LINK III

Mouse icon in page 811

Some Results

1. The ring $(Z_m, +_m, \times_m)$ is an integral domain if and only if m is a prime.

2. Division (except by zero) is possible and is unique in any field.

3. Any finite integral domain D is a field.
Proof. The nonzero elements of D form a finite monoid $(D^*, .)$ in which right translations $r(x) = xb$ and left translations $\ell(x) = ax$ are all one-one. But by finiteness, this implies that they are all bijections, so that $ax = xa = 1$ for some $x \in D^*$. Hence each (nonzero) $a \in D^*$ has an inverse in D^*. Hence D is a field.

   In any field, the (unique) solution x of $bx = a(b \neq 0)$ is denoted by a/b (read "the quotient of a by b") and we have result 4.

4. In any field, quotients obey the following laws (for $b \neq 0, d \neq 0$):
   (i) $(a/b) = (c/d)$ if and only if $ad = bc$.
   (ii) $(a/b) \pm (c/d) = (ad \pm bc)/(bd)$.
   (iii) $(a/b)(c/d) = (ac/bd)$.
   (iv) $(a/b) + (-a/b) = 0$.
   (v) $(a/b)(b/a) = 1$ if $a, b \neq 0$.

The unital subring. In any nontrivial ring R, every subring contains the unity 1 of R (the trivial ring is the ring $\{0\}$ in which $1 = 0$). Now consider the additive subgroup U of the group $(R, +)$ generated by 1 in the commutative group $(R, +)$. This subgroup consists of all "multiples" of 1. Since $1 \neq 0$, in order is atleast 2. Note that

$$n1 = \underbrace{1 + \cdots + 1}_{n\ times} \quad \begin{array}{c}(-n)1 = -(n1) = n(1) \\ 01 = 0\end{array}$$

Extension of fields. If F is isomorphic to a subfield of a field G, then G is called an extension of F. Thus the extension of a given field F corresponds to the monomorphisms from F into larger fields. The complex field C is an extension of the real field R, and R is an extension of the rational field Q. Every field F is an extension of its initial subfield (prime subfield) hence it is an extension of Q if its characteristic is ∞ or some Z_p, it its characteristic is finite.

Finite fields. By definition, a finite field is a field having a finite number of elements. Such a field must have some (finite) prime characteristic p. Hence, its order must be some power $q = p^n$ of the prime p. Every finite field has prime-power order. Finite fields are also called Galois fields. We suppose $G = GF(p^n)$ is a given field of prime-power order $q = p^m$. We have a few results. We state them without proof.

1. Every element x of $G = GF(p^n)$ satisfies the polynomial equation $x^q = x$, where $q = p^n$.

2. For any $x_i \in G$, $(x - x_i)/(x^q - x)$ in the polynomial ring $G[x]$.

3. In $G = GF(q)$, $q = p^n$, $x^q - x = \prod_{x_i \in G} (x - x_i)$

4. In a finite field $GF(p^n)$, the multiplicative group G^* of all non zero elements is cyclic.

5. Any finite field of characteristic p is a simple algebraic extension of Z_p.

When we consider finite fields, we see that any finite field G has some finite characteristic p. Hence it is an extension on Z_p of some finite degree n. Since the general element of G can be considered as an n-vector $x - (x_1, \ldots, x_n)$ with arbitrary components $x_i \in Z_p$, it follows that every finite field has prime-power order $p^n = q$.

Reference : G. Birkhoff and T.C. Bartee, Modern Applied Algebra, McGraw-Hill, 1970.

LINK IV

Mouse icon in page 816

Definition. Direct product: If $(V_1, *_1, \#_1, \dots)$, $(V_2, *_2, \#_2, \dots)$, $\dots$, $(V_n, *_n, \#_n, \dots)$ are algebraic systems of the same kind, the direct product of these systems is $V = V_1 \times V_2 \times \cdots \times V_n$, with operations defined below. The elements of V are n-tuples of the form $(a_1, \dots, a_n)$ where $a_k \in V_k$, $k = 1, \dots, n$. The systems $V_1, V_2, \dots, V_n$ are called the factors of V. There are as many operations on V as there are on the factors. Each of these operations is defined componentwise. For example, if
$(a_1, \dots, a_n), (b_1, \dots, b_n) \in V$
$(a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 *_1 b_1, a_2 *_2 b_2, \dots, a_n *_n b_n)$
$(a_1, \dots, a_n)\#(b_1, \dots, b_n) = (a_1\#_1 b_1, a_2\#_2 b_2, \dots, a_n\#_n b_n)$
On notation, if two or more consecutive factors in a direct product are identical, it is common to combine them using exponential notation. For example, $Z \times Z \times R$ can be written $Z^2 \times R$ and $R \times R \times R \times R$ can be written R^4.

A direct product of algebraic systems is not always an algebraic system of the same type as its factors. This is due to the fact that certain axioms that are true for the factors may not be true for the set of n-tuples. However, this situation does not occur with group.

Theorem. The direct product of two or more groups is a group.
Proof. We will only present the proof of this theorem for the direct product of two groups. The proof can easily be extended to the direct product of n groups.

Stating that the direct product of two groups is a short way of saying that if $[G_1; *_1]$ and $[G_2; *_2]$ are groups, then $[G_1 \times G_2; *]$ is also a group, where * is the componentwise operation on $G_1 \times G_2$.

Associativity of * : if $a, b, c \in G_1 \times G_2$,

$$\begin{aligned}
a * (b * c) &= (a_1, a_2) * ((b_1, b_2) * (c_1, c_2)) \\
&= (a_1, a_2) * (b_1 *_1 c_1, b_2 *_2 c_2) \\
&= (a_1 *_1 (b_1 *_1 c_1) a_2 *_2 (b_2 *_2 c_2)) \\
&= ((a_1 *_1 b_1) *_1 c_1, (a_2 *_2 b_2) *_2 c_2) \\
&= (a_1 *_1 b_1, a_2 *_2 b_2) * (c_1, c_2) \\
&= ((a_1, a_2) * (b_1, b_2)) * (c_1, c_2) \\
&= (a * b) * c.
\end{aligned}$$

An identity for *: As one might expect, if e_1 and e_2 are identities for G_1 and G_2, respectively, then $e = (e_1, e_2)$ is the identity for $G_1 \times G_2$. If $a \in G_1 \times G_2$,

$$\begin{aligned}
a * e &= (a_1, a_2) * (e_1, e_2) \\
&= (a_1 *_1 e_1, a_2 *_2 e_2) \\
&= (a_1, a_2) \\
&= a.
\end{aligned}$$

Similarly, $e * a = a$.
Inverses in $G_1 \times G_2$: The inverse of an element is determined componentwise: $a^{-1} = (a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$. To verify, we compute $a * a^{-1}$:

$$\begin{aligned}
a * a^{-1} &= (a_1, a_2) * (a_1^{-1}, a_2^{-1}) \\
&= (a_1 *_1 a_1^{-1}, a_2 *_2 a_2^{-1}) \\
&= (e_1, e_2) \\
&= e.
\end{aligned}$$

Similarly, $a^{-1} * a = e$.
Example.

(a) If $n \geq 2$, Z_2^n, the direct product of n factors of Z_2 is a group with 2^n elements. We will take a closer look at $Z_2^3 = Z_2 \times Z_2 \times Z_2$. The elements of this group are triples of zeros and ones. Since the operation on Z_2 is $+_2$, we will use the symbol $+$ for the operation on Z_2^3. Two of the eight triples in the group are $a = (1, 0, 1)$ and $b = (0, 0, 1)$. Their "sum" is $a + b = (1 +_2 0, 0 +_2 0, 1 +_2 1) = (1, 0, 0)$. One interesting fact about this group is that each element is its own inverse. For example

$a + a = (1, 0, 1) + (1, 0, 1) = (0, 0, 0)$; therefore $-a = a$. We use the additive notation for the inverse of a because we are using a form of addition. Note that {(0, 0, 0), (1, 0, 1)} is a subgroup of Z_2^3. Write out the "addition" table for this set. The same canbe said for any set consisting of (0, 0, 0) and another element of Z_2^3.

(b) The direct product of the positive real numbers with the integers modulo 4, $R^+ \times Z_4$ is an infinite group since one of its factors is infinite. The operations on the factors are multiplication and modular addition, so we will select the neutral symbol # for the operation on $R^+ \times Z_4$. If $a = (4, 3)$ and $b = (0.5, 2)$, then $a\#b = (4, 3)\#(0.5, 2) = (4 \times 0.5, 3 +_4 2) = (2, 1)$, $b^2 = b\#b = (0.5, 2)\#(0.5, 2) = (0.25, 0)$, $a^{-1} = (4^{-1}, -3) = (0.25, 1)$ and $b^{-1} = (0.5^{-1}, -2) = (2, 2)$.

It would be incorrect to say that Z_4 is a subgroup of $R^+ \times Z_4$, but there is a subgroup of the direct product that closely resembles Z_4. It is $\{(1, 0), (1, 1), (1, 2), (1, 3)\}$. It's table is

#	(1, 0)	(1, 1)	(1, 2)	(1, 3)
(1, 0)	(1, 0)	(1, 1)	(1, 2)	(1, 3)
(1, 1)	(1, 1)	(1, 2)	(1, 3)	(1, 0)
(1, 2)	(1, 2)	(1, 3)	(1, 0)	(1, 1)
(1, 3)	(1, 3)	(1, 0)	(1, 1)	(1, 2)

Imagine erasing (1,) throughout the table and writing $+_4$ in place of #. What would you get? You will get $(Z_4, +_4)$.

Theorem. If $G = G_1 \times G_2 \times \cdots \times G_n$ is a direct product of n groups and $(a_1, a_2, \ldots, a_n) \in G$, then:

(a) $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$.

(b) $(a_1, a_2, \ldots, a_n)^m = (a_1^m, a_2^m, \ldots, a_n^m)$.

(c) The identity of G is $(e_1, e_2, \ldots, e_n)$, where e_i is the identity of G_i.

(d) G is abelian if and only if each of the factors $G_1, \ldots, G_n$ is abelian.

(e) If $H_1, H_2, \ldots, H_n$ are subgroups of the corresponding factors, then $H_1 \times H_2 \times \cdots \times H_n$ is a subgroup of G.

Not all subgroups of a direct product are obtained like this. For example, $\{(n, n) : n \in Z\}$ is a subgroup of Z^2, but is not a direct product of two subgroups of Z.

Direct Products of Rings

Let $R_1, R_2, \ldots, R_n$ be rings under the operations of $+_1, +_2, \ldots, +_n$ and $\cdot_1, \cdot_2, \ldots, \cdot_n$ respectively. Let

$$P = {}_{\times}{}_{i=1}^{n}R_i$$

and

$$a = (a_1, a_2, \ldots, a_n), \quad b = (b_1, b_2, \ldots, b_n) \in P.$$

We see that P is an abelian group under the operation of componentwise addition:

$$a + b = (a_1 +_1 b_1, a_2 +_2 b_2, \ldots, a_n +_n b_n).$$

We also define multiplication on P componentwise:

$$ab = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2, \ldots, a_n \cdot_n b_n).$$

To show that P is a ring under the above operations, we need only show that the (multiplicative) associative law and the distributive laws hold. This is indeed the case. Details are left as exercise. If each of the rings R_i is commutative, then P is commutative, and if each of the R_i contains unity, then P is a ring with unity which is the n-tuple consisting of the unities of each of the R_i's.

Example. Since $[Z_4; +_4, \times_4]$ and $[Z_3, +_3, \times_3]$ are rings, then $Z_4 \times Z_3$ is a ring, where for example,

$$(2, 1) + (2, 2) = (2 +_4 2, 1 +_3 2) = (0, 0)$$

and

$$(3, 2)(2, 2) = (3 +_4 2, 2 +_3 2) = (2, 1).$$

To determine the unity, if it exists, in the ring $Z_4 \times Z_3$, we look for the element (m, n) such that for all elements $(x, y) \in Z_4 \times Z_3$, $(x, y) = (x, y)(m, n) = (m, n)(x, y)$, or, equivalently, $(x \times_4 m, y \times_3 n) = (m \times_4 x, n \times_3 y) = (x, y)$. So we want m such that $x \times_4 m = m \times_4 x = x$ in the ring Z. The only element m in Z_4 that satisfies this equation is the element $m = 1$. Similarly, we obtain a value of 1 for n. So the unity of $Z_4 \times Z_3$, which is unique, is $(1, 1)$. We leave to the reader to verify that this ring is commutative.

Hence, products of rings are analogous to products of groups.

LINK V

Mouse icon in page 822

1. Consider a (m, n) code and let $r = n - m$

   (a) Given an encoding matrix G, show that there exists a parity-check matrix H such that

   (i) If G is $m \times n$, H is $n \times (n - m)$

   (ii) $GH = 0$

   (iii) Each column h_i, $1 \leq i \leq n - m$ of H is such that for no scalars θ_i, not all zero, does $\sum_{i=1}^{n-m} a_i h_i = 0$. i.e., the columns of H are linearly independent.
   H is called the parity check matrix because, for any codeword C in the code generated by G, $CH = 0$.

   (b) Show that, given a parity check matrix for a code, the minimum weight of a codeword (not the 0 codeword) is equal to the minimum number of rows of H which can be added together to give 0.

2. Consider (m, n) code.
   G is given by $[IA]$,
   where I is $m \times m$,
   A is $m \times n - m$.
   Define H such that $H = \begin{bmatrix} A \\ I \end{bmatrix}$,
   where A is $m \times (n - m)$.
   I is $(n - m) \times (n - m)$.
   (i) H is of size $n \times (n - m)$.
   (ii) To show $GH = O$.
   GH is of size $m \times (n - m)$.

We have to show each element of $GH = 0$.

$$\begin{aligned}GH(i,j) &= G_{i1}H_{1j} + G_{i2}H_{2j} + G_{i3}H_{3j} + \cdots + G_{in}H_{nj} \\ &= G_{i1}H_{1j} + \cdots + G_{im}H_{mj} + G_{i(m+1)}H_{(m+1)j} \\ &\quad + G_{i(m+2)}H_{(m+2)j} + \cdots + G_{in}H_{nj}\end{aligned}$$

Only one element of G_{ik}, $1 \leq k \leq m$ is non zero. It is G_{ii}, others are 0.
Only one element of H_{qj}, $m+1 \leq q \leq n$ is 1, it is non zero.
It is $H_{(m+j)j}$, others are 0.
Hence $GH(i,j) = G_{ii}H_{ij} + G_{i(m+j)}H_{(m+j)j}$.
$H_{ij} = G_{i(m+j)} = a_{ij}$ the ijth element of A.
Hence $GH(i,j) = a_{ij} + a_{ij}$.
This is 0 whether $a_{ij} = 0$ or 1.
Hence for all $1 \leq i \leq m$, $1 \leq j \leq n-m$,
$GH(i,j) = 0$, i.e., $GH = O$.
(iii) To show that the columns of H are linearly independent.
$C = \begin{bmatrix} I_1 & A \\ A^T & I_2 \end{bmatrix}$ is a $n \times n$ matrix,
where I_1 is of size $m \times m$ (identity matrix).
I_2 is of size $(n-m) \times (n-m)$ (identity matrix).
A is of size $m \times (n-m)$.
A^T is of size $(n-m) \times m$.
The determinant of C is non zero.
So columns of C are linearly independent.
The columns of H is a subset of this and hence linearly independent.
Let C be a code word and m the corresponding message word.
$C = mG$.
$CH = mGH = mO = O$.
(b) H is a parity check matrix for a (m,n) code
H is of size $n \times (n-m)$, where $n > (n-m)$.
Hence the rows of H are not linearly independent.
Let C_1 be a code word of minimum weight r say. Then if $C = C_1 \ldots C_n$, r of C_i's are 1 and rest of them of 0.
Let $C_{i_1}, C_{i_2}, \ldots, C_{i_r}$ be 1.
Then since $CH = O$, the $i_1, i_2, \ldots, i_r$th row added together give 0.

3. How single error correction is done is illustrated by the following example.

Let $a(2,5)$ code be generated by the following generator matrix

$$h = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$e(00) = 00000$
$e(01) = 01110$
$e(10) = 10101$
$e(11) = 11011$
$m = 2$, $n = 5$

H is 5×3 matrix $\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

If instead of codeword 01110, 01010 is received, the third bit is in error and single error has occured. This is identified as follows:

(received word) H gives

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 100$$

This is the third row of H.

Hence third bit is in error and corrected as 1. Hence the code word is 01110 and decoded as 01.

Reference Books

References

[1] D.F. Stanat and D.F. McAllister, Discrete Mathematics in Computer Science, Prentice Hall International Inc., 1977.

[2] J.B. Fraliegh, A First course in Abstract Algebra, Reading Mass, Addison-Wesley, 1969.

[3] A. Gill, Applied Algebra for the Computer Sciences, Englewood Cliffs, N.J : Prentice-Hall Inc., 1976.

[4] I.N. Herstein, Topics in Algebra, Waltham Mass, Blaisdell, 1964.

[5] G. Birkhoff and T.C. Bontee, Modern Applied Algebra, McGraw-Hill Book Company, 1970.

[6] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, 1968.

[7] W.W. Petersen and E.J. Weldon Jr., Error Correcting Codes, M.I.T. Press, 1972.

[8] A. Doen and K. Levasseur, Applied Discrete Structures for Computer Science, Galgotia Publications Pvt. Ltd., 1986.

[9] S. Lin, An Introduction to error-correcting codes, Prentice-Hall Englewood Cliffs, N.J., 1970.

[10] C.L. Liu, Elements of Discrete Mathematics, McGraw-Hill Book Company, 1985.

[11] J.P. Tremblay and R. Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw-Hill Book Company, 1975.

[12] G. Birkhoff and S. Maclane, A survey of Modern Algebra, MacMillan & Co. Ltd., London, 1965.

Some Useful Websites

1. http://dogschool.tripod.com
2. http://www.math.uconn.edu/∼kconrad/math216/whygroups.html
3. http://www.rubikssolver.com/
4. http://www.math.csusb.edu/notes/advanced/algebra/gp/node6.html
5. http://nptel.iitm.ac.in/courses/117106031/
6. http://rutherglen.science.mq.edu.au/wchen/Indmfolder/dm11.pdf
7. http://www.maths.uq.edu.eu/∼victors/Algebra/ch4.pdf
8. http://math.mit.edu/∼shor/18.310/polycode.pdf