作业答案或提示

习题1

1.略

2.此题有同学想简单的用势来说明, 其实是不对的. 因为即使维数不同的有限维线性空间也有相同的势. 这里可以根据线性空间的性质,

$$\dim \mathrm{Ker} f + \dim \mathrm{Im} f = n$$

3. 映射有n^m个；$m > n$时, 0个单射, 反之有A_n^m个单射；有m^{m^2}个二元运算.

5.每个实对称阵合同对角元素为0, ±1的对角矩阵. 等价类有（n+2）（n+1）/2个

6.每个实对称矩阵可以正交相似与对角矩阵, 对角元为矩阵的特征值, 对角元顺序改变不影响相似. 注意：有同学等价类写成

$$\begin{bmatrix} x_1 & & & \\ & x_2 & & \\ & & \ddots & \\ & & & x_n \end{bmatrix}$$

$x_1, \ldots, x_n$为任意实数. 这是不严谨不准确, 应该要说明其中的对角元素位置可以改变, 也可以给它规定一个顺序, 如：$x_1 \leq \cdots \leq x_n$. 也有同学简单的说有相同的特征值, 这也是不严谨不准确的.

7.$(n, i) = 1$

习题2.1

1.略

2.验算结合律, 单位元（左右）, 逆元（左右）, 这里只需单位元是左右单位元即可, 从而逆元也是左右的.

3.同上.

4.对任意$g \in G$, g_r表示g的右逆元, 于是

$$g_r(g_r)_r = e_r = gg_r$$

$$g_rg = g_r(ge_r) = g_r(gg_r(g_r)_r) = g_r(gg_r)(g_r)_r = e_r$$

$$e_rg = gg_rg = g$$

综上, e_r是G的单位元.

6, 7略

8.易知$a^{-1} = a$, $a(ba)b = (ab)^2 = e = a^2b^2 = a(ab)b$, 故$ab = ba$.

习题2.2

3.利用拉格朗日定理(书本P34 定理4.4). 设群$|G|=p$, $a\neq e$. 记$H=\langle a\rangle$, 由拉格朗日定理知$|H|$ 整除$|G|$, 同时因为p 是素数, 所以$|H|=p$, 从而$G=H$ 是循环群.

4.证明是子群略, $C_G(A)$不一定包含A, 除非 A 是 Abel 群.

5.显然$H(K\cap L)$含于L, 另一方面任意$l\in L$, $l=hk$, $h\in H$, $k\in K$, 只需说明k也属于L就行了, 事实上, $k=h^{-1}l$属于L.

6.首先证明 $\bigcap\limits_{g\in G} g^{-1}Hg$是群, 对任意$g\in G$, 可以验证$g^{-1}Hg$ 是子群, 而任意子群的交还是子群. 接着说明其正规性：

$$(g')^{-1}(\bigcap_{g\in G} g^{-1}Hg)g'=\bigcap_{g\in G}(gg')^{-1}Hgg'=\bigcap_{g\in G} g^{-1}Hg$$

注意:后面等号成立是由于群有消去律, 当g取遍G的元素时, gg'也取遍G的元素.

7.先证明是群再说明其正规, 略.

8. 根据矩阵乘法的定义和行列式性质: $|AB|=|A||B|$ 可证$SL_n(\mathbb{Z})$ 是$GL_n(\mathbb{R})$ 的子群, 但不是正规子群.

习题2.3

1.(12)(45)

2.$(i_1\dots i_t)=(i_1i_t)\dots(i_1i_3)(i_1i_2)$

3.略

4. 设$\sigma=\sigma_1\sigma_2\cdots\sigma_s$, $\sigma_1,\cdots,\sigma_s$ 是互不相交的轮换, 设t_i 是σ_i 的阶, t 是σ 的阶, t' 是$t_1,\cdots,t_s$的最小公倍数. 因为$\sigma_1,\cdots,\sigma_s$ 是互不相交的轮换, 所以其乘积可交换, 因此有

$$\sigma^{t'}=(\sigma_1\sigma_2\cdots\sigma_s)^{t'}=\sigma_1^{t'}\sigma_2^{t'}\cdots\sigma_s^{t'}=1,$$

$$1=\sigma^t=(\sigma_1\sigma_2\cdots\sigma_s)^t=\sigma_1^t\sigma_2^t\cdots\sigma_s^t,$$

所以t_i 整除t, 同时t整除t', 因此$t=t'$.

5.方法一：已知$\{(12),(13),\dots(1n)\}$是生成元集, 由$(1i)=(1i-1)(i-1i)(1i-1)$结合归纳法, 或直接由$(1i)=(12)$,$(i-1i)(i-2i-1)(i-3i-2)$,(12)可得.

方法二：已知$\{(12),(12\dots n)\}$是生成元集, 而(123,n) $=(12)(23)$,$(n-1n)$.

6.$n=4k$ or $4k+1$偶置换, $n=4k+2$ or $n=4k+3$奇置换

习题2.4

1. 没有, 6不能整除20.

2.充分性：gH=Hg, 所以关于H的左陪集也是右陪集. 必要性：由条件知, 对任意的a, 存在b, 使得aH=Hb, 由于1∈H, 推出a∈Hb 从而Ha=Hb=aH.

5.证$x^{-1}Kx\in K$对每个对换成立即可, 例如（1 2）.剩下可验证S_3是左陪集的一组代表元.

6.证明：任意$h,h'\in H$, $hK=h'K$等价于$h'^{-1}h\in K$, 即$h'^{-1}h\in H\cap K$ 这等价于$h(H\cap K)=h'(H\cap K)$. 故

$$\frac{|HK|}{|K|}=\frac{|H|}{|H\cap K|}$$

习题2.5

1. 由$f(g^n)=f(g)^n$知, g的阶是$f(g)$阶的倍数.

2. 由K=Ker f知, f(KM)=f(K)f(M)=f(M)（有同学可能会在这里就直接得结论）, 即$KM\subset f^{-1}(f(M))$. 另一方面任意$a\in f^{-1}(f(M))$, 故存在$m\in M$ 使得f(a)=f(m). 又由f是群同态知$f(am^{-1})$=e, 所以$am^{-1}\in K$, 所以$a=(am^{-1})m\in KM$.

3. 用定义证明即可.

4.先说明f是同态再用同态基本定理.

5.设G/C(G)由gC(G)生成, 则任意$a,b\in G$, 存在$c,d\in C(G)$使得$a=g^mc$, $b=g^nd$, 由此可得ab=ba.

习题2.6

1.记a是群的生成元, Aut（G）=$\{f_1,f_2,f_3,f_4\}$, 对应把a映射到a^i（i=1, 5, 7, 11）. 事实上Aut（G）和K_4的任意把1映到1的一一对应都同构.

2.K_4中非单位元素的阶均是2, 而Z_4中有阶为4的非单位元素, 故不同构.

3.略

4. (1) 设g^s的阶为t', 则$g^{st'}=1$, 所以$t|st'$, 又因为$(t,s)=1$, 所以$t|t'$. 另一方面, $(g^s)^t=(g^t)^s=1$, 所以$t'|t$. 因此$t=t'$.

(2) 考虑g^k, 利用(1)结论即可.

5.（1）这里只能证明g_1g_2的阶整除t_1,t_2 的最小公倍数, 不能证明g_1g_2的阶恰好是t_1,t_2的最小公倍数(反例:设g的阶为素数p, 取$g_1=g,g_2=g^{p-1}$, 则g_1,g_2的阶均为p, 而g_1g_2 的阶为1).

（2）存在整数a,b, 使得$at_1+bt_2=1$, 令$g_1=g^{bt_2}$,$g_2=g^{at_1}$即为所求.

6.显然$<a^{[m,n]}>\subseteq<a^m>$且$<a^{[m,n]}>\subseteq<a^n>$, 即$<a^{[m,n]}>\subseteq<a^m>\cap<a^m>$. 另一方面, 任意$<a^m>\cap<a^n>$中的元素$a^k$, $n|k$且$m|k$, 故$[m,n]|k$, 即$a^k\in<a^{[m,n]}>$.

习题2.7

1. 设Inn$G$ 是是G 的内自同构群, 从而是循环群.

$$\varphi:a\mapsto\varphi(a),\quad \varphi(a):x\mapsto axa^{-1}$$

是G到G 内自同构群的满同态. 可以验证Kerφ恰好是G 的中心C, 由同态定理知

$$G/C \cong \mathrm{Inn}G$$

由书本p47第5题结论可得结果.

习题2.8

1.只证明必要性：Abel群的子群都是正规子群. 设G的阶为$p^r m$, p为素数, 则由Sylow定理知G一定有p阶子群, 所以由G是单群知, G是p阶群.

2.看书中提示, 略.

3.设$a \in M, b \in N$, 由于M, N是正规子群, 所以$ba^{-1}b^{-1} \in M, aba^{-1} \in N$ 有$aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in M \cap N = \{e\}$.

4.由Sylow定理直接可得.

5.$x^{-1}Hx = y^{-1}Hy$等价于$(xy^{-1})^{-1}Hxy^{-1} = H$等价于$xy^{-1} \in N_G(H)$ 等价于$N_G(H)x = N_G(H)y$.

9.看书中提示, 略.

10.由推论8.3和题设知G 的中心的阶只能是p或p^2, 如果是p^2, 则可由由书本p47第5题结论推出矛盾.

习题2.9

1. 注意：有同学直接证明$f(H) + f(K)$是直和, 这是不对的.

可以用(h,k)表示$H \oplus K$的元素, 用矩阵形式表示同构f, 因为$f(K) = K'$, 所以

$$f = \begin{bmatrix} f_{11} & 0 \\ f_{21} & f_{22} \end{bmatrix}$$

其中$f_{11} : H \mapsto H'$, $f_{21} : H \mapsto K'$, $f_{22} : K \mapsto K'$, $f(h,k) = (f_{11}(h), f_{21}(h) + f_{22}(k))$.

下面只需证明f_{11} 是群同构, f_{11}也可以通过f与$H' \oplus K'$到H'的投影的复合得到, 因此, f_{11} 是群同态(也可以用定义验证).

f_{11}是满射,是说明略. 证明f_{11} 是单射, 设$h \in H$ 使得$f_{11}(h) = 0$, 因为$f_{22}(K) = f(K) = K'$, 所以存在$k \in K$, 使得$f_{22}(k) = -f_{21}(h)$. 因此可验证$(h,k) \in \mathrm{Ker}f$, 所以$h = 0$.

2. $392 = 2^3 \times 7^2$, 有$3 \times 2 = 6$ 个392阶Abel群. $\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{7^2}$, $\mathbb{Z}_{2^3} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$, $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{7^2}$, $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{7^2}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$

4. 参考书本提示.

习题2.10

1.$G_1 = G_2 = \{(1),(34)\}$, $G_3 = G_4 = \{(1),(12)\}$.

2.验证书本定义10.2 的两个条件. 这里只有一条轨道, 也就是所有陪集, 而gH的稳定子群为gHg^{-1}, 其阶数与H的阶数相等, 所以轨道公式是$|G/H| = |G|/|H|$

5.设m_1, m_2为M中任意两个元素, 由M在G作用下可迁知, 存在$g \in G$使得$m_1 = gm_2$, 证明在N作用下每个轨道长度相等, 只需证明Nm_1和Nm_2一一对应即可, 这里对应是$hm_1 \to g^{-1}hgm_2$, 这是一一对应是由N是正规矩阵得(这里具体说明需要自己补充, 略).

6.略.

2.11 1. 此处$n = 4$, $r = 2$. 考虑D_4 的元素：

$$(1),\ (1234),\ (13)(24),\ (1432),\ (14)(23),\ (24),\ (12)(34),\ (13)$$

其中型为$(4, 0, 0, 0)$ 有1个, $(2, 1, 0, 0)$ 有2个, $(0, 2, 0, 0)$ 有3个, $(0, 0, 0, 1)$ 有2个. 所以项链数为：

$$t = \frac{1}{2 \times 4}(1 \times 2^4 + 2 \times 2^3 + 3 \times 2^2 + 2 \times 2^1) = 6$$

习题3.1

1.略

3.验证对加法和乘法封闭

4.按定义验算, 略.

7.满足$m < n$,$(m, n) = 1$的所有$\overline{m}$

8.由复数乘法知, 若该环的两个元素乘积为0, 则必有其中一元为0, 所以是整环. 由$(a+b\sqrt{-3})(c+d\sqrt{-3}) = 1$可得$ac-3bd = 1$, $ad+bc = 0$,可推出$a^2+3b^2 = 1$,故$a = 1, -1$, $b = 0$, 单位只有± 1.

10.只有Q本身

11.验证略, 其子域只有Q和它本身

12. $(a + a) = (a + a)^2 = 4a^2 = 4a = 2(a + a)$, 所以$a + a = 0$, 同时有$a = -a$. 其交换性：$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$, 因此有$ab + ba = 0$, 从而$ab = -ba = ba$.

14. $F^{\times} = F - \{0\}$ 是一个乘法群, 且有限, 所以F 中任意非零元素a均满足$a^{|F^{\times}|} = 1$, 从而$a^{|F|} = a$. 若$a = 0$, 则$a^{|F|} = a$显然成立.

15.(i)按定义验证略. (ii)不考虑零乘环的情况. 证明略. (iii)略. (iv) 把R 中每一个元素r看成re.

(v) 因为G 是有限群, 所以存在非零元素

$$a = \sum_{g \in G} rg, \quad r \neq 0$$

任取R 中非零元素r', 任取G 中元素h, 则

$$r'ha = r'\sum_{g\in G} rhg = r'\sum_{g\in G} rg = r'a$$

所以

$$(r'e - r'h)a = 0$$

注意这里$\sum_{g\in G} rhg = \sum_{g\in G} rg$成立是因为等号两边均是$G$ 中所有元素乘以相同的系数再求和, 所以相等.

习题3.2

1. 略.

2.(i)从定义出发, 略. (ii)当f不是0同态时, 因为同态保持乘法, 所以有f(a)f(1)=f(a), 因为是满同态, 所以f(a)取遍整个R', 因此f(1)是R'的单位元, 第二个式子略. （iii）略（iv）略

3.验证略, -1和0分别是新环的零元和单位元, 同构为把a映射到a-1.

4.只能证明其是主理想环而不一定是整环. 反例见同一题第二问, Zm是Z的一个同态像, 取m为非素数, 则, Zm有零因子. （这是一道有问题的题目）

5. 略

6. 略

7. 是同构. 注意构造同构时需要把乘法单位元对应, $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$ 的单位元为$\overline{1}$, $2\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{2}, \overline{4}\}$ 的单位元为$\overline{4}$.

8. 按定义验证略

10. (1)ϕ 是单射. 假设$J_1/I = J_2/I$, $\forall a \in J_1$, 则$a + I \in J_2/I$, 从而存在$b \in J_2$ 使得$a + I = b + I$, 这推出$a - b \in I \subset J_2$, 从而$a = a - b + b \in J_2$, 即$J_1 \subseteq J_2$, 反之$J_2 \subseteq J_1$成立.

(2)ϕ 是满射. R/I的任意一个理想均是子环, 从而必定是形如J/I, 其中J 是R 的子环, 下面只需验证J 是理想即可, 略.

11.（1）略（2）不能, 例：取二阶矩阵环, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$和$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$均是幂零, 但是它们的和不是幂零. （3）验证N为理想. （这里要注意搞清楚商环的零元素）.

12. 设$a^m, b^n \in I$, $c \in R$ 因为R 是交换环, 所以$ac = ca$, 从而有

$$(ac)^m = a^m c^m \in I$$

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} C_{m+n}^i a^i b^{m+n-i} \in I$$

. (注意：上式中的$i\geq m$ 和$m+n-i\geq n$ 至少有一式成立. 即a^i, b^{m+n-i}中至少有一项属于I).

14. (1)同构把生成元映到生成元, 而$\mathbb{Z}$ 中只有生成元1, 所以只有恒等映射是同构.

(2) 设同构$\varphi:\mathbb{Z}_n\to\mathbb{Z}_n$, $\varphi(\overline{1})=\overline{i}$, 其中$1\leq i\leq n-1$, 且$(i,n)=1$.
由态射的性质知

$$\varphi(\overline{1})=\varphi(\overline{1}\cdot\overline{1})=\overline{i}\cdot\overline{i}$$

所以$\overline{i}=\overline{i^2}$, 从而有$n|i^2-i=i(i-1)$, 故只能是$i-1=0$. 所以φ 是恒等映射.

习题3.3

1.$\mathbb{Z}[x]/\langle x\rangle=\mathbb{Z}$ 是整环, 所以$\langle x\rangle$是素理想. 或直接从定义出发也可以.

2.必要性：当P是R的素理想时, 如果$ab\in P$, 则$\langle a\rangle\langle b\rangle=\langle ab\rangle\subset P$ （前面等号用到了R是交换的前提条件）, 所以$\langle a\rangle$或$\langle b\rangle\subset P$, 从而$a$或$b\in P$.

充分性：用反证法. 假设P不是素理想, 即存在理想I和J, 使得$IJ\subset P$ 但$I,J\nsubseteq P$, 则存在$a\in I$, $a\notin P$和$b\in J$, $b\notin P$. 但$ab\in IJ\subseteq P$, 与假设条件矛盾.

3.P是素理想, 等价于R/P是整环, 而R有限, 故R/P是有限整环, 即为域, 所以由命题3.1知P是极大理想.

5.（i）第一步先说明$f(P)$是真理想（略）, 第二步说明它是素理想：设I, J是S的理想使得$IJ\subseteq f(P)$, 则$f^{-1}(I)f^{-1}(J)\subseteq f^{-1}(f(P))$, 接着说明$f^{-1}(I)$和$f^{-1}(J)$是$R$的理想, 且$f^{-1}(f(P))=P$(这里用到条件$P\supseteq K$,略), 结合$P$是素的, 可得$f(P)$是素的. （注意：此题不能用命题3.1, 因为$R$和$S$并非交换的. 同理第2题结论也要慎用）

（ii）先说明$f^{-1}(Q)$是真理想（略）, 任意R中理想I,J, 使得$IJ\subseteq f^{-1}(Q)$, 则$f(I)f(J)\subseteq Q$, 由Q是素理想知$f(I)$或$f(J)\subseteq Q$, 所以I或$J\subseteq f^{-1}(Q)$.（注：这里的$f^{-1}(Q)\supseteq K$）

(iii)结合（i）和（ii）可得结论.

7.由第3题知Z_m的素理想也是极大理想. 而$\mathbb{Z}_m$的每个素理想对应与m的一个素因子n, 故其所有素理想为$n\mathbb{Z}/m\mathbb{Z}$.

12. $\mathbb{Q}[\sqrt{-1}]$

14. 因为K 和F 有相同的单位元, 其作为加法群中元素的阶相同, 若阶有限, 则为同一个素数p, 此时, char$F$=char$K$=p, 否则,char$F$=char$K$=0.

习题3.4

1. $x\equiv 23(\mod 30)$

2.(1)设$r\in$Ker$f$, 即$(r+I,r+J)=0$, 这等价于$r\in I\cap J$.

(2) f 是满同态当且仅当对任意$r_1, r_2 \in R$, 存在$r \in R$ 使得$f(r) = (r+I, r+J) = (r_1+I, r_2+J)$.

假设f为满同态, 对任意的$r \in R$, 考虑$(r+I, J)$ 在f的原象, 不妨设$r' \in R$ 使得$f(r') = (r+I, J)$, 则$r' \in J$ 且$r - r' \in I$, 所以$r = r - r' + r' \in I + J$.

假设$I + J = R$, 设任意的$x, y \in R$, 则可固定分解$x = x_1 + x_2$, $y = y_1 + y_2$, 其中$x_1, y_1 \in I$, $x_2, y_2 \in J$. 则取$r = x_2 + y_1$, 可得$f(r) = (x_2 + I, y_1 + J) = (x + I, y + J)$.

习题3.5

1.$x^3 + 3x^2 + 5x + 5$

2.设$x = a + bi + cj + dk$, $\forall a, b, c, d \in$R.

$$-2 = x^2 = a^2 - b^2 - c^2 - d^2 + 2abi + 2acj + 2adk$$

解得$a = 0$, $b^2 + c^2 + d^2 = 2$, 因此满足此条件的x均是方程的解.

3.先考虑在$\mathbb{Z}[x]$上的分解: $x^9 - x = x(x-1)(x+1)(x^2+1)(x^4+1)$, 接着只需考虑$x^2+1$和$x^4+1$在$\mathbb{Z}_3[x]$的分解即可. 可以列举$\mathbb{Z}_3[x]$中一次和二次的不可约多项式:

$$x, x+1, x+2, x^2+1, x^2+x+2, x^2+2x+2, 2x^2+x+1, 2x^2+2x+1$$

可以验证$x^4 + 1 = (x^2+x+2)(x^2+2x+2) = (2x^2+x+1)(2x^2+2x+1)$

4.统一记多项式为f. (1)当$p = 2$ 时, $f = (x+1)^2$ 可约. 当$P \neq 2$ 时, 即p 为奇素数, 令$x = y - 1$, 则$f(y-1) = (y-1)^p + p(y-1) + 1 = y^p + pyg(y) - p$, 其中$g(y)$是关于$y$的一个多项式. 则由艾森斯坦判别法知$f(y-1)$不可约.

(2)当$p = 2$ 时, $f = x^2 - 2x - 1$没有有理根, 所以在$\mathbb{Q}$上不可分解, 即不可约. 当p 为奇素数时, 设$x = y - 1$, $f(y-1) = (y-1)^p - p(y-1) - p + 1$, 恰好常数项和一次项系数均为0, 故有因式$y^2$.

5.(1)把2代入为0, 故有因式$x - 2$或$x + 1$. (2)将, 0, 1, 2代入均不为零, 故原式可能不可约或为两个二次不可约多项式的乘积. 结合第3题, 可以验证（2）中多项式不可约.

7.定义映射$\varphi : \mathbb{Z}[\sqrt{-2}\,] \to \mathbb{N}_0$为$\varphi(a + b\sqrt{-2}) = a^2 + 2b^2$. 则$\varphi(\alpha) = 0$当且仅当$\alpha = 0$; $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$, $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$. 设$\alpha, 0 \neq \beta \in \mathbb{Z}[\sqrt{-2}]$. 令$\alpha\beta^{-1} = x + y\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}\,]$. 取$a, b \in \mathbb{Z}$使得$c = x - a$, $d = y - b$满足$|c| \le \frac{1}{2}$, $|d| \le \frac{1}{2}$. 于是有

$$\alpha = (a + b\sqrt{-2})\beta + r,$$

其中$r = (c + d\sqrt{-2})\beta \in \mathbb{Z}[\sqrt{-2}\,]$, 并且

$$\varphi(r) = \varphi(c + d\sqrt{-2})\varphi(\beta) = (c^2 + 2d^2)\varphi(\beta) \le \frac{3}{4}\varphi(\beta).$$

由定义知$\mathbb{Z}[\sqrt{-2}]$是ED.

8.设d是D中非零的不可逆元, 则$\langle d,x\rangle$不是主理想. 否则, 设$\langle d,x\rangle=\langle f(x)\rangle$. 则由$d\in\langle d,x\rangle$知$f(x)$只能是零次多项式, 记为$c$. 于是

$$\langle d,x\rangle=\langle c\rangle\,,\ c\in D$$

再由$x\in\langle c\rangle$可知c是D中的可逆元, 从而$d\in\langle d,x\rangle=D[x]$. 于是存在$g(x),h(x)\in D[x]$使得

$$1=dg(x)+xh(x)$$

因此$1=dg_0$, g_0是$g(x)$的常数项. 这与d的选取矛盾.

9. 若a 为可逆元, 则包含a的主理想只有R. 若$a\neq 0$ 不是可逆元, 则在相差一个可逆元的情况下存在唯一分解$a=p_1^{r_1}\cdots p_n^{r_n}$. $a\in<b>$ 当且仅当$b|a$, 因此这样的b是有限的.

习题4.1

2.因u是K中任一不属于F的元, 故$[F(u):F]>1$. 由望远镜公式$[K:F]=[K:F(u)][F(u):F]$, 由于$[K:F]$为素数, 所以$[K:F]=[F(u):F]$, 从而$K=F(u)$.

3.只需证明$u\in F(u^2)$. 设$f(x)$是u的极小多项式, 因为f的最高次为奇数, 所以$f(x)=xg(x^2)+h(x^2)$, 其中$g(t)$为非0多项式. 由于f是u的极小多项式, 所以$g(u^2)\neq 0$, $h(u^2)\neq 0$, $ug(u^2)+h(u^2)=0$. 故, $u=-h(u^2)/g(u^2)\in F(u^2)$.

4.若超越扩张F/K是有限扩张, 取F中一个K的超越元u, 则由望远镜公式得$[F:K]=[F:K(u)][K(u):K]$, 而$K(u)\simeq K(x)$是K得无限扩张, 矛盾.

5.(i)由E定义, 我们只需证明E是包含F的域即可. 显然$F\subset E$. 接着证明E是域, 设$a,0\neq b\in E$, 则$a-b,ab^{-1}\in F(a,b)$. 而$F(a,b)$是F的有限扩域从而是代数扩域, 所以$a-b,ab^{-1}$在F上代数, 即$a-b,ab^{-1}\in E$, 故E是域.

(ii)用反证法. 如果a在E上代数, 则$E(a)/E$为有限代数扩张, 又E/F是代数扩张, 所以$E(a)/F$为代数扩张, 所以$a\in E$, 矛盾.

6.(1)$x^2-2\sqrt{2}x-1$ (2)x^4-10x^2+1
这一题中, 我们可以发现$\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$但不属于$\mathbb{Q}$和$\mathbb{Q}(\sqrt{2})$, 而$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$, 由此可见$\sqrt{2}+\sqrt{3}$在$\mathbb{Q}(\sqrt{2})$上的极小多项式的次数为2, 而在$\mathbb{Q}$上的极小多项式的次数为4.

7.(1)根据艾森斯坦判别法(取p=3), 题中多项式在$\mathbb{Q}$上不可约.

(2) $u^3+1=6u^2-9u-2$;

用待定系数法, 设$(u-1)^{-1}=au^2+bu+c$, 则$(au^2+bu+c)(u-1)=1$, 计算略, 得$(u-1)^{-1}=\frac{-u^2+5u-4u}{7}$.

类似地, 用待定系数法算出$(u^2-2u+4)^{-1}=\frac{-3u^2-u+61}{283}$.

8.$x^{\frac{n}{m}}-a$. 若有另外的一个多项式$g(x)$次数小于$\frac{n}{m}$ 零化u^m, 则$g(x^m)$ 次数小于n, 且次数小于n, 这与假设矛盾.

9.(i)p次方程最多只有p个根, 可以验算每个$u+i$是$f(x)$的解：$f(u+i)=(u+i)^p-(u+i)-c=u^p+i^p-u-i-c=u^p-u-c=0$

(ii)用反证法, 若x^p-x-c可约, 则$x-u, x-(u+1), \ldots, x-(u+p-1)$中有t个一次多项式的积在$F[x]$中, 其中$1\le t<p$, 即$(x-(u+i_1))\cdots(x-(u+i_t))\in F[x]$, 但其$x^{t-1}$的系数为$-(tu+i_1+\cdots+i_t)$, 从而$tu\in F$. 但$t\neq 0$, 故$u\in F$, 矛盾.

(iii)设$\frac{1}{u+1}=a_0+a_1u+\cdots+a_{p-1}u^{p-1}$, 结合$u^p-u-c=0$化简$(a_0+a_1u+\cdots+a_{p-1}u^{p-1})(u+1)=1$.

当$p=2$, 上式化简得: $a_0+a_1c+(a_0+2a_1)u=a_0+a_1c+a_0u=1$, 因此可得$c=a_1=1$, $a_0=0$.

当$p>2$, p为奇素数, 上式化简得: $(a_0+a_{p-1}c)+(a_0+a_1+a_{p-1})u+(a_1+a_2)u^2+\cdots+(a_{p-2}+a_{p-1})u^{p-1}=1$. $a_{p-1}=-a_{p-2}=\cdots=(-1)^{p-2}a_1=-a_1$, 而$a_0+a_1+a_{p-1}=0$, 所以得$a_0=0$, $a_{p-1}=c^{-1}$.

4.2

1. 设$f(x)=(x-x_1)(x-x_2)\cdots(x-x_n)$, $x_i\in E$, 由望远镜公式知

$$[E:F]=[F(x_1,x_2,\cdots,x_n):F(x_1,x_2,\cdots,x_{n-1})]\cdots[F(x_1,x_2):F(x_1)][F(x_1):F]$$

其中

$$[F(x_1,x_2,\cdots,x_{k+1}):F(x_1,x_2,\cdots,x_k]\le\deg\frac{f(x)}{(x-x_1)\cdots(x-x_k)}=n-k$$

所以$[E:F]\le n!$.

3.由上一节第9题知$f(x)$在E上的所有根为

$$u,u+1,\cdots,u+p-1$$

所以$E=F(u)$, $[E:F]=p$. 因此Galois群Gal(E/F)是一个p阶循环群$<\sigma>$, 其中$\sigma(u)=u+1$.