $\phi : A \to A$ that is both one-to-one and onto.

Polynomial over a Ring. Let R be a ring. A *polynomial* $f(x)$ with coefficients in R is an infinite formal series

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i. The a_i are *coefficients* of $f(x)$. If for some $i \geq 0$ it is true that $a_i \neq 0$, then the largest such value of i is the *degree* of $f(x)$. If all $a_i = 0$, then the degree of $f(x)$ is undefined. If $a_i = 0$ for all $i \in \mathbb{N}$, then $f(x)$ is called a *constant polynomial*. We denote the set of all polynomials with coefficients in R as $R[x]$.

Rational Numbers. The *rational numbers* are $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$.

Real Numbers. The *real numbers*, denoted $\mathbb{R}$, form a complete ordered field.

Relation. A *relation* between sets A and B is a subset $\mathcal{R}$ of $A \times B$. if $(a, b) \in \mathcal{R}$ we say a is related to b, denoted $a \, \mathcal{R} \, b$.

Ring. A *ring* $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and $\cdot$, called *addition* and *multiplication*, respectively, defined on R such that:

$\mathcal{R}_1$: $\langle R, + \rangle$ is an abelian group.

$\mathcal{R}_2$: Multiplication $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

$\mathcal{R}_3$: For all $a, b, c \in R$, the *left distribution law* $a \cdot (b + c) = (a \cdot c) + (b \cdot c)$ and the *right distribution law* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

Ring with Unity. A ring with a multiplicative identity element is a *ring with unity*. The multiplicative unit is called *unity*.

Same Cardinality. Two sets X and Y have the *same cardinality* if there exists a one to one function mapping X onto Y (that is, if there is a one-to-one correspondence between X and Y).

Simple Group. A group is *simple* if it is nontrivial and has no proper nontrivial normal subgroups.

Strictly Skew Field. A noncommutative division ring is called a *strictly skew field*.

Structural Property. A *structural property* of a binary structure $\langle S, * \rangle$ is a property shared by any binary structure $\langle S', *' \rangle$ which is isomorphic to $\langle S, * \rangle$.

Subgroup. If a subset H of a group G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a *subgroup* of G. We denote this as $H \leq G$ or $G \geq H$. If H is a subgroup of G and $H \neq G$, we write $H < G$ or $G > H$. If G is a group, then G itself is a subgroup of G called the *improper subgroup* of G; all other subgroups are *proper subgroups*. The subgroup $\{e\}$ is the *trivial subgroup*; all other subgroups are *nontrivial subgroups*.

Symmetry Group. Let A be the finite set $\{1, 2, \ldots, n\}$. The group of all permutations of A is the *symmetric group on n letters*, denoted S_n.

Transposition. A cycle of length 2 is a *transposition*.

Whole Numbers. The *whole numbers* are $\mathbb{W} = \{0, 1, 2, 3, \ldots\}$.

Zero of a Polynomial. Let F be a subfield of a field E, and let $\alpha \in E$. Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in F[x]$ and let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism (see Theorem 22.4). We denote

$$\phi_\alpha(f(x)) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

as $f(\alpha)$. If $f(\alpha) = 0$, then α is a *zero* of $f(x)$.

Revised: 1/7/2013