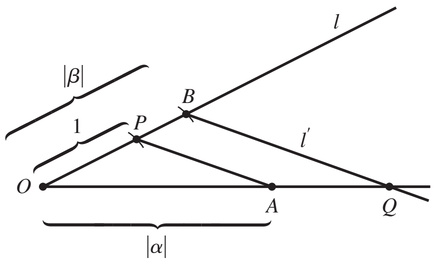
breakdown into cases according to their signs shows that $\alpha + \beta$ and $\alpha - \beta$ are still constructible.

The construction of $\alpha\beta$ is indicated in Fig. 41.3. We shall let $\overline{OA}$ be the line segment from the point O to the point A, and shall let $|\overline{OA}|$ be the length of this line segment. If $\overline{OA}$ is of length $|\alpha|$, construct a line l through O not containing $\overline{OA}$. (Perhaps, if O is at $(0, 0)$ and A is at $(a, 0)$, you use the line through $(0, 0)$ and $(4, 2)$.) Then find the points P and B on l such that $\overline{OP}$ is of length 1 and $\overline{OB}$ is of length $|\beta|$. Draw $\overline{PA}$ and construct l' through B, parallel to $\overline{PA}$ and intersecting $\overline{OA}$ extended at Q. By similar triangles, we have

$$\frac{1}{|\alpha|} = \frac{|\beta|}{|\overline{OQ}|},$$

so $\overline{OQ}$ is of length $|\alpha\beta|$.

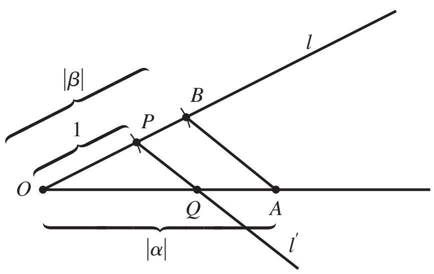


41.3 Figure

Finally, Fig. 41.4 shows that α/β is constructible if $\beta \neq 0$. Let $\overline{OA}$ be of length $|\alpha|$, and construct l through O not containing OA. Then find B and P on l such that $\overline{OB}$ is of length $|\beta|$ and $\overline{OP}$ is of length 1. Draw BA and construct l' through P, parallel to $\overline{BA}$, and intersecting $\overline{OA}$ at Q. Again by similar triangles, we have

$$\frac{|\overline{OQ}|}{1} = \frac{|\alpha|}{|\beta|},$$

so $\overline{OQ}$ is of length $|\alpha/\beta|$. ◆



41.4 Figure

41.5 Corollary The set of all constructible real numbers forms a subfield F of the field of real numbers.

Proof Proof of this corollary is immediate from Theorem 41.1. ◆

Thus the field F of all constructible real numbers contains $\mathbb{Q}$, the field of rational numbers, since $\mathbb{Q}$ is the smallest subfield of $\mathbb{R}$.

From now on, we proceed analytically. We can construct any rational number. Regarding our given segment

0______1

of length 1 as the basic unit on an x-axis, we can locate any point (q_1, q_2) in the plane with both coordinates rational. Any further point in the plane that we can locate by using a compass and a straightedge can be found in one of the following three ways:

1. as an intersection of two lines, each of which passes through two known points having rational coordinates,
2. as an intersection of a line that passes through two points having rational coordinates and a circle whose center has rational coordinates and whose radius is rational.
3. as an intersection of two circles whose centers have rational coordinates and whose radii are rational.

Equations of lines and circles of the type discussed in 1, 2, and 3 are of the form

$$ax + by + c = 0$$

and

$$x^2 + y^2 + dx + ey + f = 0,$$

where a, b, c, d, e, and f are all in $\mathbb{Q}$. Since in Case 3 the intersection of two circles with equations

$$x^2 + y^2 + d_1x + e_1y + f_1 = 0$$

and

$$x^2 + y^2 + d_2x + e_2y + f_2 = 0$$

is the same as the intersection of the first circle having equation

$$x^2 + y^2 + d_1x + e_1y + f_1 = 0,$$

and the line (the common chord) having equation

$$(d_1 - d_2)x + (e_1 - e_2)y + f_1 - f_2 = 0,$$

we see that Case 3 can be reduced to Case 2. For Case 1, a simultaneous solution of two linear equations with rational coefficients can only lead to rational values of x and y, giving us no new points. However, finding a simultaneous solution of a linear equation with rational coefficients and a quadratic equation with rational coefficients, as in Case 2, leads, upon substitution, to a quadratic equation. Such an equation, when solved by the quadratic formula, may have solutions involving square roots of numbers that are not squares in $\mathbb{Q}$.

In the preceding argument, nothing was really used involving $\mathbb{Q}$ except field axioms. If H is the smallest field containing those real numbers constructed so far, the argument shows that the "next new number" constructed lies in a field $H(\sqrt{\alpha})$ for some $\alpha \in H$, where $\alpha > 0$. We have proved half of our next theorem.

41.6 Theorem The field F of constructible real numbers consists precisely of all real numbers that we can obtain from $\mathbb{Q}$ by taking square roots of positive numbers a finite number of times and applying a finite number of field operations.

Proof We have shown that F can contain no numbers except those we obtain from $\mathbb{Q}$ by taking a finite number of square roots of positive numbers and applying a finite number