欧式作图

2024 年 1 月 25 日

目录

在这章，让我们舍弃一些线性代数的基础内容，快进到这里。

我们在这章解决一些几何问题：能把每个角都三等分吗？可以构造一个正n边形吗？能“化圆为方”吗？也就是说，可以构造一个面积等于给定圆面积的正方形吗？

注意： 令P和Q是平面上的点，我们用PQ表示具有端点P和Q的线段。我们把长度记为$\mid PQ \mid 0$

令$L[P,Q]$为由P和Q确定的直线，再令$C[P;PQ]$表示为以P为原点和以$\mid PQ \mid$为半径的园。

我们来讨论一开始谈到的问题，注意P,Q是平面上不同的点，则$L[P,Q]$是由这两点确定的直线，并且$C[P;PQ]$是由点P和PQ确定的圆。

为了描述尺规作图的严肃，我们做如下的解释，用代数来描述尺规作图。

0.1 定义：

令$E \neq F$和$G \neq H$为平面上的点，说点Z为从E,F,G和H出发可构作的，如果它满足如下条件：

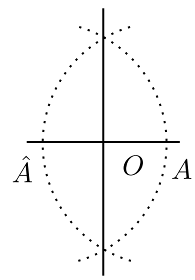
1. $Z \in L[E,F] \cap L[G,H]$，其中$L[E,F] \neq L[G,H]$
2. $Z \in L[E,F] \cap C[G;GH]$或者$Z \in L[G,H] \cap C[E;EF]$
3. $Z \in C[E;EF] \cap C[G;GH]$，其中$C[E;EF] \neq C[G;GH]$

点Z称为可构作的，若$Z = A$或者$Z = \hat{A}$或存在点$P_1, \cdots, P_n$由$Z = P_n$且对所有$j \geq 1$，点P_{j+1}是从$\{A, \hat{A}, P_1, \cdots, P_n\}$中可构作的。

0.1.1 例子

我们来证明$Z = (0,1)$是可构造的。定义点$P_2 = (0, \sqrt{3})$和点$P_3 = (0, -\sqrt{3})$，这两点可以从$C[A; A\hat{A}] \cap C[\hat{A}, \hat{A}A]$构造来，其中$A = (0,1)$而$\hat{A} = (-1,0)$。因此$y$轴上的直线$L[P_2,P_3]$可以被画出来，我们就得到

$$Z = (0,1) \in L[P_2,P_3] \cap C[O,OA]$$



0.2 定义：可构造的复数

一个复数$z = x + iy$是可构造的，若其点(x, y)是可构造点。

刚才的例子给了一些信息，即$1, -1, 0, i\sqrt{3}, -i\sqrt{3}i$和$-i$都是可构造数。

0.3 引理

一个复数$z = x + iy$是可构造的当且仅当实部x和其虚部y是可构造的

证明： 若z是可构造的，则标准欧几里得构造可以画出穿过点(x, y)的垂线L，其中L平行于y轴。这告诉了我们x是可构造的，为此$(x, 0)$也是可构造的，它是L和x轴的交点。类似的讨论可以得到$(0, y)$是L'平行于x轴但与y轴相交的直线，L'穿过点(x, y)。我们得到$P = (0, y)$是可构造的，因为$C[O : OP]$正是它和x轴的交点。所以y是可构造的。

反之，我们设x, y是可构造数，因此$Q = (x, 0)$和$P = (y, 0)$是可构造的点。而点$(0, y)$是可构造的，因为y轴和$C[O, OP]$的交点正是它。最后，(x, y)作为他们的交点，我们只需要画出过$(x, 0)$的垂线和过$(0, y)$的水平线即可得到，所以(x, y)是可构造的点。从而$z = x + iy$是一个可构作的数。

0.4 定义：构作数

我们用K表示C中所有可够作数组成的集合。

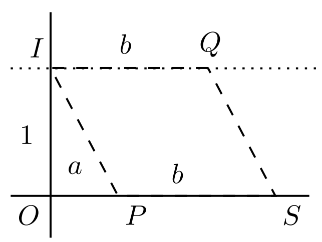
0.5 定理

可构造实数$K\cap R$集是R的子域，且对正元素的平方根封闭。

证明： 令a,b是可构造实数。

1. $-a$是可构造的，若$P=(a,0)$，则$(-a,0)$是x轴与$C[O,OP]$在另一边的交点。

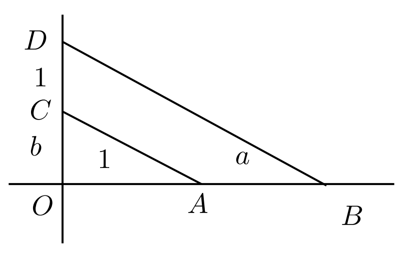
2. $a+b$也是可构造的



像上图一样，我们定义a,b是正的，令$I=(0,1)$，$P=(a,0)$和$Q=(b,1)$。则Q是可构造的，因为我们可以通过I构造水平线与过点$(b,0)$的垂线作交点。通过点Q且平行IP的直线与x轴相交在点S，得。证

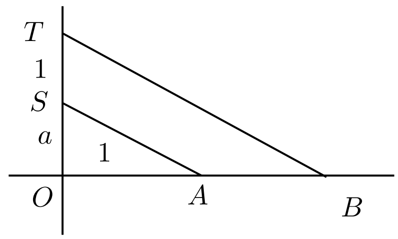
3. ab也是可构作的我们假设a,b是正的。$A=(1,0),B=(1+a,0)$和$C=(0,b)$。定义D是过点B且平行于AC的直线和y轴的交点。由于三角形OAC和三角形OBD相似，则

$$\mid OB\mid/\mid OA\mid=\mid OD\mid/\mid OC\mid$$



由于$(a+1)/1=(b+\mid CD\mid)/b$，且$\mid CD\mid=ab$。因此$b+ab$是可构造的的。因此$-b$是可构造的利用第二部分即可得到$ab=b((1+a)-1)$是可构造的。

4. 若$a \neq 0$，则a^{-1}是可构造的。令$A = (1, 0)$，$S = (0, a)$和$T = (0, 1+a)$。定义B是过点T且平行于AS的直线和x轴相交的点。

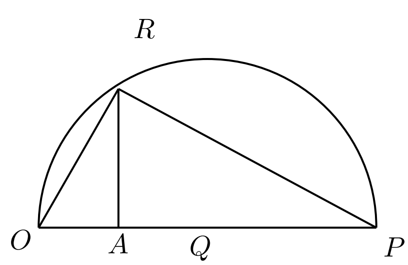


因此，$B = (1 + u, 0)$对某个u成立。而三角形OSA和三角形OTB相似给出了

$$| OT | / | OS |=| OB | / | OA |$$

所以，$(1 + a)/a = (1 + u)/1$有$u = a^{-1}$，因此$1 + a^{-1}$是可构造的并且$(1 + a^{-1}) - 1 = a^{-1}$ 是可构造的。

5. 若$a \geq 0$，则$\sqrt{a}$也是可构造的。令$A = (1, 0)$和$P = (1 + a, 0)$。现在我们构造点Q在OP中间，定义R是圆$C[Q : QO]$和过点A的垂线的交点。



而三角形AOR和三角形ARP相似，因此

$$| OA | / | AR |=| AR | / | AP |$$

稍微的简化就得到了$| AR |= \sqrt{a}$

0.6 推论

可构作集K在平方根下构成C的子域。

证明： 若$z=a+ib$和$\omega=c+id$是可构造的，则a,b,c,d都是可构造实数，有$a,b,c,d\in K\cap R$。因此$a+c,b+d\in K\cap R$。由于$K\cap R$是R的子域。那么$(a+c)+i(b+d)\in K$。类似的，$z\omega=(ac-bd)+i(ad+bc)\in K$，若$z\neq 0$，则$z^{-1}=(a/z\bar{z})-i(b/z\bar{z})$。现在$a,b\in K\cap R$，利用引理4.3得到$z\bar{z}=a^2+b^2\in K\cap R$。由于$K\cap R$是一个$C$中的域，那么就有$z^{-1}=a-ib\in K$得到$K$是$C$的子域。

最后，若$z=a+ib\in K$，那么由引理0.3可知$a,b\in K\cap R$和$r^2=a^2+b^2\in K\cap R$。因为r^2是非负的，我们由$\sqrt{r}\in K\cap R$。现在$z=re^{i\theta}$。那么$e^{i\theta}=r^{-1}z\in K$。由于K是C的域。则每个角可以二等分得到$e^{i\theta/2}\in K$，所以$\sqrt{z}=\sqrt{r}e^{i\theta/2}$

0.7 推论

若a,b,c是可构造的，则ax^2+bx+c的根也是可构造的。

证明： 利用二次公式

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

由于a,b,c是可构造的，现在我们由推论0.6就可以得到$-b$是可构造的。且对平方根封闭，因此二次多项式是可构作的。

0.8 定义：2-塔

一个2-塔指的是C的一个上升的子域塔

$$Q(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$$

其中$[F_j:F_{j-1}]\leq 2$对所有$j\geq 1$成立。而一个复数z称为多重二次的，若存在一个$2-$塔使得$z\in F_n$，并把所有多重二次的复数的集合记为P

0.9 引理

若F/k是一个域的扩张。则$[F:k]\leq 2$当且仅当$F=k(u)$，其中$u\in F$是某个二次多项式$f(x)\in k[x]$的根

证明： 若$[F:k]=2$，则$F\neq k$和这里有一些元素$u\in F$使得$u\notin k$。那么就存在一些多项式$f(x)\in k[x]$使得u是其的一个根。[1]。我们由$2=[F:k]=[F:k(u)][k(u):k]$。现在，由于$k(u)\neq k$，因此$[k(u):k]\neq 2$有$[F:k(u)]=1$，因此$F=k(u)$。所以我们有$\deg(f)=2$并且u是该二次多项式的根。

反之，令$F=k(u)$，其中u是二次多多项式$f(x)\in k[x]$的根。我们设$f(x)$是可分解的，那么$u\in k$有$F=k$与$[F:k]=2$矛盾。其次，由于k在$k(u)$上的基为1，那么$[F:k]=[k(u):k]=2$。

0.10 引理

1. P是C在平方根运算下封闭的子域。
2. 复数$z=a+ib$，其中$a,b\in R$是多重二次的当且仅当a,b是多重二次的。

证明： 若$z,z'\in P$，则这里有一个2-塔$Q(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$和$Q(i)=F_0'\subseteq F_1'\subseteq\cdots\subseteq F_m'$使得$z\in F_n$和$z'\in F_m'$。由于$[F_j:F_{j-1}]\leq 2$意味着有$F_j=F_{j-1}(u_j)$，其中$u_j\in F-j$是$f_j(x)\in F_{j-1}[x]$中的根。对全部$j,1\leq j\leq n$定义$F_j''=F_m'(u_1,\cdots,u_j)$。由于$F_j''=F_{j-1}''(u_j)$，那么$F_{j-1}=F_0'(u_1,\cdots,u_{j-1})\subseteq F_m'(u_1,\cdots,u_j)=F_{j-1}''$[2]，那么$f_j(x)\in F_{j-1}''[x]$得到$[F_j'':F_{j-1}'']\leq 2$。那么我们就有

$$Q(i)=F_0'\subseteq F_1'\subseteq F_m'\subseteq F_1''\subseteq\cdots\subseteq F_n''$$

是一个2-塔。这意味着每个F_n''的元素都是多重二次的。由于F_n''包含z,z'。那么他也包含他们的和还有逆和乘积。因此P是域。

其次，令$z\in P$。若$Q(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n$是2-塔使得$z\in F_n$，则$Q(i)=F_0\subseteq F_1\subseteq\cdots\subseteq F_n\subseteq F_n(\sqrt{z})$依然是一个域

[1] 若K的是k的一个域扩张，则这里存在一些元$u\in K$使得在k中是线性相关集的，则我们总能找到一个$u\in K$但$u\neq k$使得对不全为零的量$a_i,i=1,2,\cdots,t$有$a_1u+\cdots+a_tu^t$是线性相关的。

[2] $F_{j-1}=F_0'(u_1,\cdots,u_j)$可以由一开始的定义$Q(i)=F_0=F_0'$得到

证明2： 若$a, b \in P$，则$a + bi \in P$，因为P是包含i得到的域。反之，我们令$Q(i) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$是2-塔使得$z \in F_n$。由于复共轭是$C$上的一种自同构，我们可以找到一个$\bar{z}$使得$Q(i) = \bar{F}_0 \subseteq \cdots \subseteq \bar{F}_n$里面有$\bar{z} \in \bar{F}_n$的元素存在。所以$\bar{z}$也是多重二次的，就有$a = \frac{1}{2}(z + \bar{z}) \in P$，并且类似的方法我们可以得到$b = \frac{1}{2i}(z - \bar{z}) \in P$。

0.11 引理

令$P = a + ib$，$Q = c + id \in P$，那么

1. 直线$L[P, Q]$是垂直的(c=a)，那么其方程为$x = a$或者是非垂直($c \neq a$)的有$y = mx + q$，其中m, q是多重二次的。
2. 圆$C[P, PQ]$的方程为$(x-a)^2 + (y-b)^2 = r^2$，其中a, b, r是多重二次的。

证明1： 利用引理0.10可知a, b, c, d都是多重二次的。若$L[P, Q]$是非垂直的，则方程$y = mx + q$，其中$m = \frac{(d-b)}{(c-a)}$并且$q = -ma + b$，因此$m, q \in P$

证明2： 我们知道圆的方程是$(x-a)^2 + (y-b)^2 = r^2$，那么对于圆$C[P : PQ]$。其中r是P到Q的距离。利用引理0.10，P对平方根封闭，那么就有$r = \sqrt{(c-a)^2 + (d-b)^2} \in P$

0.12 引理

每个多重二次z是可构造的

证明： 若$z \in P$，则存在一个2-塔$Q(i) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$使得$z \in F_n$我们对$n \geq 0$归纳来证明$z \in K$是可构作的。基础步骤是$F_0 = Q(i) \subseteq K$，这是成立的，因为$Q(i)$是有理数和$i$构成的最小域。利用推论0.6，由于$Q$中的数可构造，那么$Q(i) \subseteq K$。现在我们继续下一步。我们由$F_n = F_{n-1}(u)$，其中$u$是某个二次多项式$f(x) = x^2 + ax + b \in F_{n-1}[x]$的根。利用二次公式，我们知道$u \in F_{n-1}(\sqrt{b^2 - 4c})$，利用推论0.6我们知道$K$对平方根在$C$中封闭。所以$\sqrt{b^2 - 4c} \in K$，由归纳法有$F_{n-1} \subseteq K$。由于$F_{n-1}(\sqrt{b^2 - 4c})$是封闭的域，那么利用求根公式，$u$就在$F_{n-1}(\sqrt{b^2 - 4c})$中。综上所述，我们

就可以给出

$$z \in F_{n-1}(\sqrt{b^2-4c}) \subseteq K(\sqrt{b^2-4c}) \subseteq K$$

0.13 一个复数$z \in C$是可构造的当且仅当 z是多重二次的

证明： 引理0.12告诉了我们$P \subseteq K$，并且证明了每个可构造的z都是多重二次的。则这里存在一些复数$1, \omega_0 = -1, \omega_1, \cdots, \omega_m = z$使得对所有$j \geq 0$，$\omega_j$可以从$\omega_0, \cdots, \omega_{j-1}$构造。我们通过对$m \geq 0$归纳证明$\omega_m$是多重二次的。因为$-1 \in Q(i) = F_0$，所以它是多重二次的。接下来，为了证明$\omega_m$是多重二次的，我们只需证明$z$是由$P, Q, R, S$构成的，其中这四个域的元素也是多重二次的。

1 $z \in L[P,Q] \cap L[R,S]$

注意$P, Q, R, S \in P$，现在开始我们的证明，若$L[P,Q]$是垂直的，则它的方程就是$x = a$，若非垂直，由引理0.11可知它的方程为$y = mx + q$，其中m, q在P中。类似的讨论我们可以得到$L[R,S]$的方程是$x = c$或者$y = m'x + p$，其中$m', p \in P$。若不是平行的，那么我们就可以解线性方程

$$y = mx + q$$
$$y = m'x + p$$

得到其交点$z = x_0 + iy_0 \in L[P,Q] \cap L[R,S]$，那么就有$z = x_0 + iy_0 \in P$[3]

2 $z \in L[P,Q] \cap C[R;RS]$

设$R = (u,v)$和$S = (s,t)$是多重二次的，圆$C[R;RS]$的方程为$(x-u)^2 + (y-v)^2 = r^2$，其中$r^2 = (u-s)^2 + (v-t^2)$是一定的。对于其他的，利用引理0.11可知其所有系数都在P中。若$L[P,Q]$垂直，则$x = a$是其方程，对$z = x_0 + iy_0 \in L[P,Q] \cap C[R;RS]$。有$(x_0-u)^2 + (y_0-v)^2 = \rho^2$得到$y_0$是$P[x]$上一个次数为2的根，利用域的扩张，首先，多项式的每个系数都在P中，那么就有一个二次扩张域K包含所有系数，它是一个2-tower，现在有$[K(y_0) : K] \leq 2$。我们可以得到一个次数为2的用y_0当基的扩域。因此$y_0 \in P$有$z = a + iy_0 \in P$。

其次，若直线$L[P,Q]$不是垂直的。则方程为$y = mx + q$，其中$m, q \in P$。若$z = x_0 + iy_0 \in L[P,Q] \cap C[R;RS]$，则$(x-u)^2 + (mx_0 + q - v)^2 =$

[3]解$q = mx + y$和$p = mx'$得到结果。

r^2得到x_0是$P[x]$中的二次根，因此同样的方法可知$y_0 = mx_0 + q \in P$有$z = x_0 + iy_0 \in P$

3 $z \in C[P; PQ] \cap C[R; RS]$

设$R = (u, v)$和$S = (s, t)$，则圆$C[R; RS]$的方程为$(x-u)^2 + (y-v)^2 = r^2$，其中$r^2 = (u-s)^2 + (v-t)^2$。同样的，设$P = (a, b), Q = (c, d)$。可以得到和上面一样的结果。并且方程的所有系数都在P中。现在，设$z = x_0 + iy_0 \in C[P; PQ] \cap C[R; RS]$。则我们展开方程，得到

$$x_0^2 + y_0^2 + \alpha x_0 + \beta y_0 + \gamma = x_0^2 + y_0^2 + \alpha' x_0 + \beta_0' y_0 + \gamma'$$

我们消去$x_0^2 + y_0^2$得到新的方程$\lambda x + \mu y + v = 0$其中$\lambda, \mu, v \in P$。并且这个方程是某条线$L[P', Q']$的方程。其中$P', Q' \in P$[4]。那么该点$z$实际上就是直线和两个圆中任意一个的交点，利用第二个命题则可以证明$z \in P$

0.14 推论

若复数z是可构造的，则$[Q(z) : Q]$的次数为2的幂次

证明： 利用命题0.13可知，一个复数z可构造当且仅当z是多重二次的。那么就存在一个上升塔使得$Q(i) = F_0 \subseteq \cdots$，其中对每个$n = 0, 1, \cdots$都有$[F_n : F_{n-1}] \leq 2$，那么$F_n$作为$F_{n-2}$的一个扩域且$F_{n-1}$作为其中间域，那么有两种结果，一是$[F_n : F_{n-2}] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] = 2^2$，是一个2的幂次。对于第二种，我们假设$[F_n : F_{n-1}] = 2$而另一个为1，则结果为2是2的一个幂次，综上所述。若z是可构造的，则$[Q(z) : Q] = 2^m$，其中m是正整数。

注意：该定理逆命题不成立，有一个不可够作的复数使得$[Q(z) : Q] = 4$

0.15 定理：万提斯

利用尺规来倍立方体是不可能的

[4]例如，我们可以选择$P' = (0, -v/\mu)$和$Q' = [-v/\lambda]$

证明： 该定理的意思是$z = \sqrt[3]{2}$是否可构作。由于$x^3 - 2$是不可约的，所以$[Q(z):Q] = 3$利用定理0.13可知其不可构作。

0.16 定理：万提斯

用尺规作图三等分$60°$是不可能的。

证明： 我们设角的一条边在x轴上，这个问题就转化为了$z = \cos 20° + i \sin 20°$是否可构作，若$z$是可构作的，那么就有$\cos 20°$是可够作的。利用三倍角公式，我们有$\cos 3a = 4\cos^3 a - 3\cos a$，令$a = 20°$，那么我们把$\cos 20°$用$x$代替就得到方程$4x^3 - 3x - 1/2 = 0$，其中$\cos 60° = 1/2$。那么我们的问题就转为了该方程存在根否。方程又可以化为$f(x) = 8x^3 + 6x - 1 = 0$，但$F_7[x]$中该方程是不可约的，因此$f(x) \in Z[x] \subseteq Q(x)$也是不可约的。所以存在一个方程的根为方程的扩域，并且可以表示为多项式

$$b_0 + b_1 z + b_2 z^2$$

因此$[Q(z):Q] = 3$是不可构作的。

0.17 定理：林德曼

尺规作图来化圆为方是不可能的

证明： 该问题指的是是否可构造一个正方形，使得其面积等于单位圆的面积。

证明： 若正方形边长为z，那么就是再问$z = \sqrt{\pi}$是否可构作的。其中$Q(\pi)$是$Q(\sqrt{\pi})$的子空间，而π是Q上的超越数。则一个超越扩张里面的元素都是π与有理数的运算，因而$[Q(\pi):Q]$是无限域，进一步的有$[Q(\sqrt{\pi}):Q]$也是无限的。因此是不可构作的。

0.18 定理：高斯-万提斯

若p是奇素数，则正$p-$边形可构作当且仅当存在$t \geq 0$使得$p = 2^{2^t} + 1$对某个$t \geq 0$成立。

证明： 我们只证明存在性，这个问题的意思$z = e^{2\pi i/p}$是否可构作，其中z是分圆多项式$\phi_p(x)$的一个根。而分圆多项式是次数为$p-1$的不可约多项式。

现在，因为z是可构作的，那么$p-1=2^s$，得到

$$p = 2^s + 1$$

我们证明s是2的幂次，否则就存在$k>1$是奇数使得$s=km$，可以得到k是奇数，这样子就得到-1是方程的一个根了。这不是我们想要的、但事实上，我们有

$$x^k + 1 = (x+1)(x^{k-1} - x^{k-2} + x^{k-3} - \cdots + 1)$$

在$Z[x]$中是因式分解。最后，令$x = 2^m$次幂，我们就得到了一个不可能的因式分解

$$\begin{aligned} p =& 2^s + 1 = (2^m)^k + 1 \\ =& (2^m+1)((2^m)^{k-1}(2^m)^{k-2} + (2^m)^{k-3} - \cdots + 1) \end{aligned}$$

其中km不是2的幂次。矛盾。