**Abstract Algebra**

zty

2020.6

**Chapter 1 Relations and Functions**

1.1 Sets and Set Operations

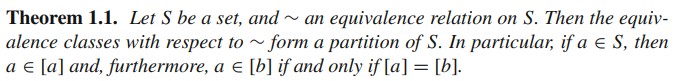
集合，元素，空集，非空集合，子集，真子集proper subset，交集，并集，差集，笛卡尔积

1.2 Relations

关系，反身性reflexive，对称性symmetric，传递性transitive

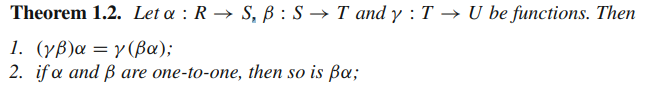
1.3 Equivalence Relations

等价关系，等价类，划分partition

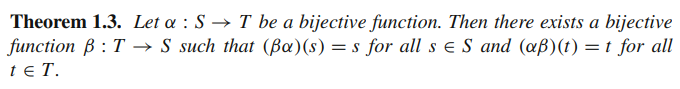


1.4 Functions

函数，单射injective，满射surjective，一一映射bijective，函数的复合，反函数





 置换permutation是双射，二元运算binary operation

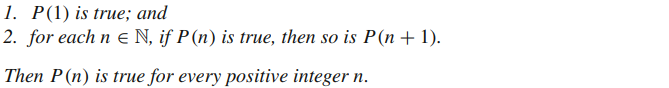
**Chapter 2 The Integers and Modular Arithmetic**

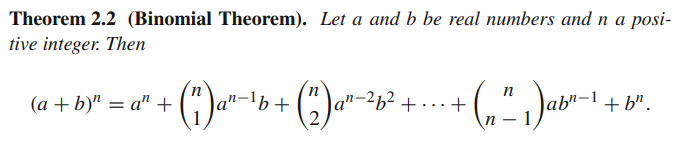
2.1 Induction and Well Ordering

命题proposition，数学归纳法Principle of Mathematical Induction，二项式定理Binomial Theorem，强归纳法Strong Induction

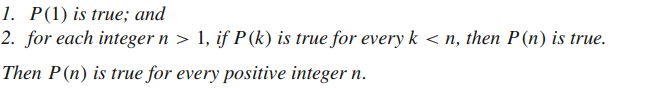








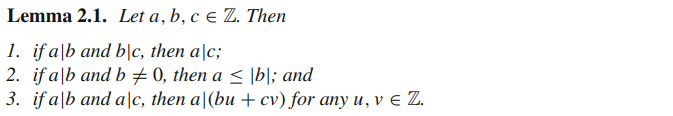




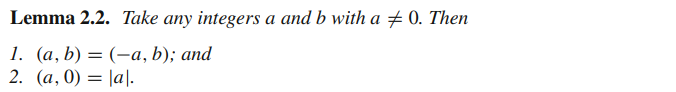
2.2 Divisibility



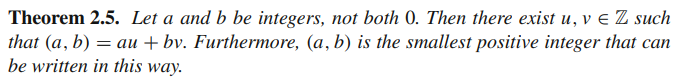
商quotient，余数remainder，整除divides，倍数multiple，整除的表示a | b



最大公约数greatest common divisor (gcd)，written (a, b)



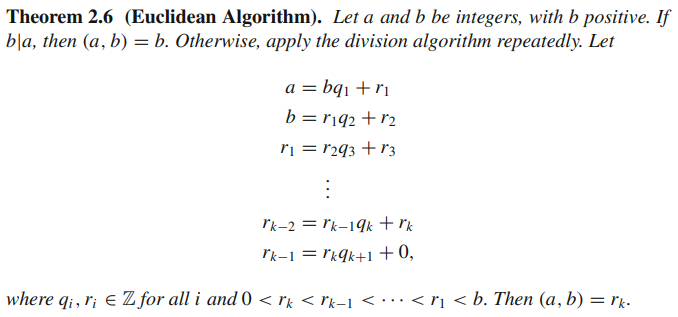
互质relatively prime





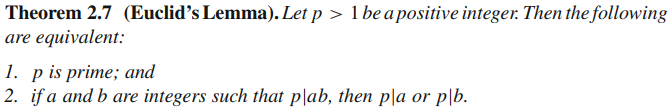




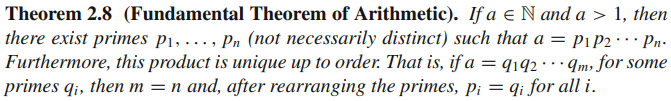


2.3 Prime Factorization

质数prime，合数composite，质因数分解prime factorization









2.4 Properties of the Integers

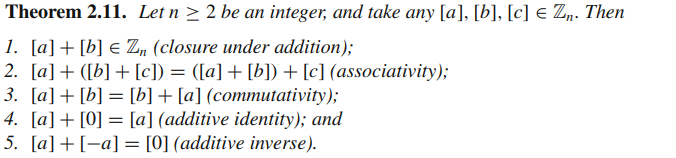
整数上加法与乘法的封闭性closed、结合性associative、可交换性commutative、分配律distributive law，加法单位元additive identity，乘法单位元multiplicative identity，加法逆元additive inverse，乘法逆元multiplicative inverses一般不存在

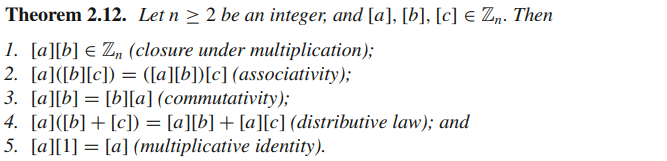
2.5 Modular Arithmetic

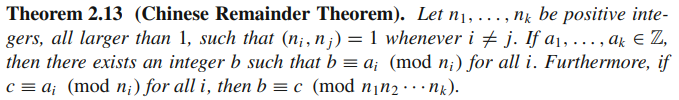
a与b模n同余congruent to b modulo n，模n剩余类integers modulo n，定义其加法和乘法







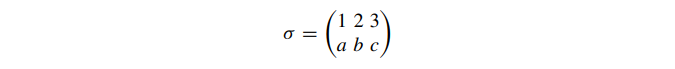




**Chapter 3 Introduction to Groups**

3.1 An Important Example

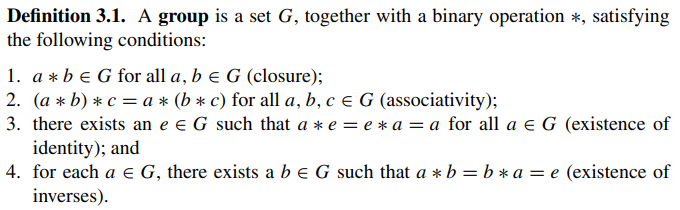
有限集合置换的表示法



置换的封闭性closure即置换的复合还是置换，置换的结合性associativity，恒等置换identity，逆置换inverse

n次对称群Sn symmetric group on n letters指的是由n个元素组成的集合中的所有双射构成的群，置换群为n次对称群的子群

3.2 Groups



单位元identity，逆元inverse，交换群/加群/Abel群，群的运算表示group table



例3.3：欧拉函数构成的群U(n)，为小于正整数n且与n互素的所有正整数的集合在模n乘法下构成的群，是交换群/Abel群

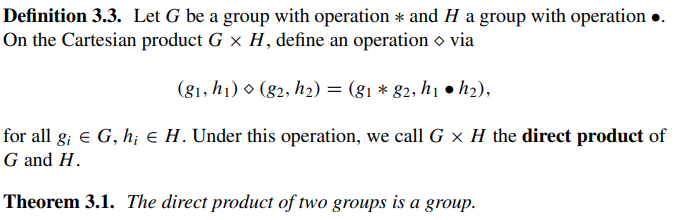
例3.4：单位根群，为n次单位根在乘法下构成的群，是循环群、交换群/Abel群。

平凡群trivial group为一元群，即只含单位元的群

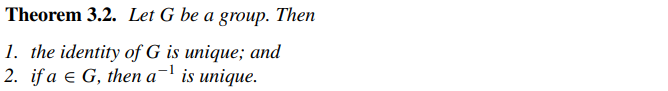
例3.5：n次对称群当n≥3时Sn为非交换群

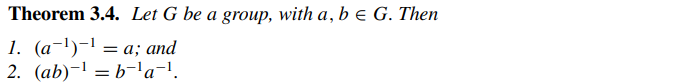
例3.6：一般线性群general linear group，written GLn(F)为数域F上n维可逆矩阵构成的群

群的直积direct product



3.3 A Few Basic Properties



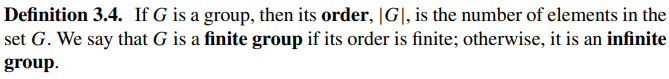


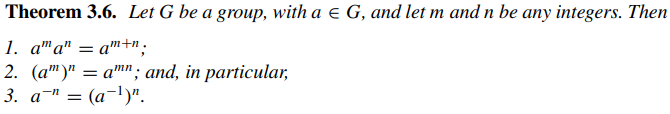
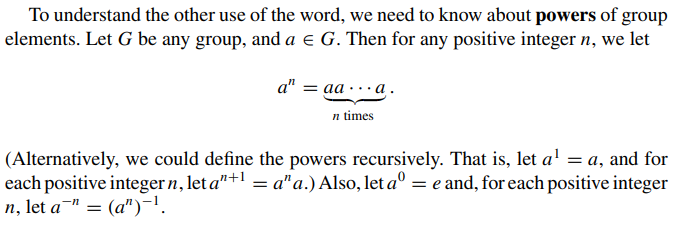


消去律告诉我们，在运算表中的每行、每列都是元素的一个排列，不含相同的元素。

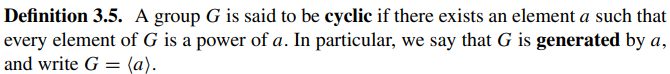


3.4 Powers and Orders

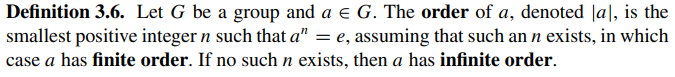




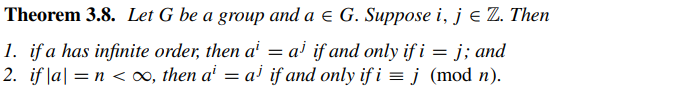
循环群cyclic group的定义为任何一个元素都可以表示为某一个元素a的幂次，称为由a生成的循环群，循环群是交换群。

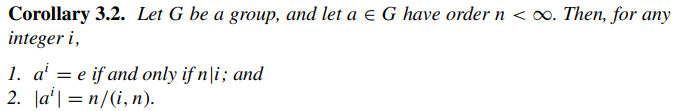


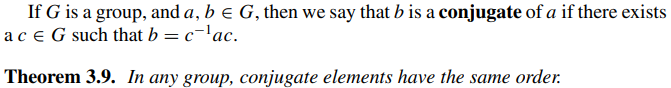




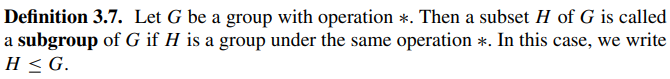
群的阶为群中元素的个数；元素的阶为元素的最小幂幺指数，且为群的阶的因数，元素与其逆元的阶相同。

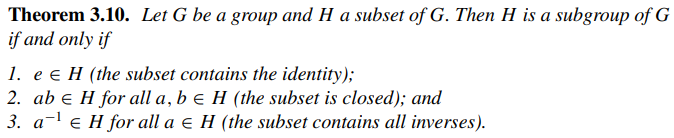




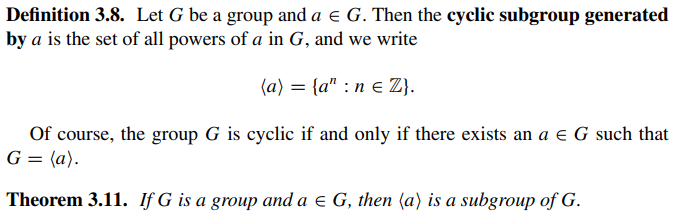


3.5 Subgroups

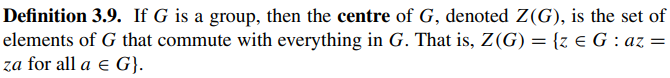




循环子群cyclic subgroup generated by a

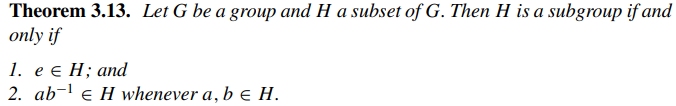


群的中心指的是群中与所有元素可交换的元素的集合。

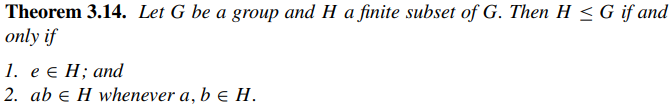




上述定理表明，群的中心是子群。

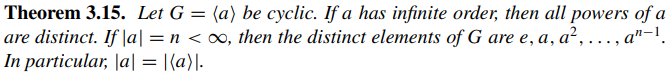


上述定理给出了子群的成立条件。



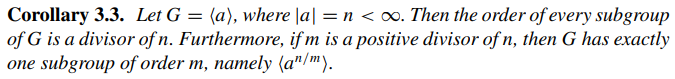
例：8阶二面体群D8

3.6 Cyclic Groups

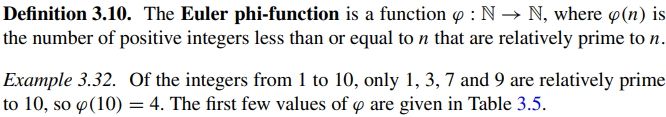


一个循环群如果阶数有限，则与模n剩余类加群同构；如果阶数无限，则与整数加群同构。



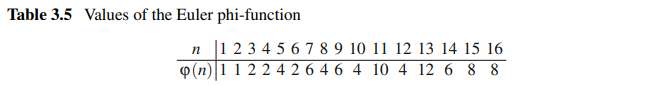


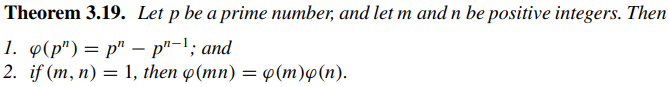
这个推论说明了，有限循环群的子群的阶数都是该群的因数。一个n阶循环群的固定阶子群是唯一的。例如Z6的2阶子群有且只有Z2。







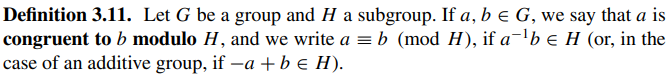




对于n阶循环群，其生成元有φ(n)个。补充定理：如果群G是n阶有限群。若对n的每一个因子m，G至多只有一个m阶子群，则G是循环群。

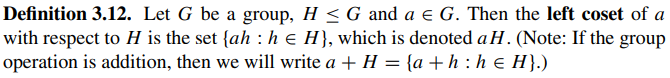
3.7 Cosets and Lagrange’s Theorem

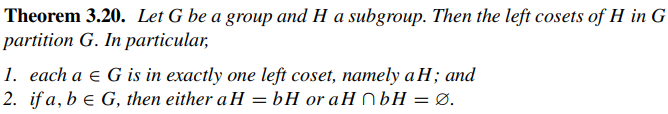
对于某个子群H的左右陪集的含义，个数相等











Lagrange定理：有限群的子群的阶都整除群的阶，这个倍数即为该子群对应陪集的个数，称为H在G中的指数

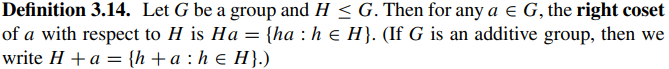












上述定理表明，子群的阶数整除群的阶数。

**Chapter 4 Factor Groups and Homomorphisms**

4.1 Normal Subgroups

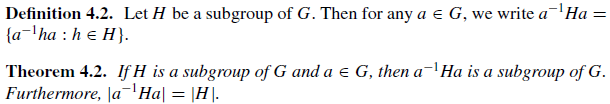
我们希望一个子群的陪集按某种运算可以构成群，但未必如此。

正规子群normal subgroup

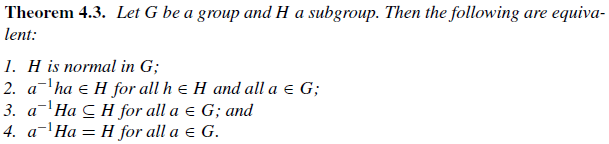


只含单位元的子群和群的中心都是正规子群。交换群的子群都是正规子群。





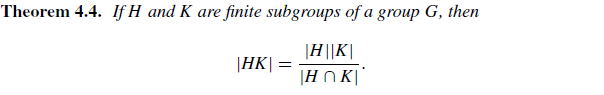
正规子群的判定方法通常用下述定理的第4条：



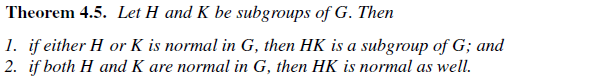
例4.5：设SLn(R)表示所有n阶一般线性群中行列式为1的矩阵，称为特殊线性群special linear group，它是一般线性群的正规子群。

指数为2的子群是G的正规子群。



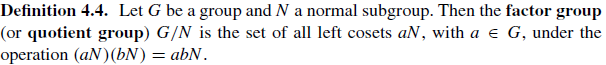


这里，如果H和K中有正规子群，则HK是一个子群。



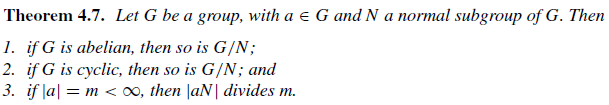
4.2 Factor Groups

商群factor group/quotient group，指的是正规子群的所有陪集构成的群。

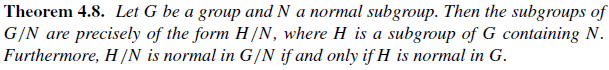




显然，商群的阶数是陪集的个数，也即指数，可以整除原群的阶数。



注意，a的阶数未必等于aN的阶数。

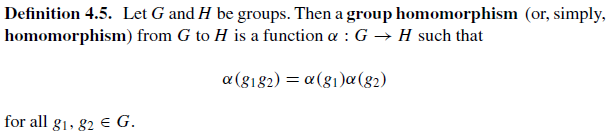


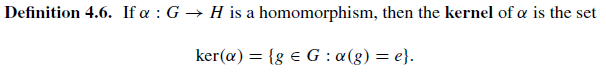


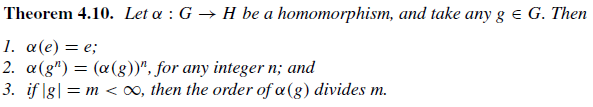


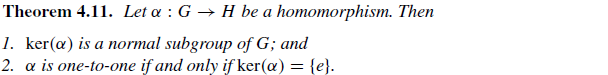
4.3 Homomorphisms

群同态group homomorphism，映射的核kernel

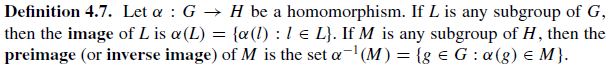


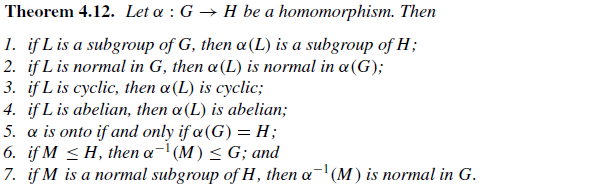






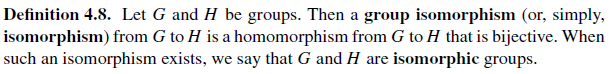
上述定理告诉我们，同态映射的核是原群的正规子群；通过核可以判断同态映射是否为单射。





4.4 Isomorphisms

群同构group isomorphism，映射的核kernel





判断群同构的方法：构造两个群之间的同态映射，验证其良定义性，并证明其为一一映射。





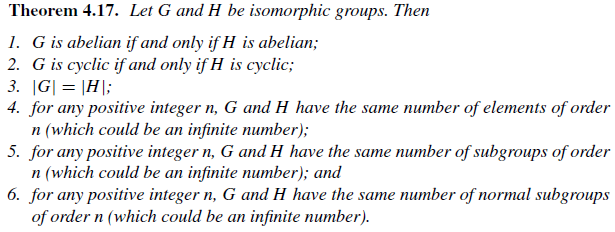












4.5 The Isomorphism Theorems for Groups

三个群同态基本定理

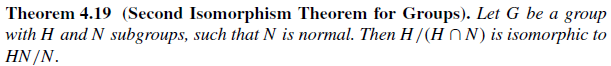


群同态第一定理表明了，同态映射使得原群对于映射核的商群，与像群同构。群G的任何一个同态像群，都同构于G的一个商群。当需要证明同构时，只要构造一个核为N的同态映射即可，而不需要考虑在陪集上定义映射的良定义性。

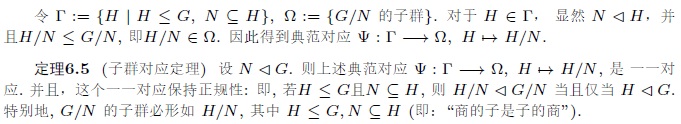
例1：典范同态或自然同态。设N是群G的正规子群，则定义映射f：g→gN，显然N就是f的核。映射的像是G/N，即这是一个群到商群的满同态。

例2：满同态det：GLn(R)→R\*，该映射的核为SLn(R)

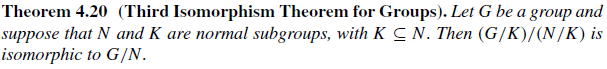
例3：Z/nZ与Zn同构。



首先给出一个子群对应定理。

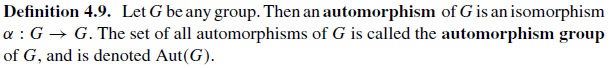


群同态第二定理中注意，N是HN的正规子群，从而有商群HN/N。考虑群的从H到HN/N满同态映射h→hN，其核为H与N的交集，由群同态第一定理可证明第二定理。

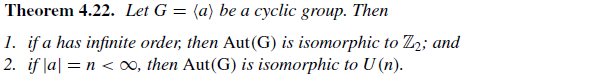


4.6 Automorphisms

自同构automorphisms，所有的自同构可以做成一个群Aut(G)

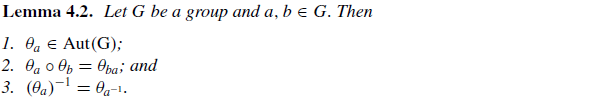




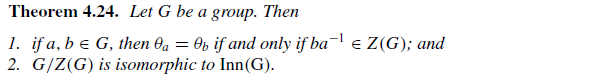


内自同构inner automorphism





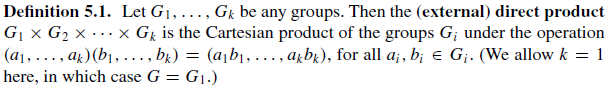




**Chapter 5 Direct Products and the Classification of Finite Abelian Groups**

5.1 Direct Products

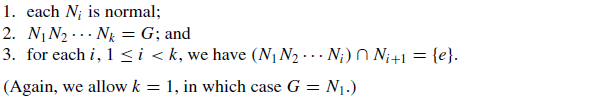
外直积external direct product，内直积internal direct product





此处外直积中的“外”表明这些群Gi并不是直积结果的子群，也不是子集合。虽然可以构造出外直积的一个子群可以使Gi与之同构，即



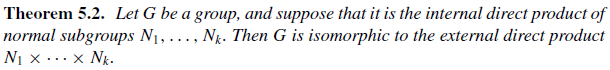


内直积说明是由一个大群构造出一系列正规子群，内直积中的积即为原始群中的乘法。





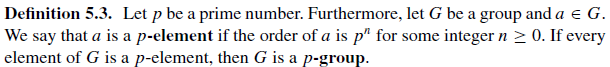




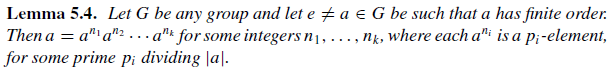
该定理说明，一系列正规子群的内直积与外直积同构。因此在书写时可以将内直积写成外直积的形式。

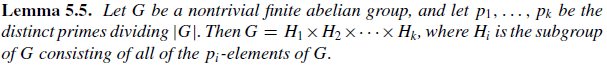
5.2 The Fundamental Theorem of Finite Abelian Groups

p-群p-group，即每个元素的阶都是同一个质数p的幂









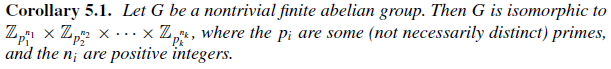
上述定理说明，任何一个有限交换群都可以做成一系列子群的外直积，这些子群是由G中的p-元素构成的。

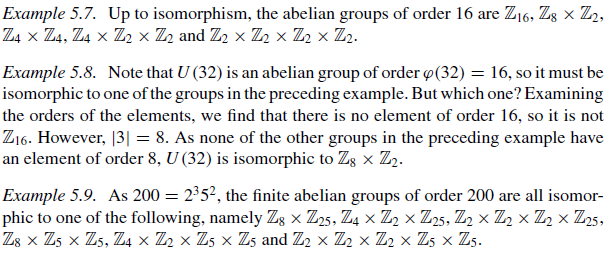






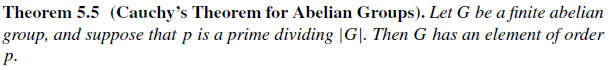
上述定理说明，有限交换p-群可以做成一系列循环群的外直积。







上述定理表明，如果分解出的循环子群的阶数两两互质，则该群是循环群。而相同阶数的循环群都同构于Zn，因此Z200与Z8×Z25同构。





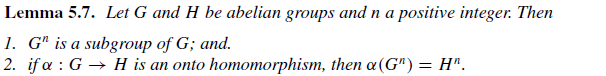
5.3 Elementary Divisors and Invariant Factors

初等因子elementary divisors，不变因子invariant factors



上述定理表明，根据群的阶的质因数分解可以得到直积表达的初等因子组。





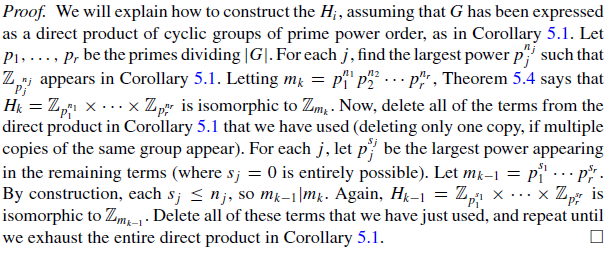


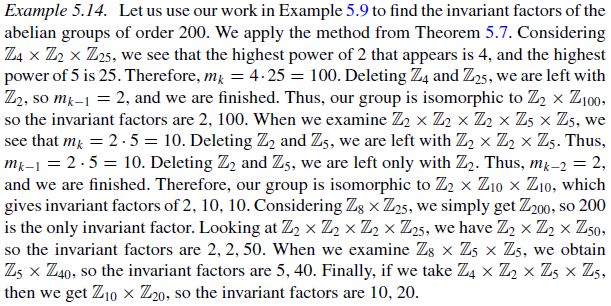
上述定理表明，两个有限阶Abel群同构等价于其初等因子组相同。





不变因子的构造方法如下：







5.4 A Word About Infinite Abelian Groups

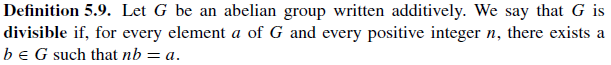
The word is messy.





该定理表明，有限Abel群不可分解的条件是该群为循环p-群。





**Chapter 6 Symmetric and Alternating Groups**

6.1 The Symmetric Group and Cycle Notation

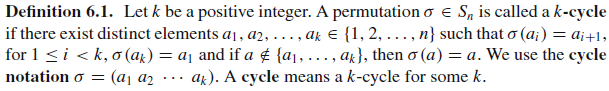
有限n次对称群symmetric group的阶为n！，包括了n元集合的所有置换（一一映射）。

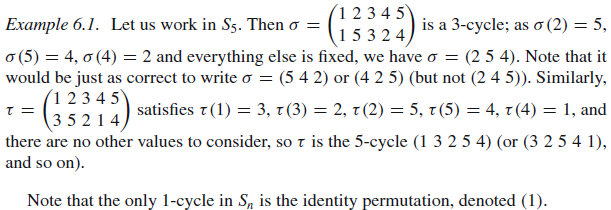


上述定理中P(G)表示G上所有的一一映射。定理表明，任一个群都同构于某个变换群；任一个有限群都同构于某个置换群。

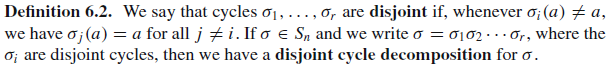


k-循环置换k-cycle











上述定理表明，可以把任何一个置换分解成几个不相连的循环置换。





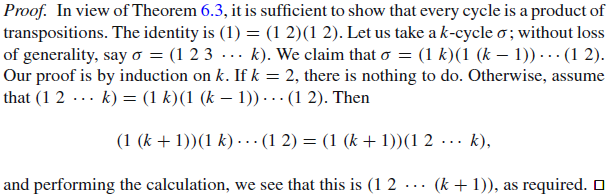


上述定理表明，几个不相连的循环置换之积的阶是其长度的最小公倍数。

6.2 Transpositions and the Alternating Group

对换transposition











置换的奇偶性：若一个置换能分解成奇数个对换的乘积则称为奇置换（或轮换的长度为偶数）



交错群alternating group





共轭类：将置换写成互不相交的轮换的乘积，其中长为i的轮换有mi个，则可以将(m1,m2,…,mn)称为置换的型。两个置换共轭当且仅当其型相同。

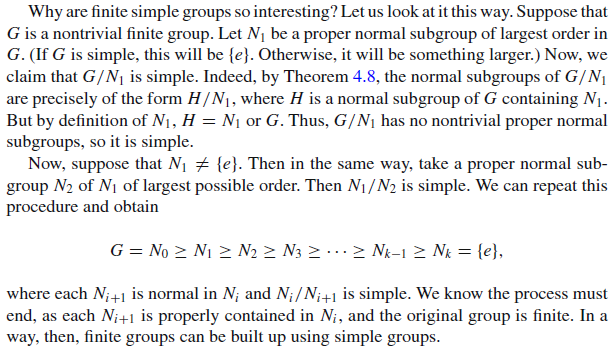
6.3 The simplicity of the Alternating Group

单群simple group



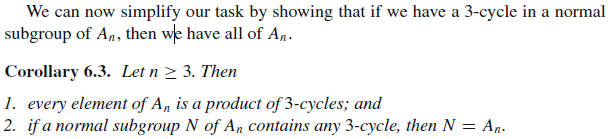


上述定理表明，如果一个群是交换群，则它是单群当且仅当它是质数阶循环群。但非交换群的情况格外复杂，这里只考虑5阶及以上的交错群。A5是最小的非Abel单群，且每个60阶单群都与A5同构。第二小的非Abel单群是射影特殊线性群PSL(2, 7)，阶为168。研究有限单群的意义在于可以构造一系列正规子群链，详细解释如下。最大的散在单群为魔群。



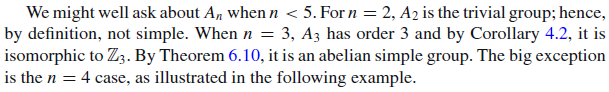


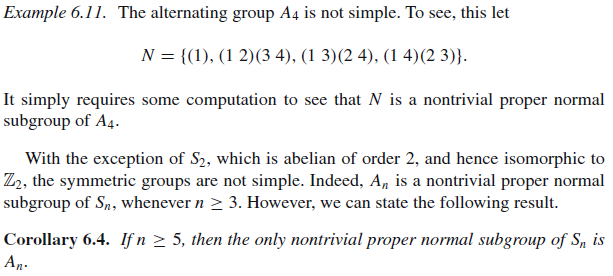






上述定理证明过程较长。



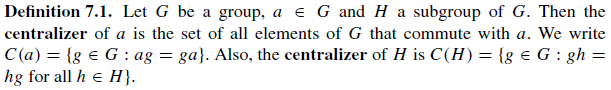


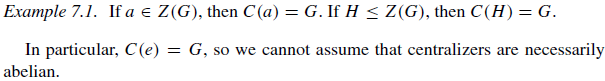
上述推论指出，Sn的非平凡正规子群只有交错群An。

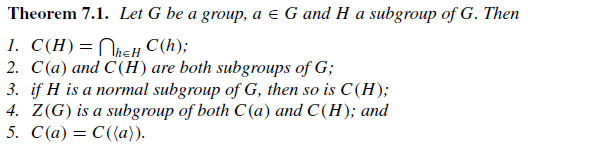
**Chapter 7 The Sylow Theorems**

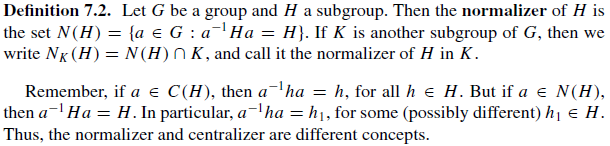
7.1 Normalizers and Centralizers

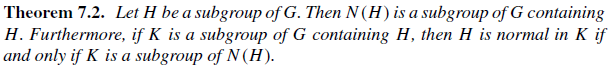
中心化子centralizer，正规化子normalizer

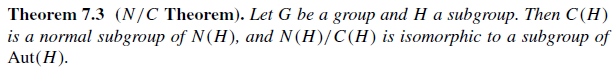






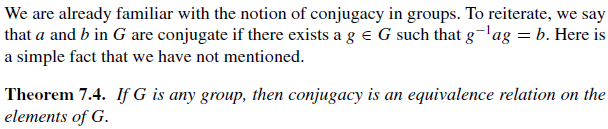






7.2 Conjugacy and the Class Equation

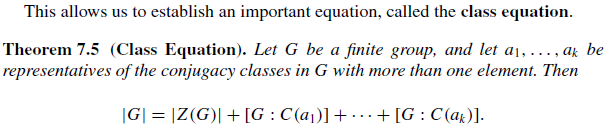
共轭conjugacy





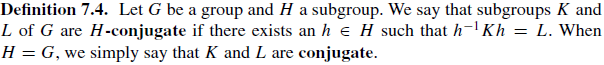
注意，共轭类是G的子集而非子群。









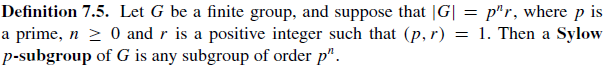






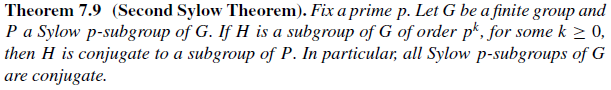
7.3 The Three Sylow Theorems

Sylow p-子群

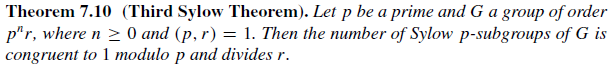




Sylow第一定理表明，任何一个有限群都至少有一个Sylow p-子群。



Sylow第二定理表明，Sylow p-子群总是共轭存在的。



Sylow第三定理表明，G的Sylow p-子群的个数模p余1且能被G的阶数整除，即能被r整除。

7.4 Applying the Sylow Theorems



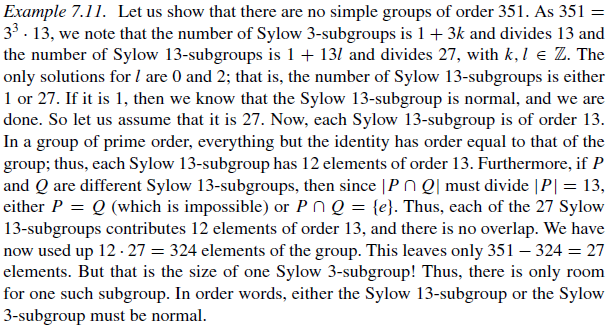






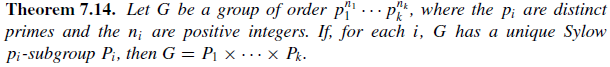
上述定理的特殊形式：如果在以上条件下还有p不整除q-1，则pq阶群为循环群。

例子：分析351阶群的Sylow p-子群。





上述定理表明，如果一个群的阶数是三个互不相同质数的乘积，则它不是单群。



上述定理表明，G中的每个元素都可以写成p-元素的乘积，即G可以写成一系列Sylow p-子群的内直积。

7.5 Classification of the Groups of Small Order

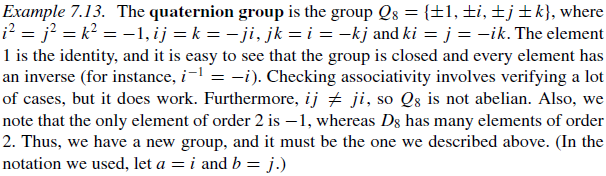
本节研究所有阶数为1至15的群的结构。

1阶群为平凡群，只含单位元。根据推论4.2，{2, 3, 5, 7, 11, 13}阶群为循环群，都与Zn同构。根据推论7.2，{4, 9}阶群是p2-子群，例如4阶群与Z4或Z2×Z2同构。根据定理4.15，{6, 10, 14}阶群的阶数为2p，与Z2p或D2p同构。还剩阶数为8、12、15的群。



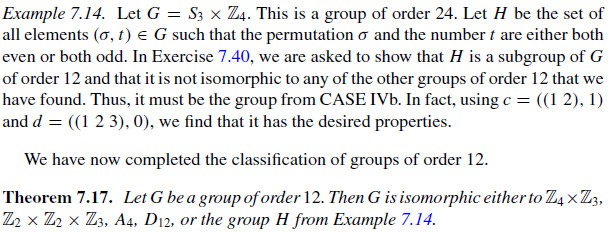
证明：根据Sylow第三定理，Sylow 3-子群的数量为1+3k且能整除5，因此k=0，只有一个Sylow 3-子群。而根据定理7.12，阶数3×5的群中Sylow 5-子群正规，但正规的Sylow 5-子群表明Sylow 5-子群只有一个。根据定理7.14，15阶的子群都可以分解成Z3和Z5的外直积。而由于互质，Z15与Z3×Z5同构。

对于8阶群，根据推论5.1已经知道，8阶交换群同构于{Z8, Z4×Z2, Z2×Z2×Z2}中的一个。对于8阶非交换群，群中的非单位元的阶数总为2、4或8，但如果某个元素阶数为8，则该群是循环群，从而是交换群。如果群中的非单位元阶数都是2，则群也是交换群（习题3.32）。因此8阶非交换群中总存在一个阶数为4的非单位元。接下来的构造过程略。





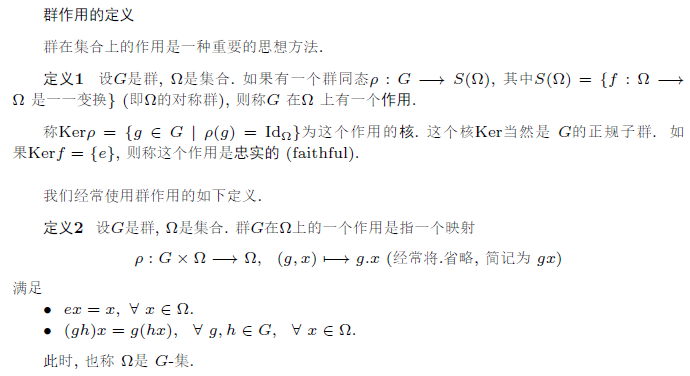
对于12阶群，其Sylow 3-子群的个数为1+3m且整除4，因此数量为1或4。同理，Sylow 2-子群的个数为1或3。

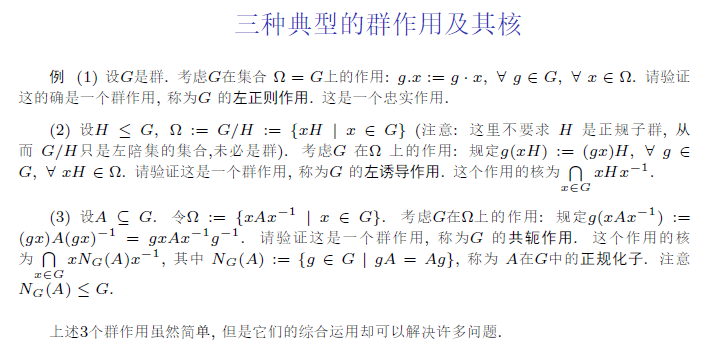


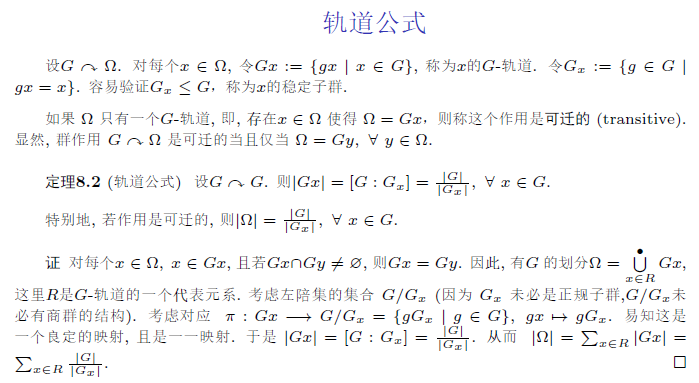
群论补充部分

（一）群在集合上的作用

群作用的定义







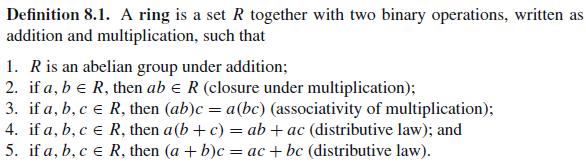
**Chapter 8 Introduction to Rings**

8.1 Rings

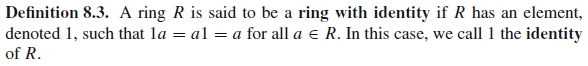
环ring，交换环commutative ring，含幺环ring with identity

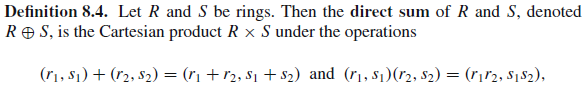
环的例子：整数环、有理数环、实数环、复数环、偶数环、一元多项式环、n阶矩阵环

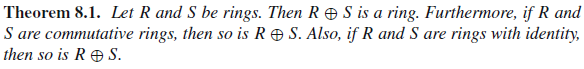
直和direct sum







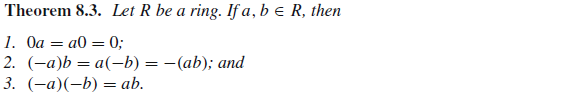




注意到，一个环对于加法是群，对于乘法是半群，因此环未必含乘法单位元和逆元。

8.2 Basic Properties of Rings







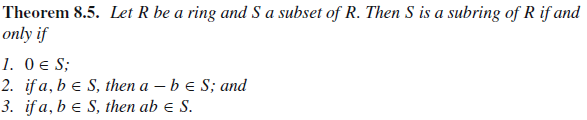


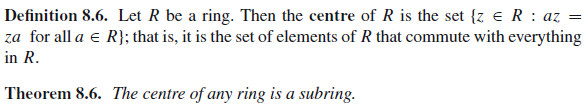
注意到，环的乘法运算没有消去律。如果为了检验一个元素a是乘法单位元，必须确保对于任意的元素b，有ab = b = ba成立。

8.3 Subrings

子环subring，含幺子环unital subring









8.4 Intergral Domains and Fields

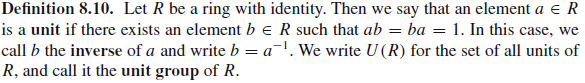
零因子zero divisor，整环integral domain，单位群unit group





上述定义等价于，整环满足三个条件（1）可交换（2）含非零元素（3）无零因子环





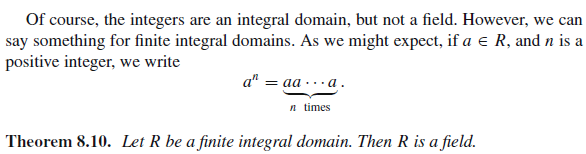


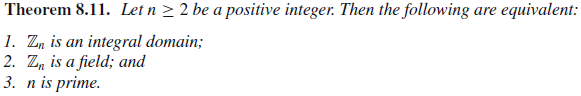
域field，子域subfield





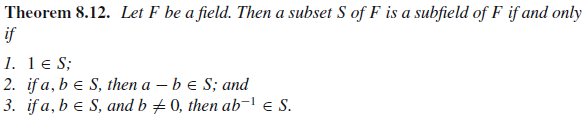




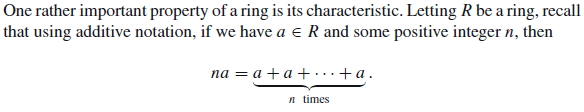


证明：如果n不是质数，则显然存在两个非零元素的乘积为0。

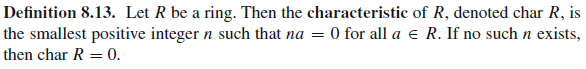




8.5 The Characteristic of a Ring



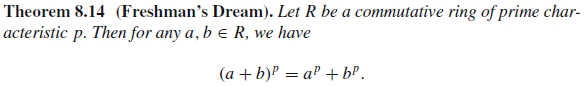
环的特征characteristic





上述定理表明，在一个含幺环中，环的特征等于乘法单位元的有限阶数，否则等于零。







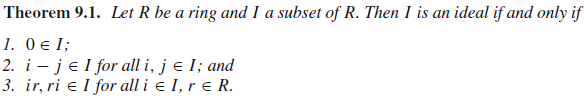
上述定理表明，整环的特征为0或质数。

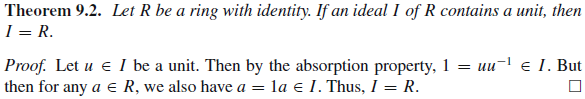
**Chapter 9 Ideals, Factor Rings and Homomorphisms**

9.1 Ideals

理想子环ideal，吸收律absorption property

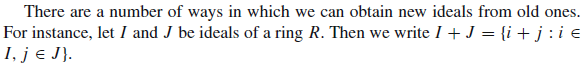




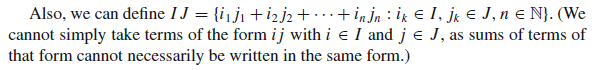




上述推论表明，域只有平凡理想。不仅如此，除环也只有平凡理想。

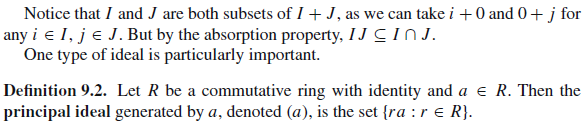




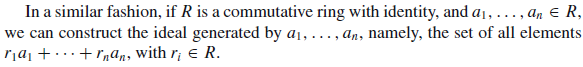




主理想principal ideal



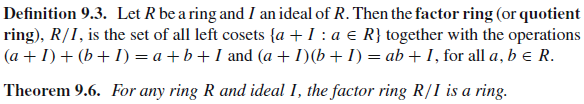




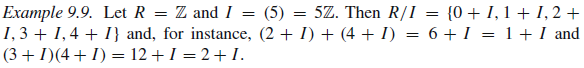
注意上述定义和定理中的前提为交换环和含幺环。

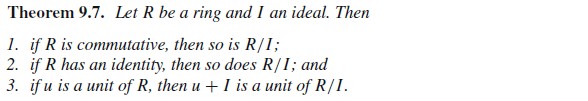
9.2 Factor Rings

商环factor ring



上述定义和定理表明，可以根据理想做成环的左右陪集，理想子环与正规子群对应。

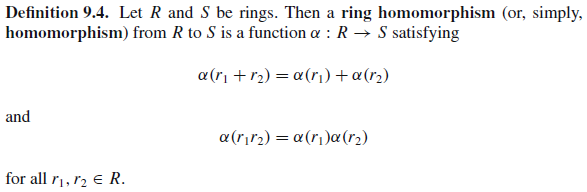






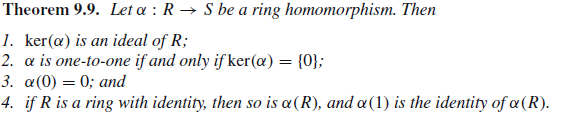
9.3 Ring Homomorphisms

环同态ring homomorphism

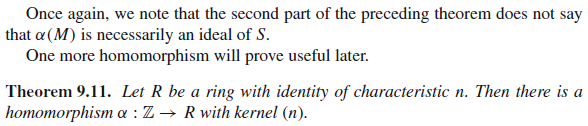






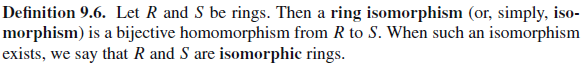


注意，上述定理中的第四条性质，并不是值域S而是像集中的单位元。



9.4 Isomorphisms and Automorphisms

环同构ring isomorphism



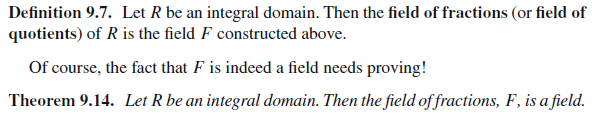




对于一个环R，其子环未必是一个域。事实上，如果R是一个整环，则可以构造一个包含同构于R的环的域，构造的方式与所谓的除法有关。具体方式为定义一个等价关系(a, b) ~ (c, d)满足ad = bc，具体方式如下：



分式域field of fractions





自同构automorphism





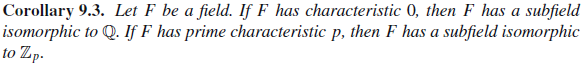
9.5 Isomorphism Theorems for Groups

三个环同态基本定理



上述定理与群同态第一定理类似。环同态第一定理表明了，同态映射使得原群对于映射核的商环，与像环同构。当需要证明同构时，只要利用环同态第一定理即可。





素子域prime subfield







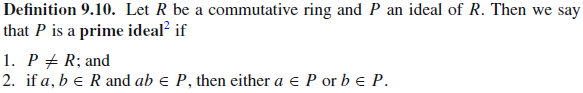
上述三个定理都与群同态基本定理类似。

9.6 Prime and Maximal Ideals

极大理想maximal ideal，素理想







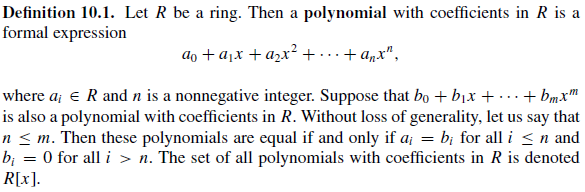




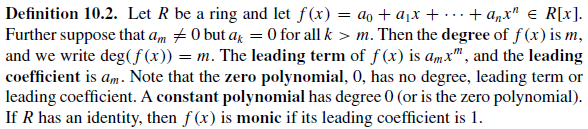
**Chapter 10 Special Types of Domains**

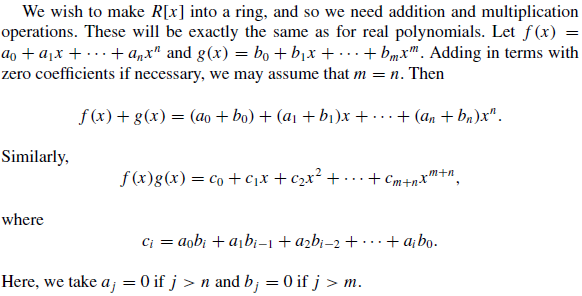
10.1 Polynomial Rings

多项式polynomial

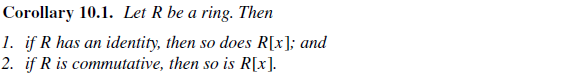


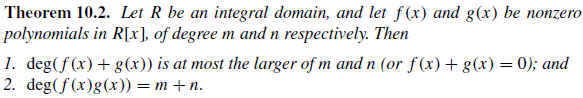
关于多项式的一些定义如下：









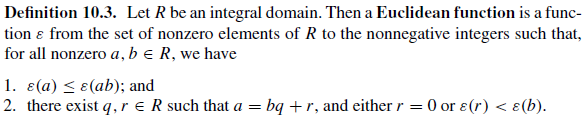




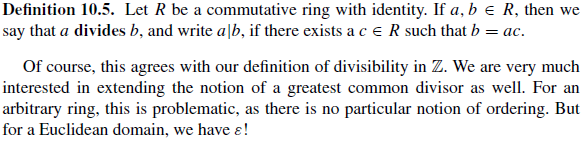


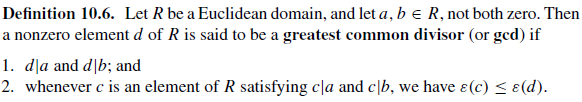
10.2 Euclidean Domains

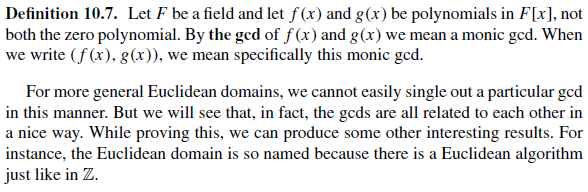
欧几里得整环Euclidean domain



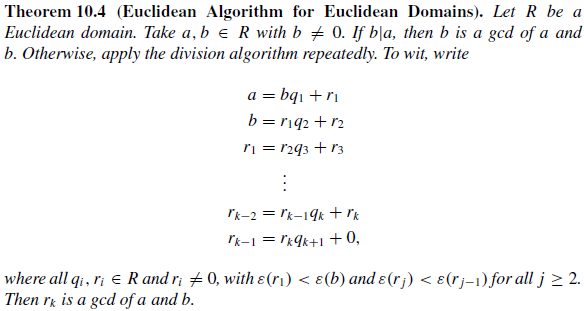


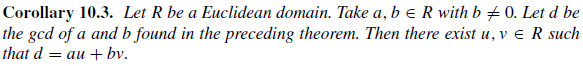


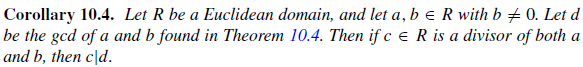


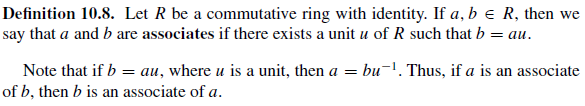


欧几里得算法

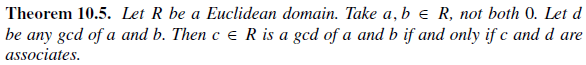




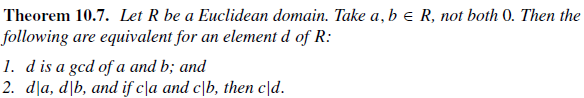






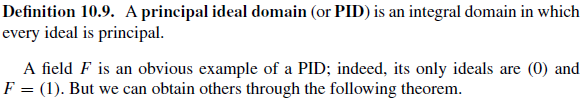




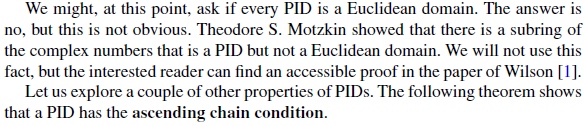


10.3 Principal Ideal Domains

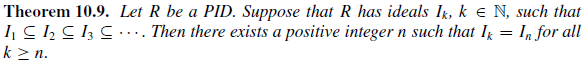
主理想整环principal ideal domains





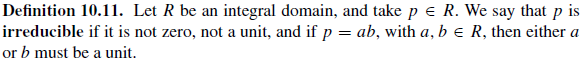


主理想整环的升链

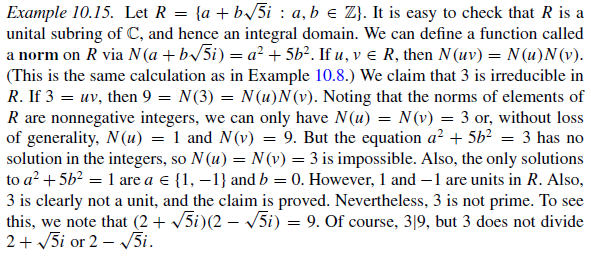


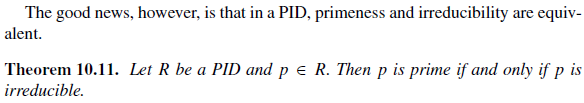












10.4 Unique Factorization Domains

唯一因子分解域unique factorization domain





