



吴宏锋 邹建成 陈小光◎编著

Xinxi Anquan de  
Shuxue Jichu

# 信息安全的数学基础



北京邮电大学出版社  
[www.buptpress.com](http://www.buptpress.com)

# 信息安全的数学基础

吴宏锋 邹建成 陈小光 编著

本书是“十一五”国家重点图书出版规划项目成果，也是“十一五”国家信息化规划项目成果。

本书系统地介绍了信息安全的基本概念、原理和方法，展示了信息安全领域的最新研究成果。

本书可作为高等院校信息安全专业的教材，也可供从事信息安全工作的科研人员参考。

本书在编写过程中参考了大量国内外文献，吸收了国内外在信息安全方面的最新研究成果。

本书由吴宏锋、邹建成、陈小光编著，由北京邮电大学出版社出版。



北京邮电大学出版社  
www.buptpress.com

## 内 容 简 介

《信息安全的数学基础》围绕信息安全相关课程所需的数学基础,介绍组合数学、抽象代数、数论的基本原理和方法。本书的内容包括组合数学基础、群、环、域、整数、同余、数论函数、Legendre 符号、Jacobi 符号等。本书根据信息时代的需要精选内容,抓住主线,整合知识点,简洁且通俗易懂,注重培养学生科学的思维方式。本书各章末尾都附有相当数量的习题,便于教学与自学。

《信息安全的数学基础》可作为信息安全专业、密码学专业、计算机专业的本科生和研究生的教科书,也可以供从事信息安全工作的科研人员参考。

### 图书在版编目(CIP)数据

信息安全的数学基础 / 吴宏锋, 邹建成, 陈小光编著. -- 北京 : 北京邮电大学出版社, 2016. 7

ISBN 978-7-5635-4730-2

I. ①信… II. ①吴… ②邹… ③陈… III. ①信息安全—应用数学 IV. ①TP309②O29

中国版本图书馆 CIP 数据核字 (2016) 第 071913 号

---

书 名: 信息安全的数学基础

著作责任者: 吴宏锋 邹建成 陈小光 编著

责任编辑: 刘 颖

出版发行: 北京邮电大学出版社

社 址: 北京市海淀区西土城路 10 号 (邮编: 100876)

发 行 部: 电话: 010-62282185 传真: 010-62283578

E-mail: publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 北京通州皇家印刷厂

开 本: 787 mm×960 mm 1/16

印 张: 5.75

字 数: 121 千字

印 数: 1—2 000 册

版 次: 2016 年 7 月第 1 版 2016 年 7 月第 1 次印刷

---

ISBN 978-7-5635-4730-2

定 价: 18.00 元

• 如有印装质量问题, 请与北京邮电大学出版社发行部联系 •

# 前　　言

近年来随着信息技术的迅猛发展,人们对信息安全的需求越来越广泛,各高校也陆续开设了相关的课程,包括密码学、信息安全、编码理论等等。信息安全是一个涉及数学、计算机与信息科学等多个领域的交叉学科,数学在信息安全中起着核心作用。目前国内已出版了不少信息安全的数学基础等相关方面的书籍。本书旨在为信息安全专业、密码学专业等所需的数学知识提供一个简明而完备的入门教程,使读者了解组合理论、群论、初等数论、域论等方面的基础知识,拓展学生的数学视野,并为进一步学习更专业的知识提供便利。本书在编写过程中力求做到叙述简明,科学严谨,并不假定读者具有很多的数学知识,大学低年级的学生不查看其它书籍资料就能看懂本书。

本书可作为信息安全专业、密码学专业、计算机专业的本科生和研究生的教科书,也可供从事信息安全工作的科研人员参考。

在本书的编写过程中,我们参考了国内外许多相关的书籍,我们将它们一一列在本书最后的参考文献中。本书中很多章节的内容、例题、习题都并非作者原创,而是取材于这些参考文献,在此一并致谢。由于水平有限,书中难免有疏漏和不当之处,敬请读者批评指正。

第1章　　序	1
第2章　　集合与映射	2
2.1　　集合	2
2.2　　映射	10
2.3　　关系	12
2.4　　等价关系与划分	14
2.5　　偏序关系	16
2.6　　函数	18
2.7　　逆像与复合映射	20
2.8　　单射、满射与双射	22
2.9　　映射的性质	24
2.10　　映射的运算	26
2.11　　映射的逆像	28
2.12　　映射的复合	30
2.13　　映射的性质	32
2.14　　映射的逆像	34
2.15　　映射的复合	36
2.16　　映射的逆像	38
2.17　　映射的复合	40
2.18　　映射的性质	42
2.19　　映射的逆像	44
2.20　　映射的复合	46
2.21　　映射的性质	48
2.22　　映射的逆像	50
2.23　　映射的复合	52
2.24　　映射的性质	54
2.25　　映射的逆像	56
2.26　　映射的复合	58
2.27　　映射的性质	60
2.28　　映射的逆像	62
2.29　　映射的复合	64
2.30　　映射的性质	66
2.31　　映射的逆像	68
2.32　　映射的复合	70
2.33　　映射的性质	72
2.34　　映射的逆像	74
2.35　　映射的复合	76
2.36　　映射的性质	78
2.37　　映射的逆像	80
2.38　　映射的复合	82
2.39　　映射的性质	84
2.40　　映射的逆像	86
2.41　　映射的复合	88
2.42　　映射的性质	90
2.43　　映射的逆像	92
2.44　　映射的复合	94
2.45　　映射的性质	96
2.46　　映射的逆像	98
2.47　　映射的复合	100
2.48　　映射的性质	102
2.49　　映射的逆像	104
2.50　　映射的复合	106
2.51　　映射的性质	108
2.52　　映射的逆像	110
2.53　　映射的复合	112
2.54　　映射的性质	114
2.55　　映射的逆像	116
2.56　　映射的复合	118
2.57　　映射的性质	120
2.58　　映射的逆像	122
2.59　　映射的复合	124
2.60　　映射的性质	126
2.61　　映射的逆像	128
2.62　　映射的复合	130
2.63　　映射的性质	132
2.64　　映射的逆像	134
2.65　　映射的复合	136
2.66　　映射的性质	138
2.67　　映射的逆像	140
2.68　　映射的复合	142
2.69　　映射的性质	144
2.70　　映射的逆像	146
2.71　　映射的复合	148
2.72　　映射的性质	150
2.73　　映射的逆像	152
2.74　　映射的复合	154
2.75　　映射的性质	156
2.76　　映射的逆像	158
2.77　　映射的复合	160
2.78　　映射的性质	162
2.79　　映射的逆像	164
2.80　　映射的复合	166
2.81　　映射的性质	168
2.82　　映射的逆像	170
2.83　　映射的复合	172
2.84　　映射的性质	174
2.85　　映射的逆像	176
2.86　　映射的复合	178
2.87　　映射的性质	180
2.88　　映射的逆像	182
2.89　　映射的复合	184
2.90　　映射的性质	186
2.91　　映射的逆像	188
2.92　　映射的复合	190
2.93　　映射的性质	192
2.94　　映射的逆像	194
2.95　　映射的复合	196
2.96　　映射的性质	198
2.97　　映射的逆像	200
2.98　　映射的复合	202
2.99　　映射的性质	204
2.100　　映射的逆像	206
2.101　　映射的复合	208
2.102　　映射的性质	210
2.103　　映射的逆像	212
2.104　　映射的复合	214
2.105　　映射的性质	216
2.106　　映射的逆像	218
2.107　　映射的复合	220
2.108　　映射的性质	222
2.109　　映射的逆像	224
2.110　　映射的复合	226
2.111　　映射的性质	228
2.112　　映射的逆像	230
2.113　　映射的复合	232
2.114　　映射的性质	234
2.115　　映射的逆像	236
2.116　　映射的复合	238
2.117　　映射的性质	240
2.118　　映射的逆像	242
2.119　　映射的复合	244
2.120　　映射的性质	246
2.121　　映射的逆像	248
2.122　　映射的复合	250
2.123　　映射的性质	252
2.124　　映射的逆像	254
2.125　　映射的复合	256
2.126　　映射的性质	258
2.127　　映射的逆像	260
2.128　　映射的复合	262
2.129　　映射的性质	264
2.130　　映射的逆像	266
2.131　　映射的复合	268
2.132　　映射的性质	270
2.133　　映射的逆像	272
2.134　　映射的复合	274
2.135　　映射的性质	276
2.136　　映射的逆像	278
2.137　　映射的复合	280
2.138　　映射的性质	282
2.139　　映射的逆像	284
2.140　　映射的复合	286
2.141　　映射的性质	288
2.142　　映射的逆像	290
2.143　　映射的复合	292
2.144　　映射的性质	294
2.145　　映射的逆像	296
2.146　　映射的复合	298
2.147　　映射的性质	300
2.148　　映射的逆像	302
2.149　　映射的复合	304
2.150　　映射的性质	306
2.151　　映射的逆像	308
2.152　　映射的复合	310
2.153　　映射的性质	312
2.154　　映射的逆像	314
2.155　　映射的复合	316
2.156　　映射的性质	318
2.157　　映射的逆像	320
2.158　　映射的复合	322
2.159　　映射的性质	324
2.160　　映射的逆像	326
2.161　　映射的复合	328
2.162　　映射的性质	330
2.163　　映射的逆像	332
2.164　　映射的复合	334
2.165　　映射的性质	336
2.166　　映射的逆像	338
2.167　　映射的复合	340
2.168　　映射的性质	342
2.169　　映射的逆像	344
2.170　　映射的复合	346
2.171　　映射的性质	348
2.172　　映射的逆像	350
2.173　　映射的复合	352
2.174　　映射的性质	354
2.175　　映射的逆像	356
2.176　　映射的复合	358
2.177　　映射的性质	360
2.178　　映射的逆像	362
2.179　　映射的复合	364
2.180　　映射的性质	366
2.181　　映射的逆像	368
2.182　　映射的复合	370
2.183　　映射的性质	372
2.184　　映射的逆像	374
2.185　　映射的复合	376
2.186　　映射的性质	378
2.187　　映射的逆像	380
2.188　　映射的复合	382
2.189　　映射的性质	384
2.190　　映射的逆像	386
2.191　　映射的复合	388
2.192　　映射的性质	390
2.193　　映射的逆像	392
2.194　　映射的复合	394
2.195　　映射的性质	396
2.196　　映射的逆像	398
2.197　　映射的复合	400
2.198　　映射的性质	402
2.199　　映射的逆像	404
2.200　　映射的复合	406
2.201　　映射的性质	408
2.202　　映射的逆像	410
2.203　　映射的复合	412
2.204　　映射的性质	414
2.205　　映射的逆像	416
2.206　　映射的复合	418
2.207　　映射的性质	420
2.208　　映射的逆像	422
2.209　　映射的复合	424
2.210　　映射的性质	426
2.211　　映射的逆像	428
2.212　　映射的复合	430
2.213　　映射的性质	432
2.214　　映射的逆像	434
2.215　　映射的复合	436
2.216　　映射的性质	438
2.217　　映射的逆像	440
2.218　　映射的复合	442
2.219　　映射的性质	444
2.220　　映射的逆像	446
2.221　　映射的复合	448
2.222　　映射的性质	450
2.223　　映射的逆像	452
2.224　　映射的复合	454
2.225　　映射的性质	456
2.226　　映射的逆像	458
2.227　　映射的复合	460
2.228　　映射的性质	462
2.229　　映射的逆像	464
2.230　　映射的复合	466
2.231　　映射的性质	468
2.232　　映射的逆像	470
2.233　　映射的复合	472
2.234　　映射的性质	474
2.235　　映射的逆像	476
2.236　　映射的复合	478
2.237　　映射的性质	480
2.238　　映射的逆像	482
2.239　　映射的复合	484
2.240　　映射的性质	486
2.241　　映射的逆像	488
2.242　　映射的复合	490
2.243　　映射的性质	492
2.244　　映射的逆像	494
2.245　　映射的复合	496
2.246　　映射的性质	498
2.247　　映射的逆像	500
2.248　　映射的复合	502
2.249　　映射的性质	504
2.250　　映射的逆像	506
2.251　　映射的复合	508
2.252　　映射的性质	510
2.253　　映射的逆像	512
2.254　　映射的复合	514
2.255　　映射的性质	516
2.256　　映射的逆像	518
2.257　　映射的复合	520
2.258　　映射的性质	522
2.259　　映射的逆像	524
2.260　　映射的复合	526
2.261　　映射的性质	528
2.262　　映射的逆像	530
2.263　　映射的复合	532
2.264　　映射的性质	534
2.265　　映射的逆像	536
2.266　　映射的复合	538
2.267　　映射的性质	540
2.268　　映射的逆像	542
2.269　　映射的复合	544
2.270　　映射的性质	546
2.271　　映射的逆像	548
2.272　　映射的复合	550
2.273　　映射的性质	552
2.274　　映射的逆像	554
2.275　　映射的复合	556
2.276　　映射的性质	558
2.277　　映射的逆像	560
2.278　　映射的复合	562
2.279　　映射的性质	564
2.280　　映射的逆像	566
2.281　　映射的复合	568
2.282　　映射的性质	570
2.283　　映射的逆像	572
2.284　　映射的复合	574
2.285　　映射的性质	576
2.286　　映射的逆像	578
2.287　　映射的复合	580
2.288　　映射的性质	582
2.289　　映射的逆像	584
2.290　　映射的复合	586
2.291　　映射的性质	588
2.292　　映射的逆像	590
2.293　　映射的复合	592
2.294　　映射的性质	594
2.295　　映射的逆像	596
2.296　　映射的复合	598
2.297　　映射的性质	600
2.298　　映射的逆像	602
2.299　　映射的复合	604
2.300　　映射的性质	606
2.301　　映射的逆像	608
2.302　　映射的复合	610
2.303　　映射的性质	612
2.304　　映射的逆像	614
2.305　　映射的复合	616
2.306　　映射的性质	618
2.307　　映射的逆像	620
2.308　　映射的复合	622
2.309　　映射的性质	624
2.310　　映射的逆像	626
2.311　　映射的复合	628
2.312　　映射的性质	630
2.313　　映射的逆像	632
2.314　　映射的复合	634
2.315　　映射的性质	636
2.316　　映射的逆像	638
2.317　　映射的复合	640
2.318　　映射的性质	642
2.319　　映射的逆像	644
2.320　　映射的复合	646
2.321　　映射的性质	648
2.322　　映射的逆像	650
2.323　　映射的复合	652
2.324　　映射的性质	654
2.325　　映射的逆像	656
2.326　　映射的复合	658
2.327　　映射的性质	660
2.328　　映射的逆像	662
2.329　　映射的复合	664
2.330　　映射的性质	666
2.331　　映射的逆像	668
2.332　　映射的复合	670
2.333　　映射的性质	672
2.334　　映射的逆像	674
2.335　　映射的复合	676
2.336　　映射的性质	678
2.337　　映射的逆像	680
2.338　　映射的复合	682
2.339　　映射的性质	684
2.340　　映射的逆像	686
2.341　　映射的复合	688
2.342　　映射的性质	690
2.343　　映射的逆像	692
2.344　　映射的复合	694
2.345　　映射的性质	696
2.346　　映射的逆像	698
2.347　　映射的复合	700
2.348　　映射的性质	702
2.349　　映射的逆像	704
2.350　　映射的复合	706
2.351　　映射的性质	708
2.352　　映射的逆像	710
2.353　　映射的复合	712
2.354　　映射的性质	714
2.355　　映射的逆像	716
2.356　　映射的复合	718
2.357　　映射的性质	720
2.358　　映射的逆像	722
2.359　　映射的复合	724
2.360　　映射的性质	726
2.361　　映射的逆像	728
2.362　　映射的复合	730
2.363　　映射的性质	732
2.364　　映射的逆像	734
2.365　　映射的复合	736
2.366　　映射的性质	738
2.367　　映射的逆像	740
2.368　　映射的复合	742
2.369　　映射的性质	744
2.370　　映射的逆像	746
2.371　　映射的复合	748
2.372　　映射的性质	750
2.373　　映射的逆像	752
2.374　　映射的复合	754
2.375　　映射的性质	756
2.376　　映射的逆像	758
2.377　　映射的复合	760
2.378　　映射的性质	762
2.379　　映射的逆像	764
2.380　　映射的复合	766
2.381　　映射的性质	768
2.382　　映射的逆像	770
2.383　　映射的复合	772
2.384　　映射的性质	774
2.385　　映射的逆像	776
2.386　　映射的复合	778
2.387　　映射的性质	780
2.388　　映射的逆像	782
2.389　　映射的复合	784
2.390　　映射的性质	786
2.391　　映射的逆像	788
2.392　　映射的复合	790
2.393　　映射的性质	792
2.394　　映射的逆像	794
2.395　　映射的复合	796
2.396　　映射的性质	798
2.397　　映射的逆像	800
2.398　　映射的复合	802

## 第1章 预备知识

## 目 录

<b>第1章 预备知识</b>	1
1.1 集合	1
1.2 集合上的关系	2
1.3 偏序集合	4
1.4 排列与组合	5
习题	12
<b>第2章 代数学基础</b>	14
2.1 群	14
2.1.1 群和子群	14
2.1.2 群的同态	21
2.2 环	23
2.2.1 环、子环和理想	23
2.2.2 商环和环的同态	24
2.2.3 素理想和极大理想	27
2.2.4 多项式环	29
2.2.5 整环的整除性	30
2.3 域和扩域	34
习题	38
<b>第3章 有限域初步</b>	41
3.1 有限域的结构	41
3.2 迹和范数	47
3.3 分圆多项式	50
习题	52

<b>第4章 初等数论基础</b>	55
4.1 整数的可除性	55
4.2 数论函数	61
4.3 同余	65
4.4 二次剩余	71
4.4.1 二次剩余	72
4.4.2 勒让德符号	74
4.4.3 雅可比符号	79
习题	81
<b>参考文献</b>	83

# 第1章 预备知识

本章作为开端,简要回顾一些基础知识。这一章我们介绍集合论的一些基本知识。集合是数学的基本概念之一,但是,值得注意的是集合这一基本概念,没有一个严谨的数学定义,只有一个描述性的说明。但这里介绍的集合论通常称为朴素的集合论,不涉及逻辑学中的悖论,本书中的集合指的是具有一定属性的事物形成的一个集体。我们假设读者已经熟悉集合论的基本概念,如交集、并集、子集、包含、映射以及德·摩根(De Morgan)定律等。进一步的内容参看文献[9]。

## 1.1 集合

**定义 1.1.1** 把人们直观或思维中某些确定的能够区分的对象汇合在一起,使之成为一个整体,这一整体就是集合。组成集合的这些对象称为这一集合的元素(或简称为元)。

没有任何元素的集合称为空集,记作 $\emptyset$ 。

设 $A$ 是一个集合, $a$ 是一个元素。如果 $a$ 是 $A$ 的元素,记作 $a \in A$ ,读作 $a$ 属于 $A$ 。如果 $a$ 不是 $A$ 的元素,则记作 $a \notin A$ ,读作 $a$ 不属于 $A$ 。

**定义 1.1.2** 如果集合 $A$ 的每一个元素都是集合 $B$ 的元素,即若 $a \in A$ ,则 $a \in B$ ,记作 $A \subset B$ 或 $B \supset A$ ,分别读作 $A$ 包含于 $B$ 和 $B$ 包含 $A$ 。

如果 $A \subset B$ ,则称 $A$ 为 $B$ 的子集。如果 $A$ 是 $B$ 的子集,但 $A$ 又不等于 $B$ ,即 $B$ 中至少有一个元素不是 $A$ 的元素,则称 $A$ 为 $B$ 的真子集。

**定义 1.1.3** 给定集合 $X$ ,称 $X$ 所有子集构成的集合为集合 $X$ 的幂集,记作 $P(X)$ 。

**定义 1.1.4** 给定集合 $X$ ,称 $X$ 中的元素个数为集合 $X$ 的基数,记为 $|X|$ 。若 $|X|=n$ ,称 $X$ 为一个 $n$ -集合。

若 $X$ 为一个 $n$ -集合,则显然 $|P(X)|=2^n$ 。

**定义 1.1.5** 设 $A$ 和 $B$ 是两个集合,集合

$$\{x \mid x \in A \text{ 或 } x \in B\}$$

称为集合 $A$ 与 $B$ 的并集或并,记作 $A \cup B$ 。集合

$$\{x \mid x \in A \text{ 并且 } x \in B\}$$

称为集合 $A$ 与 $B$ 的交集或交,记作 $A \cap B$ 。

若 $A \cap B = \emptyset$ ,则称 $A$ 与 $B$ 不相交。反之,若 $A \cap B \neq \emptyset$ ,则称 $A$ 与 $B$ 有非空交。

### 定义 1.1.6 集合

$$\{x \mid x \in A \text{ 并且 } x \notin B\}$$

称为集合  $A$  与  $B$  的差集, 记作  $A - B$  或  $A \setminus B$ 。

**定理 1.1.1** 设  $A, B, C$  都是集合, 则以下等式成立:

$$(1) A \cup A = A, A \cap A = A;$$

$$(2) (\text{交换律}) \quad A \cup B = B \cup A, A \cap B = B \cap A;$$

$$(3) (\text{结合律}) \quad (A \cup B) \cup C = A \cup (B \cup C), (A \cap B) \cap C = A \cap (B \cap C);$$

$$(4) (\text{分配律}) \quad (A \cap B) \cup C = (A \cup C) \cap (B \cup C), (A \cup B) \cap C = (A \cap C) \cup (B \cap C);$$

$$(5) (\text{De Morgan 律}) \quad A - (B \cup C) = (A - B) \cap (A - C), A - (B \cap C) = (A - B) \cup (A - C).$$

## 1.2 集合上的关系

设  $X, Y$  是任意两个集合。任取  $x \in X, y \in Y$ , 给定顺序的元素对  $(x, y)$  称为一个有序对。这时两个有序对  $(x_1, y_1) = (x_2, y_2)$  当且仅当  $x_1 = x_2, y_1 = y_2$ 。全体有序对的集合

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

称为两个集合  $X$  和  $Y$  的笛卡儿积(Cartesian 积)。

当  $|X| = m, |Y| = n$  时, 显然有  $|X \times Y| = m \times n$ 。

一个从  $X$  到  $Y$  的关系  $R$ , 记为  $R: X \rightarrow Y$ , 定义为  $X \times Y$  的一个子集。若  $|X| = m, |Y| = n$ , 则从  $X$  到  $Y$  的关系有  $2^{mn}$  个。

关系  $R$  的定义域为  $\{x \in X \mid \text{存在 } y \in Y \text{ 使得 } (x, y) \in R\}$ , 值域为  $\{y \in Y \mid \text{存在 } x \in X, \text{ 使得 } (x, y) \in R\}$ 。若  $(x, y) \in R$ , 则称  $x$  与  $y$  有关系  $R$ 。对于  $x \in X$ ,  $x$  的像为  $R(x) = \{y \in Y \mid (x, y) \in R\}$ , 故  $R$  的值域为  $\bigcup_{x \in X} R(x)$ 。对于  $y \in Y$ ,  $y$  的原像为  $R^{-1}(y) = \{x \in X \mid (x, y) \in R\}$ .  $R$  的反关系  $R^{-1}: Y \rightarrow X$  定义为  $R^{-1} = \{(y, x) \mid (x, y) \in R\}$ 。

例如, 实数集合  $\mathbf{R}$  中的小于顺序“ $<$ ”是  $\mathbf{R}$  上的一个二元关系, 空间两直线平行或者不平行也是一个关系。

设  $R$  是  $X$  上的一个关系, 即一个  $X$  到  $X$  的关系, 称  $R$  是自反的, 若对任意  $x \in X$ ,  $(x, x) \in R$ ;  $R$  是对称的, 对  $x, y \in X$ , 若  $(x, y) \in R$ , 则  $(y, x) \in R$ ;  $R$  是反对称的, 若对  $(x, y) \in R, (y, x) \in R$ , 则有  $x = y$ ;  $R$  是传递的, 对  $x, y, z \in X$ , 若  $(x, y) \in R, (y, z) \in R$ , 则  $(x, z) \in R$ 。

**定义 1.2.1** 设  $R$  是集合  $X$  上的一个关系, 若  $R$  是自反的、对称的和传递的, 则称  $R$  是定义在  $X$  上的一个等价关系。此时, 若  $(x, y) \in R$ , 则称  $x$  等价于  $y$ , 记作  $x \sim y$ 。

显然, “平行”是一个等价关系, “小于关系”则不是等价关系。设  $R$  为一等价关系, 对任意  $x \in X$ , 则  $x$  的像  $[x] = \{y \in X \mid (x, y) \in R\}$  称为包含元素  $x$  的等价类。由于  $a \sim a$ , 有  $a \in [a]$ 。任意元素  $a' \in [a]$  都称为类  $[a]$  的代表元。

**定义 1.2.2** 若  $X$  的非空子集的集合  $P = \{X_1, \dots, X_k\}$  满足  $X = \bigcup_{i=1}^k X_i$ , 且  $X_i \cap X_j =$

$\emptyset, i \neq j$ , 则称  $P$  是集合  $X$  的一个划分。

非空集合  $S$  的任一等价关系  $\sim$  确定  $S$  的一个划分, 这是因为  $a \in \bar{a}$ , 所以  $S = \bigcup_{a \in S} \bar{a}$ 。若  $\bar{a} \cap \bar{b} \neq \emptyset$  且  $s \in \bar{a} \cap \bar{b}$ , 则  $s \in \bar{a}, s \in \bar{b}$ , 于是  $a \sim b, \bar{a} = \bar{b}$ , 即不同的等价类互不相交, 因此所有的等价类构成集合  $S$  的一个划分。

反之, 集合  $S$  的一个划分  $\{S_\lambda\}$  确定一个等价关系如下: 规定  $a \sim b \Leftrightarrow a, b$  属于同一个  $S_\lambda$ 。

**定义 1.2.3** 设  $f$  是从  $X$  到  $Y$  的一个关系, 若  $f$  满足  $|f(x)|=1, \forall x \in X$ , 则称  $f$  是从  $X$  到  $Y$  的一个映射。对于函数  $f$ , 若对  $x_1 \neq x_2 \in X$  有  $f(x_1) \neq f(x_2)$ , 则称  $f$  为单射, 若对于任意  $y \in Y$  都有  $f^{-1}(y) \neq \emptyset$ , 则称  $f$  为满射。

$X$  到  $X$  的映射也称为  $X$  上的一个变换。两个映射相等  $F=G$ , 是指它们有相同的定义域和值域且  $\forall x \in X, F(x)=G(x)$ 。

**定义 1.2.4** 将每个元素  $x \in X$  映到自身的映射  $i_x: X \rightarrow X$  称为单位映射或恒等映射。

**定义 1.2.5** 设  $f: X \rightarrow Y, g: Y \rightarrow X$  是两个映射, 则合成映射  $fg$  和  $gf$  是确定的。如果  $fg=i_Y$ , 那么  $f$  称为  $g$  的左逆,  $g$  称为  $f$  的右逆。如果  $fg=e_Y, gf=i_X$ , 则称  $g$  为  $f$  的一个逆, 记作  $f^{-1}$ 。

映射有下面的一些属性, 读者可自行检验。

#### 性质 1.2.1

- (1)  $f$  有左逆当且仅当  $f$  是单射;
- (2)  $f$  有右逆当且仅当  $f$  是满射;
- (3)  $f$  有左逆  $g$ , 同时又有右逆  $h$ , 则  $g=h$ ;
- (4)  $f$  有逆当且仅当  $f$  是一个一一映射;
- (5) 若  $f$  有逆, 则  $f$  的逆  $f^{-1}$  是唯一的, 且  $(f^{-1})^{-1}=f$ 。

若  $|X|=m, |Y|=n$ , 则从  $X$  到  $Y$  的映射有  $n^m$  个。对于映射  $f$ , 若  $f^{-1}$  也是映射, 则称  $f$  为双射。显然  $f$  为双射当且仅当  $f$  既为单射又为满射。

**定理 1.2.1** 设  $X, Y$  为两个基数相同的有限集,  $f$  为  $X$  到  $Y$  的一个映射, 则  $f$  为单射当且仅当  $f$  为满射。

**定义 1.2.6** 设  $X, Y$  是两个集合,  $A$  是  $X$  的一个子集。映射  $f: X \rightarrow Y$  和  $g: A \rightarrow Y$  如果满足条件  $g \subset f$ , 即对于任意的  $a \in A$  有  $f(a)=g(a)$ , 则称  $g$  是  $f$  的限制, 也称  $f$  是  $g$  的一个扩张, 记作  $g=f|_A$ 。

**定义 1.2.7** 设  $X_1, \dots, X_n$  是  $n \geq 1$  个集合,  $1 \leq i \leq n$ 。从笛卡儿积  $X=X_1 \times X_2 \times \dots \times X_n$  到它的第  $i$  个坐标集  $X_i$  的投射  $P_i: X \rightarrow X_i$  定义为对每一个  $x=(x_1, x_2, \dots, x_n) \in X$ ,  $p_i(x)=x_i$ 。

一个集合的等价关系能产生新的集合。由等价关系与划分之间的一一对应, 对应于等价关系  $\sim$  的划分通常记作  $S/\sim$ , 称为  $S$  关于  $\sim$  的商集。集合  $S$  到商集  $\sim$  存在一个自然映射(或典范投影):

$$p: x \rightarrow \bar{x}, x \in S$$

它是一个满射, 并且  $p(a) = p(b)$  当且仅当  $a \sim b$ 。

设  $X, Y$  是两个集合, 且  $f: X \rightarrow Y$  是一个映射。二元关系  $R_f$  定义为

$$\forall x_1, x_2 \in X, x_1 R_f x_2 \Leftrightarrow f(x_1) = f(x_2)$$

可检验  $R_f$  是  $X$  上的一个等价关系。对任意的  $x \in X$ ,  $\bar{x} = \{x' \mid f(x') = f(x)\}$ 。规定  $\bar{f}(\bar{x}) = f(x)$ , 则映射  $f: X \rightarrow Y$  诱导一个映射  $\bar{f}: X/R_f \rightarrow Y$ 。映射  $\bar{f}$  由  $\bar{f}p(x) = f(x)$  确定, 其中  $p$  是上面的自然映射。

### 1.3 偏序集合

**定义 1.3.1** 设  $X$  是一个非空集合,  $P$  是定义在  $X$  上的具有自反性、反对称性及传递性的二元关系。则称  $P = (X, P)$  为一个偏序集 (poset)。有时在不引起混淆的情况下, 也直接称  $X$  是一个偏序集。符合上述性质的关系称为偏序关系。

通常用  $x \leqslant y$  来描述  $X$  中的元素  $x, y$  满足偏序集  $(X, P)$  中  $P$  所规定的关系, 即  $(x, y) \in P$  记为  $x \leqslant y$ , 这样偏序集  $(X, P)$  也可写成  $(X, \leqslant)$ 。根据 “ $\leqslant$ ”, 自然地定义  $X$  上二元关系 “ $<$ ”:  $x < y$  表示  $x \leqslant y$  且  $x \neq y$ 。

**例 1.3.1** 设  $Z^+$  为全体正整数组成的集合。对于  $a, b \in Z^+$ , 规定  $a \leqslant b$  当且仅当  $a | b$ , 则易验证  $Z^+$  成为一个偏序集。

**例 1.3.2** 设  $S$  是一个集合,  $P(S)$  为  $S$  的幂集, 对于  $A, B \in P(S)$ , 规定  $A \leqslant B$  当且仅当  $A \subseteq B$ , 则易验证  $P(S)$  成为一个偏序集。当  $S$  是无限集时, 令  $P_f(S)$  表示  $S$  所有有限子集组成的集合, 对于  $A, B \in P_f(S)$ , 仍如上规定  $A \leqslant B$ , 则  $P_f(S)$  也是一个偏序集。

**例 1.3.3** 设  $V$  是域  $F$  上的一个线性空间,  $L(V)$  为  $V$  的所有子空间所组成的集合, 对于  $U, W \in L(V)$ , 规定  $U \leqslant W$  当且仅当  $U \subseteq W$ , 则易验证  $L(V)$  成为一个偏序集。当  $V$  的维数无限时, 令  $L_f(V)$  表示由  $V$  的所有有限维子空间所组成的集合, 对于  $U, W \in L_f(V)$ , 仍如上规定  $U \leqslant W$ , 则易见  $L_f(V)$  也是一个偏序集。

**定义 1.3.2** 偏序集的极小元是一个元素  $a$ , 使得没有异于  $a$  的元素  $x$  满足  $x \leqslant a$ , 即若有  $x \leqslant a, x \in X$ , 则必有  $x = a$ 。类似地, 一个极大元是一个元素  $b$ , 使得没有异于  $b$  的元素  $y$  满足  $b \leqslant y$ 。

设  $A$  为偏序集合  $S$  的一个子集, 元素  $a \in S$  称为  $A$  的一个下界, 如果对于所有的  $a \in A$  都有  $s \leqslant a$ 。类似的, 元素  $a \in S$  称为  $A$  的一个上界, 如果对于所有的  $a \in A$  都有  $a \leqslant s$ 。如果  $A$  有一个下界  $s$  且  $s \in A$ , 则  $s$  称为  $A$  的一个最小元素。如果  $A$  有一个上界  $s$  且  $s \in A$ , 则  $s$  称为  $A$  的一个最大元素。注意集合  $A$  可以没有下界或者有多个下界, 同样的,  $A$  可以没有最小(大)元素。但若  $A$  有最小(大)元素, 则它是唯一的。

下面我们叙述两个重要的等价原理: 极大原理和 Zorn 引理。

**极大原理** 设  $T$  为由集合  $S$  的若干子集组成的非空集合,  $T$  按包含关系成一个偏序

集合。如果  $T$  的每个链都有上界,则  $T$  有一个极大元素。

**Zorn 引理** 若一个偏序集  $S$  的每个链都有上界,则  $S$  有一个极大元素。

极大原理和 Zorn 引理有广泛的应用,它可以简化很多证明,也可以证明一些其他方法不能证明的结果。例如,我们可以证明平面上的任何有界区域  $D$  内皆有极大的开圆盘,证法如下:令  $S$  为  $D$  内所有开圆盘构成的集合,按照包含关系构成一个偏序集合。由于  $D$  内至少有一个开圆盘,所以  $S$  是非空的。如果一些开圆盘构成的集合  $\{D_i \mid i \in I\}$  成为一个链,则  $\bigcup_{i \in I} D_i$  也是  $D$  的一个开圆盘,且是此链的一个上界。于是根据 Zorn 引理,有界区域  $D$  内必有极大的开圆盘。

## 1.4 排列与组合

这一节我们介绍组合计数的最基本概念,主要取材于参考文献[9]。处理计数问题最基础的原理是加法原理和乘法原理,两者分别对应不同的情形和独立的步骤,是最为基本的想法。

**定理 1.4.1** (加法原理) 设  $S_1, \dots, S_m$  是集合  $X$  的一个划分,则

$$|X| = |S_1| + \dots + |S_m|$$

若完成一件事情有  $m$  个方案,第  $i$  ( $i=1, \dots, m$ ) 个方案有  $n_i$  种方法可以实现,那么完成这件事情共有  $n_1 + \dots + n_m$  种方法。

**定理 1.4.2** (乘法原理) 设  $S_1, \dots, S_m$  是  $m$  个有限集,则

$$|S_1 \times S_2 \times \dots \times S_m| = |S_1| \cdot |S_2| \cdots \cdot |S_m|$$

若完成一件事情需要  $m$  个步骤,第  $i$  ( $i=1, \dots, m$ ) 个步骤有  $n_i$  种方法可以实现,如果每个步骤中方法的选取均与前面的步骤无关,那么完成这件事情共有  $n_1 \cdot n_2 \cdots n_m$  种方法。

排列(permuation)与组合(combination)是计数理论中最基本的概念。把集合  $\{a_1, a_2, \dots, a_n\}$  中的  $n$  个元素排成一排,有  $n(n-1)\cdots 2 \cdot 1$  种不同的排法,即  $n!$ 。每一个这样的排列称为一个  $n$ -排列。而利用此集合中  $r$  个元素排成的一排,称为这  $n$  个元素的一个  $r$ -排列。 $n$  个不同元素的  $r$ -排列的个数为  $n(n-1)\cdots(n-(r-1)) = \frac{n!}{(n-r)!}$ 。以上结果可以看作是应用了乘法原理。

集合  $\{a_1, a_2, \dots, a_n\}$  中的元素通常默认为互异的。如果排列中允许有相同的元素,例如,把 3 个  $A$ , 2 个  $B$ , 4 个  $C$  和 1 个  $D$  这 10 个字母排成一排,有多少种不同的排法(即有多少个不同的长为 10 的字)?如果把这 10 个字母都看成是不同的,即 3 个  $A$  看成  $A_1, A_2, A_3$  等,则有  $10!$  个字,但这时这 3 个  $A$  的任一种排列都得到同一个字,其他的字母也是这样,所以最后的答案为  $\frac{10!}{3! 2! 4! 1!}$ 。这种排列称为有重复元素的排列。

类似地,由  $r$  个  $C$  及  $n-r$  个  $R$  可构成  $\frac{n!}{r! (n-r)!}$  个长为  $n$  的字。如果用  $C$  表示

“选取”,用  $R$  表示“拒绝”,则上面的问题可改成:“从  $n$  个不同的物体中选取  $r$  个的选法数是多少?”每一个这样的选取称为这  $n$  个元素的一个  $r$ -组合。注意到每一个(无序的) $r$ -组合对应着  $r!$  个(有序的) $r$ -排列( $r$ -组合有时候也称为  $r$  个元素的“无序排列”),所以  $n$  个元素的  $r$ -组合数等于  $\frac{n!}{r!(n-r)!}$ , 记为  $\binom{n}{r}$ (读作“ $n$  选取  $r$ ”)。因此,一个  $n$ -集合的所有  $r$ -子集个数为  $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ 。

现在,有重复元素的排列又可以看作是多重组合。一般地,将  $r_1$  个  $a_1$ ,  $r_2$  个  $a_2$ ,  $\dots$ ,  $r_k$  个  $a_k$  ( $r_1 + \dots + r_k = n$ ) 排成一排。这相当于在  $n$  个位置中选取出  $r_1$  个位置留给  $a_1$ , 再从剩下的  $n - r_1$  个位置中选取出  $r_2$  个位置留给  $a_2$ ,  $\dots$ , 最后的  $r_k$  个位置留给  $a_k$ 。因此,总的排法数为

$$\begin{aligned} & \binom{n}{r_1} \binom{n-r_1}{r_2} \binom{n-r_1-r_2}{r_3} \cdots \binom{n-r_1-\cdots-r_{k-1}}{r_k} \\ &= \frac{n!}{r_1!(n-r_1)!} \frac{(n-r_1)!}{r_2!(n-r_1-r_2)!} \cdots \frac{(n-r_1-\cdots-r_{k-1})!}{r_k!0!} \\ &= \frac{n!}{r_1!r_2!\cdots r_k!} \end{aligned}$$

称以上的取法数为多重选取数或多重组合数。

通过以上的讨论,可总结出关于排列、组合(即选取)和多重选取(即多重组合,或有重复元素的排列)的计数公式。

**定义 1.4.1** (排列)排列数即  $P(n, r) = n(n-1) \cdots (n-r+1) = \frac{n!}{(n-r)!}$ , 其计数的是在  $n$  个元素中取出  $r$  个排成一排的方法数。

**定义 1.4.2** (组合或选取)组合数,或称为选取数,即  $C(n, r) = P(n, r)/r! = \frac{n!}{(n-r)!r!} = \binom{n}{r}$ , 读作“ $n$  选取  $r$ ”,其计数的是从  $n$  个元素中选取  $r$  个的方法数。

一般地,如果  $n < r$ ,则默认  $P(n, r) = C(n, r) = 0$ 。事实上,这样的排列或组合原本就不存在。

**定义 1.4.3** (有重复元素的排列或多重选取)关于参数为  $n, r_1, \dots, r_k$  的多重选取数即  $\binom{n}{r_1, r_2, \dots, r_k} = \frac{n!}{r_1!r_2!\cdots r_k!}$ , 其中要求  $n = \sum_{i=1}^k r_i$ 。

显然,参数为  $n, r_1, r_2$  的多重选取数即  $\binom{n}{r_1, r_2} = \binom{n}{r_1} = C(n, r_1)$ 。

从  $n$  个不同元素中取出  $r$  个元素排成一个圆环,称为“环排列”。按某种固定的顺序

(如逆时针)看去,完全相同者被认为是同一个环排列(但  $a-b-c-a$  和  $a-c-b-a$  则被认为是不同的)。对固定的  $n$  个元素,取其中  $r$  个进行环排列,每一个环排列均对应  $r$  种不同的“直线排列”,且不同环排列展成的直线排列彼此也必不相同。注意到把全部环排列展开所得的直线排列,恰好就是全部的直线排列,因此可得到从  $n$  个元素中取出  $r$  个元素组成的环排列个数为  $\frac{n!}{(n-r)!} \cdot \frac{1}{r}$ 。特别地,将  $n$  个元素全部取出的环排列个数为  $\frac{n!}{n} = (n-1)!$ 。

**定义 1.4.4** (环排列) 从  $n$  个不同元素中取出  $r$  个排成一个圆环的方法数是

$$\frac{n!}{(n-r)!} \cdot \frac{1}{r}.$$

**例 1.4.1** 8 对夫妇坐成一排,每对夫妇要坐在一起,有多少种不同坐法? 若在圆桌旁就坐,有多少种不同坐法?

解:8 对夫妇排成一排(不考虑每对夫妇如何坐)有  $8!$  种安排,而每对夫妇有  $2! = 2$  种坐法,所以答案为  $2^8 \cdot 8!$ 。若这 8 对夫妇坐在一个圆桌旁,此时这 8 对夫妇排成一个圆排列有  $7!$  种方法,每对夫妇仍有  $2! = 2$  种坐法,答案为  $2^8 \cdot 7!$ 。

**例 1.4.2** 4 个 C 和 8 个 R 的排列中没有两个 C 是相邻的,有多少种这样的排列?

解:先把这 8 个 R 排成一排,这只有一种方式。然后再把 4 个 C 插入这些 R 的前后及中间这 9 个位置中。注意条件要求任意两个 C 不能相邻,即等价于这 9 个位置中每个位置最多插入一个 C。从而答案就是从 9 个位置中选出 4 个位置插入 C 的方法数,即

$$\binom{9}{4}.$$

在某些已排好物体的前后及中间位置上再加入其他物体,这种方法称为“插空法”,是一种简单而重要的计数方法。

**例 1.4.3** 把集合  $\{1, 2, \dots, n\}$  划分成  $b_1$  个 1 元集,  $b_2$  个 2 元集,  $\dots$ ,  $b_k$  个  $k$  元集, 其中  $\sum_{i=1}^k i b_i = n$ , 这样的分法有多少种?

解: $n$  个元素的全排列有  $n!$  种。而对于每个划分,其中  $b_i$  个  $i$  元集是没有顺序的,且划分中每个集合的元素也是没有顺序的,因此每个划分对应  $b_1! b_2! \cdots b_k! (1!)^{b_1} (2!)^{b_2} \cdots (k!)^{b_k}$  个不同的  $n$ -排列。所以答案为

$$\frac{n!}{b_1! b_2! \cdots b_k! (1!)^{b_1} (2!)^{b_2} \cdots (k!)^{b_k}}$$

或者从多重选取数出发,再考虑到划分得到的  $i$  元集彼此之间是没有顺序的,则有

$$\frac{\binom{n}{1, \dots, 1, 2, \dots, 2, \dots, k, \dots, k}}{b_1! b_2! \cdots b_k!}$$

种分法,这和上面的答案一样。(以上多重选取公式中的  $i$  有  $b_i$  个,  $1 \leq i \leq k$ 。)

注:进一步,一个  $n$  元集的全体划分数为

$$\sum_{b_1+2b_2+\cdots+nb_n=n} \frac{n!}{b_1!b_2!\cdots b_n!(1!)^{b_1}(2!)^{b_2}\cdots(n!)^{b_n}}$$

**例 1.4.4** 用  $p_n$  表示随机选取的  $n$  个人中至少有 2 人生日相同的概率(不考虑闰年的情况),则  $n$  最小为多少可使得  $p_n > \frac{1}{2}$ ?

解:容易计算  $n$  个人中任 2 人生日都不相同的概率为

$$\frac{365 \times 364 \times \cdots \times (365-n+1)}{365^n}$$

故

$$p_n = 1 - \frac{365!}{(365-n)! 365^n}$$

利用 Stirling 公式  $n! \approx n^n e^{-n} \sqrt{2\pi n}$ , 有

$$p_n \approx 1 - \left( \frac{365}{365-n} \right)^{365.5-n} e^{-n}$$

计算可知,最小的满足条件的  $n$  是 23。同样可以得到,若  $n \geq 41$ , 则  $p_n \geq 0.9$ 。

如果允许重复,那么从  $n$  个不同物体中选取  $r$  个物体排成一排的方法数当然是  $n^r$ 。那么组合数是多少?也就是说,如果  $n$  个不同物体中的每一个都可以被重复选取任意多次,那么选取一个基数是  $r$  的多重集有多少种方法?设第  $i$  个物体被选取了  $x_i$  次,则此问题等价于求方程

$$x_1 + x_2 + \cdots + x_r = r$$

的非负整数解的个数。这又等价于求包含  $r$  个“|”和  $n-1$  个“+”的序列个数(例如,|||++||+|| 就表示方程  $x_1 + x_2 + x_3 + x_4 = 7$  的一个非负整数解  $(3, 0, 2, 2)$ ),所以答案是  $\binom{r+n-1}{r}$ 。

**定理 1.4.3** 令  $S$  为具有  $n$  种类型元素的一个多重集,每种元素均可以被重复选取任意多次,则  $S$  的  $r$ -组合数为

$$\binom{r+n-1}{r}$$

**例 1.4.5** 一家面包房生产 8 种面包。如果将一打面包装进盒内,则一共可能有多少种不同的盒装组合?若每盒必定包含所有的 8 种呢?

解:由上述定理,所求结果依次为

$$\binom{12+8-1}{12} = \binom{19}{12}$$

及

$$\binom{4+8-1}{4} = \binom{11}{4}$$

**例 1.4.6** 方程  $x_1 + x_2 + x_3 + x_4 = 20$  满足  $x_1 \geq 3, x_2 \geq 1, x_3 \geq -1, x_4 \geq 0$  的整数解有多少个?

解:令  $y_1 = x_1 - 3, y_2 = x_2 - 1, y_3 = x_3 + 1, y_4 = x_4$ , 则问题等价于求方程  $y_1 + y_2 + y_3 + y_4 = 17$  的非负整数解的个数, 故所求解的个数为

$$\binom{17+4-1}{17} = \binom{20}{17}$$

按照前面的约定, 关于组合数  $\binom{n}{k}$ , 有

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!}, & n \geq k, \\ 0, & n < k. \end{cases}$$

**定理 1.4.4** (二项式定理) 设  $n$  为正整数, 则

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

二项式定理的证明有很多种, 可以用归纳法, 也可以考虑基本的组合意义, 这里就略过了。

今后, 组合数  $\binom{n}{k}$  也称为二项式系数。以下性质都是二项式定理显而易见的推论。

**性质 1.4.1** 设  $n \geq k \geq 0$ , 则

$$\binom{n}{k} = \binom{n}{n-k}$$

**性质 1.4.2** 设  $n \geq 0$ , 则

$$2^n = \sum_{k=0}^n \binom{n}{k}$$

**性质 1.4.3** 设  $n \geq 1$ , 则

$$0 = \sum_{k=0}^n (-1)^k \binom{n}{k}$$

**推论 1.4.1** 设  $n \geq 1$ , 则

$$\sum_{k \text{ 为奇数}} \binom{n}{k} = \sum_{k \text{ 为偶数}} \binom{n}{k}$$

下面给出推论 1.4.1 的一个组合证明。

**证明** 设

$$X = \{1, 2, \dots, n\}$$

$$A = \{S \subseteq X \mid |S| \text{ 为偶数且 } 1 \in S\}$$

$$B = \{S \subseteq X \mid |S| \text{ 为奇数且 } 1 \in S\}$$

$$C = \{S \subseteq X \mid |S| \text{ 为偶数且 } 1 \notin S\}$$

$$D = \{S \subseteq X \mid |S| \text{ 为奇数且 } 1 \notin S\}$$

构造映射  $f: A \rightarrow D$  为  $f(S) = S \setminus \{1\}$ , 显然  $f$  为双射, 所以  $|A| = |D|$ , 类似地  $|B| = |C|$ , 因此

$$\sum_{k \text{ 为奇数}} \binom{n}{k} = |B| + |D| = |A| + |C| = \sum_{k \text{ 为偶数}} \binom{n}{k}$$

**定理 1.4.5** (多项式定理) 设  $n$  为正整数, 则

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{n_1 + n_2 + \cdots + n_k = n} \binom{n}{n_1, n_2, \dots, n_k} x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$$

其中,

$$\binom{n}{n_1, n_2, \dots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}$$

即多重选取数, 今后也称为多项式系数。

**证明:** 只须考虑  $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$  在  $(x_1 + x_2 + \cdots + x_k)^n$  展开式中的系数, 并应用多重选取的定义。

**例 1.4.7** 确定  $(x_1 + x_2 + \cdots + x_5)^{10}$  的展开式中  $x_1^3 x_2^4 x_3^1 x_5^2$  的系数。

**解:** 根据多项式定理知, 所求系数应为

$$\binom{10}{3, 1, 4, 0, 2} = \frac{10!}{3! 4! 2!} = 12600$$

容斥原理又称筛法, 是一个古老而简便的工具。它是利用集合之间的交、并运算来对集合内元素计数的方法。例如, 假设  $A$  和  $B$  是两个有限集合, 我们熟知

$$|A \cup B| = |A| + |B| - |A \cap B|$$

**例 1.4.8** 某班有 100 人, 其中会打篮球的有 45 人, 会打乒乓球的有 53 人, 会打排球的有 55 人; 既会打篮球也会打乒乓球的有 28 人, 既会打篮球也会打排球的有 32 人, 既会打乒乓球也会打排球的有 35 人; 三种球都会打的有 20 人。问三种球都不会打的有多少人?

**解:** 设  $E_1 = \{\text{此班会打篮球的人}\}, E_2 = \{\text{此班会打乒乓球的人}\}, E_3 = \{\text{此班会打排球}$

的人},则由条件知: $|E_1|=45$ , $|E_2|=53$ , $|E_3|=55$ ; $|E_1 \cap E_2|=28$ , $|E_1 \cap E_3|=32$ , $|E_2 \cap E_3|=35$ ; $|E_1 \cap E_2 \cap E_3|=20$ 。

可如下算出三种球都不会打的人数。先从总人数中减掉会打三种球中某一种的人数;此时会打两种球的人被减掉了两次,为得到所求,应加上他们;第二步中会打三种球的人被加了三次,从而应再减一次。易知这样所得结果确是所求,即结果为

$$\begin{aligned} & 100 - |E_1| - |E_2| - |E_3| + |E_1 \cap E_2| + |E_1 \cap E_3| + |E_2 \cap E_3| - |E_1 \cap E_2 \cap E_3| \\ & = 100 - 45 - 53 - 55 + 28 + 32 + 35 - 20 = 22 \end{aligned}$$

所以三种球都不会打的有 22 人。

对于此类问题,可借助文氏图(Venn Diagram)来获得直观的解答,也可以选择集合的角度,本题中根据条件得到了 7 个关于集合的等式后,可设只会打某一种球、只会打某两种球、三种球都会打的人数为 7 个未知量,由上述等式列出 7 个线性方程,通过解这个线性方程组求得各部分的人数。但这种方法不具备一般性,无法引出容斥原理的思想。

**例 1.4.9** 求 1 到 500 中不能被 2 和 3 整除的整数个数。

解:这是熟知的初等问题。答案是

$$500 - \left\lfloor \frac{500}{2} \right\rfloor - \left\lfloor \frac{500}{3} \right\rfloor + \left\lfloor \frac{500}{6} \right\rfloor = 167$$

**定理 1.4.6** (经典的容斥原理) 设  $S$  为一有限集,  $P = \{P_i, \dots, P_m\}$  为一族性质。对  $\{1, \dots, m\}$  的任一子集  $I$ , 令  $X_I$  表示  $S$  中满足性质  $P_i$  (对所有  $i \in I$ ) 的那些元素构成的集合。特别地,  $I = \{i\}$  时, 简记  $X_{\{i\}}$  为  $X_i$ 。记  $\overline{X_I} = S \setminus X_I$ 。则集合  $S$  中不具有  $P$  中任何一种性质的元素个数由下式给出:

$$\begin{aligned} |\overline{X_1} \cap \overline{X_2} \cap \dots \cap \overline{X_m}| &= |S| - \sum_i |X_i| + \sum_{i < j} |X_i \cap X_j| - \sum_{i < j < k} |X_i \cap X_j \cap X_k| \\ &\quad + \dots + (-1)^m |X_1 \cap X_2 \cap \dots \cap X_m| \\ &= \sum_{I \subseteq [m]} (-1)^{|I|} |X_I| \end{aligned} \quad (*)$$

证明: 对任意  $x \in S$ , 记集合  $[m] = \{1, \dots, m\}$ ,  $J_x = \{i \in [m] \mid x \in X_i\}$ 。按  $J_x$  是否为空集讨论:

(i)  $J_x = \emptyset$ , 即  $x$  不在任意一个  $X_i$  中。此时  $x$  对(\*)式左端的贡献为 1; 对于右端,  $x$  仅对  $|S|$  贡献 1, 对其余和式贡献为 0, 从而  $x$  对右端贡献也为 1。故(\*)式成立。

(ii)  $J_x \neq \emptyset$ , 即  $x$  在某些  $X_i$  中。设  $j = |J_x|$ , 则  $j > 0$ 。此时  $x$  对(\*)式左端的贡献为 0; 对于右端, 注意  $x \in X_I$  等价于  $I \subseteq J_x$ , 从而  $x$  对(\*)式右端的贡献为

$$\sum_{I \subseteq J_x} (-1)^{|I|} = \sum_{i=0}^j (-1)^i \binom{j}{i} = (1-1)^j = 0$$

故(\*)式成立。

综合(i)和(ii), 定理成立。

容斥原理是一个很有用的计数原则, 它的另一表述为, 设  $S$  是一个  $n$  元集,  $E_1$ ,