Chapter Notes

Chapter 1: The Real and Complex Number Systems

Principles of Mathematical Analysis, 3rd edition, *by Walter Rudin*

Author: Robert Lincoln, July, 2023 Updated: December, 2025

Disclaimer: These unofficial notes are provided for educational purposes. Any errors are solely the responsibility of the author.

1.1 Example

One may well wonder how Rudin came up with his formulas for q relative to p showing the set A has no largest number (all positive rationals p such that $p^2 < 2$), and the set B has no smallest number (all positive rationals p such that $2 < p^2$), a concept that touches upon the notion of a *cut* discussed in the Appendix to this chapter.

Let us first note a few things about the formulas.

$$q = \frac{2p+2}{p+2} = \frac{2(p+1)}{p+2} \Rightarrow q^2 = \frac{4(p+1)^2}{(p+2)^2}.$$

$$\therefore q^2 - 2 = \frac{4(p+1)^2}{(p+2)^2} - \frac{2(p+2)^2}{(p+2)^2} = \frac{2[2p^2+4p+2-(p^2+4p+4)]}{(p+2)^2} = \frac{2(p^2-2)}{(p+2)^2}.$$

Thus, the two formulas for q relative to p are as follows, and, importantly, each involves p^2-2 showing the relationship of p^2 to 2.

$$q = p - \frac{(p^2-2)}{p+2} = \frac{2p+2}{p+2} \qquad [3]$$

$$q^2 - 2 = \frac{2(p^2-2)}{(p+2)^2} \qquad [4]$$

[3] shows q relative to p, while [4] shows q^2 relative to 2, each with the same common term of p^2-2, showing p^2 relative to 2.

[4] shows p and q are in the same set (A or B). So, if $p^2 > 2$ then $q^2 > 2$, and if $p^2 < 2$ then $q^2 < 2$.

[3] shows if $p^2 < 2$, then $p - \frac{(p^2-2)}{p+2} > p$, so $q > p$, and as a result, there is always a larger number q greater than p but still such that $q^2 < 2$. Similarly, if $p^2 > 2$, then $p - \frac{(p^2-2)}{p+2} < p$, so $q < p$, and as a result, there is always a smaller number q less than p but still such that $q^2 > 2$. The $\frac{2p+2}{p+2}$ term assures that q is always positive when p is positive.

So, where did these formulas come from? The key insight is that expressions for q and q^2 contain a term of p^2-2 to make judgments of p^2 relative to the number 2.

Working from scratch, we want a relation of q relative to p, so start with:

$$q = p - f[p^2 - 2]$$

where f is some positive factor, so that if $p^2 > 2$ (and so in set B), then we subtract from p to get a smaller number in order to get $q < p$, and when $p^2 < 2$ (and so in set A), then q will be bigger then p. We are going to have to square q to get some relation of q^2 relative to 2, so let $f = \dfrac{1}{p+k}$, where k is some constant. That way, when we simplify, we will get rid of the p^2 terms to keep things simple. Thus,

$$q = p - \frac{(p^2-2)}{p+k} = \frac{p^2 + kp - (p^2-2)}{p+k} = \frac{kp+2}{p+k}$$

Now when we square q, we get terms with p^2 instead of p^4. So, doing this, and showing q^2 relative to 2, we get:

$$q^2 - 2 = \frac{(kp+2)^2}{(k+p)^2} - 2 = \frac{k^2p^2 + 4kp + 4}{(k+p)^2} - \frac{2(k+p)^2}{(k+p)^2} = \frac{(k^2-2)p^2 + 4 - 2k^2}{(k+p)^2}$$

How can we get a p^2-2 term in the numerator of that last equation? $k = 1$ gives us $-(p^2-2)$, but then $q^2 - 2$ and $p^2 - 2$ have opposite signs, and we need them to have the same sign so that p and q are in the same set (A or B). However, $k = 2$ gives $2(p^2 - 2)$ in the numerator, and so will work. So, $k = 2$ gives us the formulas used in Rudin.

A very similar analysis could be performed if we were investigating the square root of 3. In that case, $p^2 - 3$ is the important term needed in the formulas for q and $q^2 - 3$. The formulas would be, using our analysis above, and finding $k = 3$ works for our constant of choice,

$$q = p - \frac{(p^2-3)}{p+3} = \frac{3p+3}{p+3}$$

$$q^2 - 3 = \frac{6(p^2-3)}{(p+3)^2}$$

1.9 Examples

We will prove the assertion in (a): β is an upper bound of set A if and only if $\beta \in B$.

(1) If $\beta \in Q$ and β is an upper bound of A, then $\beta \in B$.

Since Q is ordered, either $\beta^2 = 2, \beta^2 < 2$, or $\beta^2 > 2$. Example 1.1 in Rudin showed $\beta^2 \neq 2$. Suppose $\beta^2 < 2$ so that $\beta \in A$. Example 1.1 showed A has no largest element, so there is an $\alpha \in A$ such that $\beta < \alpha \Rightarrow \beta$ is not an upper bound of A, a contradiction. $\therefore \beta^2 > 2 \Rightarrow \beta \in B$.

So, all rational upper bounds of A are in B.

(2) If $\beta \in B$, then β is an upper bound of A.

$\beta \in B \Rightarrow \beta^2 > 2$. Let $\alpha \in A$ so that $\alpha^2 < 2$. $\therefore \alpha^2 < \beta^2 \Rightarrow \alpha < \beta$.

Thus, B is the set of all rational bounds of A. Since B has no smallest member, A has no least upper bound in Q.

1.10 Definition

The definition doesn't say every nonempty set of S has a least upper bound. It says any nonempty subset of S *with an upper bound* in S has a least upper bound.

1.14 Proposition

It is assumed that the principle of substitution of variables holds, and that the axioms of equality hold (i.e., $a = a, a = b \Rightarrow b = a$, and $a = b$ and $b = c \Rightarrow a = c$).

For proof of (d),

$$\begin{aligned}
(-x) + [-(-x)] &= 0 && \text{using (A5)}\\
\therefore x + [(-x) + [-(-x)]] &= x + 0 = x && \text{using (A4)}\\
\therefore [x + (-x)] + [-(-x)] &= x && \text{using (A3)}\\
\therefore 0 + [-(-x)] &= x && \text{using (A5)}\\
\therefore [-(-x)] &= x && \text{using (A4)}
\end{aligned}$$

1.15 Proposition

(a) If $x \neq 0$ and $xy = xz$ then $y = z$.

Using Rudin's template in 1.14,

$y = 1y = ((\frac{1}{x})x)y = \frac{1}{x}(xy) = \frac{1}{x}(xz) = (\frac{1}{x}x)z = 1z = z$.

(b) If $x \neq 0$ and $xy = x$ then $y = 1$.

Use (a) with $z = 1$.

(c) If $x \neq 0$ and $xy = 1$ then $y = 1/x$.

Use (a) with $z = 1/x$.

(d) If $x \neq 0$ then $1/(1/x) = x$.

From (M5) we know that $1/x$ exists since $x \neq 0$. Since $x(1/x) = 1$ then $1/x \neq 0$.

As in the proof of 1.14(d),

$$\begin{aligned}
\frac{1}{x}\frac{1}{\frac{1}{x}} &= 1 && \text{using (M5)}\\
\therefore x\left(\frac{1}{x}\frac{1}{\frac{1}{x}}\right) &= x1 = x && \text{using (M4)}\\
\therefore \left(x\frac{1}{x}\right)\frac{1}{\frac{1}{x}} &= x && \text{using (M3)}\\
\therefore 1 \cdot \frac{1}{\frac{1}{x}} &= x && \text{using (M5)}\\
\therefore \frac{1}{\frac{1}{x}} &= x && \text{using (M4)}
\end{aligned}$$

1.16 Proposition

Note that 1.16(a), $0x = x$, was proved only using the field axioms for addition and (D), the distributive axiom. One can then prove $1 \neq 0$ using 1.16(a). For if $1 = 0$ then for $a \neq 0$, $a = a1 = a0 = 0$, a contradiction. So, technically, $1 \neq 0$ is not needed in (M4).

1.18 Proposition

Rudin's use of *vice versa* is somewhat confusing in 1.18(a). It usually means the converse. So if $p \to q$, *vice versa* means $q \to p$. But for $x > 0 \to -x < 0$ Rudin means $x < 0 \to -x > 0$.

1.20 Theorem

The proof of (b) depends on the assumption that for a given finite set of integers, such as $\{-m_2, -m_2+1, \ldots, m_1-1, m_1\}$, we can choose the member, call it $m-1$, that is the largest such that $m - 1 \leq nx$.

1.21 Theorem

The theorem should state that $y > 0$. For, there are two values of y such that $y^2 = 4$ $(y = -2, y = 2)$, but there is one and only one value of $y > 0$ such that $y^2 = 4$.

The theorem is obviously true for $n = 1$, so the proof of the theorem will assume $n > 1$.

Rudin first makes a statement about uniqueness. The statement $0 < y_1 < y_2 \Rightarrow 0 < y_1^n < y_2^n$ is derived from 1.18(b) and induction. So if $0 < y < z$ then assuming $0 < y^k < z^k$, then $0 < y^{k+1} < z^k y$ and $0 < z^k y < z^k z = z^{k+1}$. $\therefore 0 < y^{k+1} < z^{k+1}$. Thus, $0 < y^n < z^n$ for $n = 1, 2, 3, \ldots$.

Let us first prove the preliminary statements regarding the variable t and then prove the binomial statement before proceeding into the main proof.

For $t = x/(x+1)$, since $0 < 1$ and $0 < x$, then $0 < x < x+1 \Rightarrow 0 < x/(x+1) < 1$, so $0 < t < 1$. $\therefore 0 < t^2 < t < 1$. Assuming $0 < t^k < t < 1$ for $k > 2$, then $0 < t^{k+1} < t^2 < t < 1$. $\therefore$ For all $n \geq 2$ (and not $n = 1$), $0 < t^n < t < 1$. Also, $0 < x \Rightarrow 0 < x^2 \Rightarrow x < x + x^2 \Rightarrow x/(x+1) < x$. Thus $t < x$. $\therefore$ For $t = x/(x+1)$, we have $0 < t^n < t < x$ for $n \geq 2$.

For $t > 1 + x$, note that for $x > 0$, $1 + x > 1$ so $t > 1 \Rightarrow t^n > t$, by induction for $n \geq 2$. Also, since $1 > 0$ then $x + 1 > x$ so $t > x + 1 > x$. Thus, for $n \geq 2$, we have $t^n > t > x$.

The above statements mean the set E is not empty $(x/(x+1) \in E)$ and E is bounded above by $x+1$. Thus $E \subset R$ has a least upper bound, and since E is composed of positive numbers, the least upper bound must be positive.

Let us now prove the binomial realtion mentioned in Rudin.

Lemma $b^n - a^n = (b-a)\sum_{k=1}^{n} b^{n-k}a^{k-1} = (b-a)(b^{n-1}a^0 + b^{n-2}a^1 + \ldots + b^0 a^{n-1})$

Proof: For $n = 1$, $b - a = (b-a)b^0a^0 = b - a$.

Assume true for $m > 2$. Then $b^m - a^m = (b-a)\sum_{k=1}^{m} b^{m-k}a^{k-1}$, so

$$\begin{aligned} b^{m+1} - a^{m+1} &= b^{m+1} - ba^m + ba^m - a^{m+1} \\ &= b(b^m - a^m) + (b-a)a^m \\ &= b(b-a)\sum_{k=1}^{m} b^{m-k}a^{k-1} + (b-a)a^m \end{aligned}$$

Combining the factors $(b-a)$,

$$\begin{aligned} b^{m+1} - a^{m+1} &= b(b-a)\sum_{k=1}^{m} b^{m-k}a^{k-1} + (b-a)a^m \\ &= (b-a)\left(a^m + b\sum_{k=1}^{m} b^{m-k}a^{k-1}\right) \\ &= (b-a)\left(b^0a^m + \sum_{k=1}^{m} b^{m+1-k}a^{k-1}\right) \\ &= (b-a)\left(\sum_{k=1}^{m+1} b^{m+1-k}a^{k-1}\right) \end{aligned}$$

$\therefore$ The formula is true for $m+1$ when it is true for $m > 2$. So, it is true for $n = 1, 2, 3, ...$

Note in the formula $b^n - a^n = (b-a)\sum_{k=1}^{n} b^{n-k}a^{k-1}$, there are n terms for the sigma notation. When $0 < a < b$, $a^{k-1} < b^{k-1}$ when $k > 1$. $\therefore b^{n-k}a^{k-1} < b^{n-k}b^{k-1} = b^{n-1}$ for $n > 1$. Thus,

$$\sum_{k=1}^{n} b^{n-k}a^{k-1} < \sum_{k=1}^{n} b^{n-k}b^{k-1} = \sum_{k=1}^{n} b^{n-1} = b^{n-1}\sum_{k=1}^{n} 1 = nb^{n-1}$$

So, for $n > 1$,

$$b^n - a^n < (b-a)nb^{n-1}$$

Now back to the main proof showing for every real $x > 0$ and every integer $n > 1$ there is exactly one $y > 0$ such that $y^n = x$.

Rudin defined set $E = \{t \in R : t > 0, t^n < x\}$ and $y = \sup E$. To show $y^n < x$ is false, we find a small $h > 0$ such that $y + h \in E$, contradicting y as an upper bound of E. To show $y^n > x$ is false, we find a small $k > 0$ such that $y - k$ is an upper bound for E. Thus, $y^n = x$.

(a) $y^n < x$

Choose h such that $0 < h < 1$. Then $0 < y < y + h$ and we can use the binomial relation and its inequality relation above so that $(y+h)^n - y^n < hn(y+h)^{n-1}$. So we have only one term with h, we use $h < 1 \Rightarrow y + h < y + 1 \Rightarrow (y+h)^{n-1} < (y+1)^{n-1}$. Thus, $(y+h)^n - y^n < hn(y+1)^{n-1}$. We want $(y+h)^n - y^n < x - y^n$ so we can state $(y+h)^n < x$ in order to get $y + h \in E$. Thus, we require h such that $hn(y+1)^{n-1} < x - y^n$, which is possible since $0 < x - y^n$. So, we require h to be:

$$0 < h < 1 \text{ and } h < \frac{x - y^n}{n(y+1)^{n-1}}$$

All variables (x, y, n) are known, and this will yield $y + h \in E$, contradicting $y = \sup E$.

(b) $y^n > x$

We need a small $k > 0$ so that $0 < y - k < y$ and so that $y - k \notin E$. This will mean $y - k$ is an upper bound for E, and so contradict $y = \sup E$.

So far, $0 < k < y$, and since $0 < y - k < y$, we can use the binomial inequality relation above to further specify k. Thus, $y^n - (y-k)^n < kny^{n-1}$. Note that $0 < y^n - x$. So, if we require k such that $kny^{n-1} < y^n - x$, then $y^n - (y-k)^n < y^n - x$, so $x < (y-k)^n$, as needed. Therefore, given x, y, n, set k such that:

$$0 < k < y \text{ and } k < \frac{y^n - x}{ny^{n-1}}$$

This will yield $0 < y - k \notin E$ so that $y - k$ is an upper bound for E, contradicting $y = \sup E$.

1.21 Corollary

The proof depends on $\alpha^n \beta^n = (\alpha\beta)^n$ which is proved by induction.

Clearly true for $n = 1$. Suppose true for $k > 1$. Then

$$\begin{aligned}
\alpha^{k+1}\beta^{k+1} &= \alpha^k \alpha \beta^k \beta && \text{definition of } x^{n+1} \\
&= \alpha^k \beta^k \alpha \beta && \text{using (M2)} \\
&= (\alpha\beta)^k \alpha\beta && \text{induction hypothesis} \\
&= (\alpha\beta)^{k+1} && \text{definition of } x^{n+1}
\end{aligned}$$

Note: A number of exponential properties for R follow from 1.18(b) and by using induction.

(1) If $0 < a < b$ and $0 < c < d$, then $0 < ac < bd$.

By 1.18(b) $0 < ac < bc$ and $0 < bc < bd \Rightarrow 0 < ac < bd$ as R is an ordered set.

(2) $0 < a \Rightarrow 0 < a^n$ for any positive integer n.

Proof using induction and (1).

(3) $0 < a < b \Rightarrow 0 < a^n < b^n$ for any positive integer n.

Proof by induction and using (1).

(4) $0 < a < b \Rightarrow 0 < a^{1/n} < b^{1/n}$ for any positive integer n.

By Theorem 1.21, $(a^{1/n})^n = a$ and $(b^{1/n})^n = b$.

If $a^{1/n} = b^{1/n}$ then $a = (a^{1/n})^n = (b^{1/n})^n = b$, a contradiction.

If $b^{1/n} < a^{1/n}$ then by (3), $0 < (b^{1/n})^n < (a^{1/n})^n \Rightarrow 0 < b < a$, a contradiction.

(5) $0 < a \Rightarrow (a^m)^{1/n} = (a^{1/n})^m$ for positive integers m, n.

Let n be any positive integer. Use induction on m.

Clearly true for $m = 1$. Suppose true for $k > 1 : (a^k)^{1/n} = (a^{1/n})^k$.

$$\begin{aligned}
(a^{k+1})^{1/n} &= (a^k a)^{1/n} && \text{definition of } x^{n+1} \\
&= (a^k)^{1/n} a^{1/n} && \text{using 1.21 Corollary} \\
&= (a^{1/n})^k a^{1/n} && \text{induction hypothesis} \\
&= (a^{1/n})^{k+1} && \text{definition of } x^{n+1}
\end{aligned}$$

Therefore the statement is true for $k + 1$ when true for $k > 1$, and so is true for all positive integers m.

1.22 Decimals

Rudin makes two statements in this section that will be proved: (1) For $x > 0$, $x = \sup E$, the set of numbers containing the decimal expansion of x, and (2) set E is bounded above.

(1) $x = \sup E$

Choose n_0

Given any $x > 0$, by the Archimedean property there is an integer n such that $0 < x < n$. From the finite set $\{0, 1, 2, \ldots, n-1\}$ choose the largest integer n_0 such that $n_0 \leq x$. Therefore,

$$n_0 \leq x < n_0 + 1$$

Choose n_1

$\therefore 10n_0 \leq 10x < 10n_0 + 10$, so $0 \leq 10x - 10n_0 < 10$. From the set $\{0, 1, 2, \ldots, 9\}$ choose n_1 to be the largest integer such that $0 \leq n_1 \leq 10x - 10n_0 < 10$. Thus, we have

$$n_1 \leq 10x - 10n_0 < n_1 + 1$$

or $10n_0 + n_1 \leq 10x < 10n_0 + n_1 + 1$. Dividing by 10,

$$n_0 + \frac{n_1}{10} \leq x < n_0 + \frac{n_1}{10} + \frac{1}{10}$$

Choose n_2

$\therefore 10^2 n_0 + 10n_1 \leq 10^2 x < 10^2 n_0 + 10n_1 + 10$, so $0 \leq 10^2 x - 10^2 n_0 - 10n_1 < 10$. From the finite set $\{0, 1, 2, \ldots, 9\}$ choose n_2 to be the largest integer such that $0 \leq n_2 \leq 10^2 x - 10^2 n_0 - 10n_1 < 10$. Thus, we have

$$n_2 \leq 10^2 x - 10^2 n_0 - 10n_1 < n_2 + 1$$

or $10^2 n_0 + 10n_1 + n_2 \leq 10^2 x < 10^2 n_0 + 10n_1 + n_2 + 1$. Dividing by 10^2,

$$n_0 + \frac{n_1}{10} + \frac{n_2}{10^2} \leq x < n_0 + \frac{n_1}{10} + \frac{n_2}{10^2} + \frac{1}{10^2}$$

Choose n_k

Having chosen $n_0, n_1, \ldots, n_{k-1}$, choose n_k from the finite set $\{0, 1, 2, \ldots, 9\}$ to be the largest integer such that

$$n_k \leq 10^k x - 10^k n_0 - 10^{k-1} n_1 - \ldots - 10 n_{k-1} < n_k + 1$$

Rearranging and dividing by 10^k,

$$n_0 + \frac{n_1}{10} + \ldots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k} \leq x < n_0 + \frac{n_1}{10} + \ldots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k} + \frac{1}{10^k} \qquad [1]$$

The process will stop if, for some k, $n_0 + \frac{n_1}{10} + \ldots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k} = x$. Otherwise, it will continue indefinitely.

Let E be the set of numbers $E = \left\{n_0, n_0 + \frac{n_1}{10}, n_0 + \frac{n_1}{10} + \frac{n_2}{10^2}, \ldots\right\}$. From the construction above, clearly x is an upper bound of E.

To prove $x = \sup E$, suppose y is another upper bound of E such that $0 < y < x$. $\therefore 0 < x - y$ so $0 < \frac{1}{x-y}$. By the Archimedean property of R (Theorem 1.20), there is a positive integer n such that $\frac{1}{x-y} < n$. Note that $n < 10^n$, which is easily proved by induction. $\therefore$ From the finite set $\{0, 1, 2, \ldots, n\}$, choose the smallest integer k such that $\frac{1}{x-y} \leq 10^k$. $\therefore 0 < 10^{-k} \leq x - y \Rightarrow y + \frac{1}{10^k} \leq x$. Since y is an upper bound of E, for the member of E taken to the k-th decimal, $n_0 + \frac{n_1}{10} + \ldots + \frac{n_k}{10^k} \leq y$. Therefore,

$$n_0 + \frac{n_1}{10} + \ldots + \frac{n_k}{10^k} + \frac{1}{10^k} \leq y + \frac{1}{10^k} \leq x$$

But then $n_0 + \frac{n_1}{10} + \ldots + \frac{n_k}{10^k} + \frac{1}{10^k} \leq x$ which contradicts [1]. Thus, $x = \sup E$.

(2) E is bounded above

Proof is by induction. Using the definition of E in (1) and the construction of the elements of E, we will show that $n_0 + 1$ is an upper bound for E by showing it is greated than every element in E.

Clearly $n_0 < n_0 + 1$.

$n_1 < 10$ by definition, so $\frac{n_1}{10} < 1 \Rightarrow n_0 + \frac{n_1}{10} < n_0 + 1$.

Suppose for any $k > 1$, $n_0 + \frac{n_1}{10} + \ldots + \frac{n_k}{10^k} < n_0 + 1$. Therefore,

$$10^k n_0 + 10^{k-1} n_1 + \ldots + n_k < 10^k n_0 + 10^k$$

Note that all the terms in the above inequality are integers. Therefore we can remove the strict inequality by subtracting 1 from the right side,

$$10^k n_0 + 10^{k-1} n_1 + \ldots + n_k \leq 10^k n_0 + 10^k - 1$$

Multiplying by 10,

$$10^{k+1}n_0 + 10^k n_1 + \ldots + 10n_k \leq 10^{k+1}n_0 + 10^{k+1} - 10$$

Since $n_{k+1} \leq 9$ by definition, then by adding this to the above inequality,

$$10^{k+1}n_0 + 10^k n_1 + \ldots + 10n_k + n_{k+1} \leq 10^{k+1}n_0 + 10^{k+1} - 1$$

Again the terms are all integers, so we can go back to the strict inequality by removing the term -1 from the right side,

$$10^{k+1}n_0 + 10^k n_1 + \ldots + 10n_k + n_{k+1} < 10^{k+1}n_0 + 10^{k+1}$$

Now, dividing by 10^{k+1},

$$n_0 + \frac{n_1}{10} + \ldots + \frac{n_k}{10^k} + \frac{n_{k+1}}{10^{k+1}} < n_0 + 1$$

Thus, $n_0 + 1$ is greater than every element in E and so is an upper bound of E.

1.31 Theorem

Let $z = (a, b) = a + bi$ and $w = (c, d) = c + di$.

(a) $\overline{z + w} = \overline{z} + \overline{w}$

$$\begin{aligned}
\overline{z+w} &= \overline{(a,b)+(c,d)} && \text{definition of } z,\ w\\
&= \overline{(a+c,b+d)} && \text{definition of } z+w\\
&= (a+c,-(b+d)) && \text{definition of conjugate}\\
&= (a+c,-b-d) && -(x+y) = -x-y\\
&= (a,-b)+(c,-d) && \text{definition of complex addtion}\\
&= \overline{z}+\overline{w} && \text{definition of } \overline{z},\overline{w}
\end{aligned}$$

(b) $\overline{zw} = \overline{z} \cdot \overline{w}$

$$\begin{aligned}
\overline{zw} &= \overline{(a,b)(c,d)} && \text{definition of } z, w\\
&= \overline{(ac-bd,ad+bc)} && \text{definition of } z \cdot w\\
&= (ac-bd,-(ad+bc)) && \text{definition of conjugate}\\
&= (ac-bd,-ad-bc) && -(x+y) = -x-y\\
&= (ac-(-b)(-d),a(-d)+(-b)c) && \text{using 1.16(c),1.16(d)}\\
&= (a,-b)(c,-d) && \text{definition of complex multiplication}\\
&= \overline{z}\cdot\overline{w} && \text{definition of } \overline{z},\overline{w}
\end{aligned}$$

(c) $z + \overline{z} = 2\mathrm{Re}(z), z - \overline{z} = 2i\mathrm{Im}(z)$

For $z = a + bi$, $a = \mathrm{Re}(z), b = \mathrm{Im}(z)$.

$z + \overline{z} = a + bi + a - bi = 2a = 2\mathrm{Re}(z)$.

$z - \overline{z} = a + bi - (a - bi) = 2bi = 2ib = 2i\mathrm{Im}(z)$.

(d) *$z\overline{z}$ is real and positive (except when $z = 0$).*

$z\overline{z} = (a,b)(a,-b) = (a^2 - b(-b), a(-b) + ba) = (a^2 + b^2, 0) = a^2 + b^2$.

If $z \neq 0$ then $a \neq 0$ or $b \neq 0$, or both. If $a \neq 0, a^2 > 0$, if $b \neq 0, b^2 > 0$, using 1.18(d).

$\therefore$ If $z \neq 0$ then $z\overline{z} = a^2 + b^2 > 0$.

If $z = 0$, then $z\overline{z} = a^2 + b^2 = 0 + 0 = 0$.

1.32 Definition

If $z = (a,b)$, then $\overline{z} = (a,-b)$, so $\overline{\overline{z}} = (a,-(-b)) = (a,b) = z$.

$\therefore |z| = (z\overline{z})^{1/2} = (\overline{z}z)^{1/2} = (\overline{z} \cdot \overline{\overline{z}})^{1/2} = |\overline{z}|$, which proves 1.33(b).

Note when x is real, $x \leq |x|$ and $-x \leq |x|$.

1.35 Theorem

In the proof, note B is real, so $B = \overline{B}$. C is complex, so $C \neq \overline{C}$. $C = \sum a_j\overline{b_j}$, so $\overline{C} = \sum \overline{a_j}b_j$.

$$\begin{aligned}
\sum |Ba_j - Cb_j|^2 &= \sum (Ba_j - Cb_j)(\overline{Ba_j - Cb_j}) \\
&= \sum (Ba_j - Cb_j)(\overline{B}\,\overline{a_j} - \overline{C}\,\overline{b_j}) \\
&= \sum (Ba_j - Cb_j)(B\overline{a_j} - \overline{C}\,\overline{b_j}) \\
&= \sum (B^2 a_j\overline{a_j} - B\overline{C}a_j\overline{b_j} - BC\overline{a_j}b_j + C\overline{C}b_j\overline{b_j}) \\
&= B^2 \sum |a_j|^2 - B\overline{C} \sum a_j\overline{b_j} - BC \sum \overline{a_j}b_j + |C|^2 \sum |b_j|^2 \\
&= B^2 A - B\overline{C}C - BC\overline{C} + |C|^2 B \\
&= B^2 A - B|C|^2 - B|C|^2 + |C|^2 B \\
&= B^2 A - B|C|^2 \\
\therefore \sum |Ba_j - Cb_j|^2 &= B(AB - |C|^2)
\end{aligned}$$

We are trying to prove $|C|^2 \leq AB$.

Since $B = \sum |b_j|^2$, a sum of all nonnegative terms, if $B = 0$ then all $b_j = 0$ and so $C = 0$ and the statement is true. $\therefore$ Assume $B > 0$.

$\sum |Ba_j - Cb_j|^2$ is also composed of all nonnegative terms, so $B(AB - |C|^2) \geq 0$. Since $B > 0$ then $(AB - |C|^2) \geq 0$, or $|C|^2 \leq AB$.

Note: If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are real, then $\sum_{j=1}^{n} a_j b_j$ can be considered the inner product, or scalar product, discussed in section 1.36, and so the Schwarz inequality becomes $|\mathbf{x}\cdot\mathbf{y}| \leq |\mathbf{x}||\mathbf{y}|$, which is Theorem 1.37(d), where $\mathbf{x} = (a_1, \ldots, a_n), \mathbf{y} = (b_1, \ldots, b_n)$.

1.36 Definition

Should state for $\mathbf{x} = (x_1, \ldots, x_,)$ and $\mathbf{y} = (y_1, \ldots, y_k), \mathbf{x} = \mathbf{y} \iff x_i = y_i, i = 1, 2, \ldots, k$.

Appendix

Step 1

Rudin uses "lower cuts", that is, sets composed of rational numbers less than a certain rational number. The set R could be constructed from "upper cuts" instead.

Examples of cuts:

(a) $A = \{p \in Q : p < 2\}$. Using $p \leq 2$ makes A not a cut since property (III) does not hold.

(b) $A = \{p \in Q : p^3 < 2\}$. Note $p < 0 \Rightarrow p^3 < 0$.

(c) $A = \{p \in Q : p^2 < 2\}$ is not a cut since all negative numbers less than, say, -2 are not in A.

(d) $A = \{p \in Q : p < 0 \text{ or } p^2 < 2\}$ is a cut.

Example (a) is the definition of a simple cut, whereas (d) is a more complex cut. In (a), any rational number could be used instead of the number 2. And, when the number 0 is used, Rudin, in Step 4, defines this cut as 0^*.

Two implications of property (II) in the definition of cuts:

(1) If $p \in \alpha$ and $q \notin \alpha$, then $p < q$.

For if $q \leq p$, then by (II), $q \in \alpha$.

(2) If $r \notin \alpha$ and $r < s$, then $s \notin \alpha$.

For if $s \in \alpha$, then by (II), $r < s \Rightarrow r \in \alpha$.

Step 2

Note Rudin uses the symbol $\subset$ to mean "subset of" and not necessarily "proper subset of". Therefore, to the statement $\beta \subset \alpha$ he adds $\beta \neq \alpha$, so that β is a proper subset of α, and so $\beta < \alpha$.

Step 3

Note that R is defined as a collection of certain subsets (*cuts*) of Q. R is not the union of all these cuts. This makes it easy to establish R as an ordered set (Step 2) having the least upper bound property. The hard part will be showing R is a field.

Given any nonempty subset A of R, it turns out that the least upper bound of A exists and happens to be the union of all the cuts of A, as shown in Rudin's proof.

Specifically, in example (a) in Step 1, A has just one member, and its member is the least upper bound of A. You could name this cut "2". Example (d) in Step 1 also has just one member, and so it's least upper bound is also the set A, and you could name this set "$\sqrt{2}$".

Step 4

(A1) In Rudin's proof for showing $\alpha + \beta \neq Q$, for $r' \notin \alpha, s' \notin \beta$, then for all $r \in \alpha, r < r'$, and for all $s \notin \beta, s < s'$. Since Q is an ordered field, then $r + s < r' + s'$.

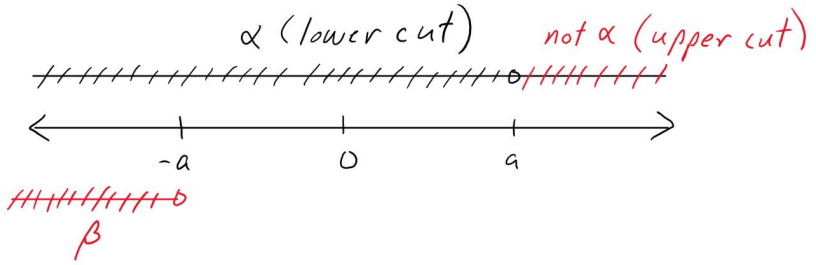
If $r' + s' \in \alpha + \beta$, then there would be an $r \in \alpha, s \in \beta$ such that $r + s = r' + s'$. But as shown, there is no such $r \in \alpha$ and $s \in \beta$.

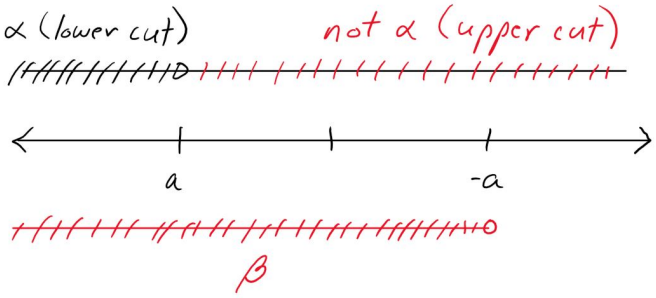
(A2) The proof involves first showing $\alpha + \beta \subset \beta + \alpha$ and then showing $\beta + \alpha \subset \alpha + \beta$.

(A3) Similar to (A2), first show $(\alpha + \beta) + \gamma \subset \alpha + (\beta + \gamma)$ and then $\alpha + (\beta + \gamma) \subset (\alpha + \beta) + \gamma$.

(A4) Again, show $\alpha + 0^* \subset \alpha$ and then show $\alpha \subset \alpha + 0^*$.

(A5) The definition of β at first seems rather convoluted. However, to see the motivation for the definition, consider initially α as a simple cut: $\alpha = \{q \in Q \text{ such that } q < a, a \in Q\}$. An upper cut for α would be $\{q \in Q \text{ such that } a < q, a \in Q\}$. Then β is just the negative of the upper cut: $\{p \in Q \text{ such that } p < -a, a \in Q\}$. See the figures below, which show simple cuts when $a > 0$ and $a < 0$. Intuitively, adding elements from α and β should result in 0^*.





Then why not define β more simply? Because we don't know if α is a simply defined cut or a cut from a more complex definition, such as (d) in Step 1. In a simple cut, we know where the boundary is. In a complex defined cut, we may not be able to specify where the boundary is in the set Q, as is the case with example (d) in Step 1.

Thus, Rudin defines β by what is *not* in cut α. What is not in α is an upper cut based on α. If $q \notin \alpha$ (and so q is in an upper cut), then analogous to property (III) for lower cuts, there should be an element in the upper cut, smaller than q, and still be in the upper cut: upper cuts have no smallest element. For some $r > 0, q - r < q$, such that $q - r$ is still in the upper cut (and so not in α). Since β is the negative of the upper cut, then $-p$ serves the purpose of q in the upper cut. Thus, $-p$ is in the upper cut and so not in α, and so $-p - r$ is in the upper cut and not in α. p is in β, the negative of the upper cut.

(1) $\beta \in R$

If $s \notin \alpha$, define $p = -s - 1$. Then $s = -p - 1$, so $-p - 1 \notin \alpha \Rightarrow p \in \beta$, so β is not empty.

Now pick any $q \in \alpha$. If $-q \in \beta$, then for some $r > 0, -(-q) - r \notin \alpha$, by definition of β. So $q - r \notin \alpha$, a contradiction to the fact that $q - r \in \alpha$ by property (II) for cuts. Thus $-q \notin \beta \Rightarrow \beta \neq Q$.

Thus, β satisfies property (I) for cuts.

Showing β satisfies property (II) uses the fact that Q is an ordered field when stating that $q < p \Rightarrow -p - r < -q - r$ for some $r > 0$.

To show β satisfies property (III), we already have $p \in \beta$ and $r > 0$ so that $-p-r \notin \alpha$. Thus, looking at $-p - r = (-p - r/2) - r/2 = -(p + r/2) - r/2$, we can define $t = p + r/2$, and use $r/2 > 0$ for our "$r > 0$" in the definition of β, which gives us $t \in \beta$, and note that $t = p + r/2 > p$ using the properties for Q as an ordered field.

(2) $\alpha + \beta \subset 0^*$

If $s \in \beta$, then there is an $r > 0$ such that $-s - r \notin \alpha$. Note that $-s - r < -s$ since $-r < 0$. Thus, if $-s \in \alpha$, then so is $-s - r$ using property (II) for the cut α. This contradiction means $-s \notin \alpha \Rightarrow r < -s$ for $r \in \alpha$, using implication (1) stated in Step 1.

(3) $0^* \subset \alpha + \beta$

The proof of this depends on the Archimedean property for rational numbers. Rudin proves the Archimedean property for real numbers in Theorem 1.20, using the least upper bound property of real numbers (Theorem 1.19) to prove that. However, the purpose of the Appendix is to prove the least upper bound property of real numbers. So, to avoid circular reasoning, we will prove now the Archimedean property for rational numbers. The proof of that depends on the Archimedean property for integers, which in turn depends on the Well Ordering Principle.

Well Ordering Principle

Every set of positive integers has a least element.

Some texts prove this by induction or using basic principles of integers. We will accept the statement as fact.

Archimedean Property for Integers

If a and b are integers and $a > 0$, there exists an integer $n > 0$ such that $b \leq na$.

Proof: Assume the contrary: $na < b$ for every integer $n > 0$. $\therefore$ The set $S = \{b - na :$ n a positive integer$\}$ consists of all positive integers, and so has a least element using the Well Ordering Principle. Call this element $b - ma$, where m is some positive integer, $m \geq 1$. Since $m+1 > m$, then $m+1$ is a positive integer, so $b-(m+1) \in S$. $\therefore b - ma \leq b - (m + 1)a \Rightarrow a \leq 0$, a contradiction to the assumption of $a > 0$.

Archimedean Property for Q

If $p, q \in Q$ and $q > 0$, then there is a positive integer $n > 0$ such that $p \leq nq$.

Proof: Let $p = r/s, q = a/b$, where r, s, a, b are integers, and for simplicity, we can assume $s > 0, b > 0$.

(a) If $p = q$, choose $n = 1$. $\therefore p \leq nq$.

(b) If $p < q$, choose $n = 1$. $\therefore p \leq nq$.

(c) If $q < p$, then $a/b < r/s \Rightarrow as < br$. Since $q > 0$, then $a/b > 0$, and since $b > 0$, then $a > 0$. Since $s > 0$, then $0 < as$. Using the Archimedean Property for Integers, there is an integer $n > 0$ such that $br \leq n(as)$. $\therefore r/s \leq n(a/b)$ since $s > 0, b > 0$. $\therefore p \leq nq$.

Now, the statement in Rudin's proof of $0^* \subset \alpha + \beta$ that needs further clarification is:

For $\alpha \in R$ and $w > 0, w \in Q$, there is an integer n such that $nw \in \alpha$ and $(n+1)w \notin \alpha$.

Proof: (i) $w \in \alpha$

Since $\alpha \neq Q$, pick $z \notin \alpha$. Using the Archimedean Property, there is an integer $m > 0$ such that $z < mw$. $\therefore mw \notin \alpha$. From the finite set $S = \{1, 2, \ldots, m\}$, choose the largest integer $n \in S$ such that $nw \in \alpha$. Then $(n+1)w \notin \alpha$. Such an n exists since for $n = 1, nw = w \in \alpha$ and for $n = m, z < nw \notin \alpha$.

(ii) $w \notin \alpha$

Since $\alpha \neq \emptyset$, pick $z \in \alpha$. Note $z < w$ using implication (1) of Step 1.

If $z \geq 0$, then $0 \in \alpha$, so choose $n = 0$ so that $0 = nw \in \alpha$ and $w = (n+1)w \notin \alpha$.

If $z < 0$, then $0 < -z$. Using the Archimedean Property, there is a positive integer $m > 0$ such that $-z < mw$, so $(-m)w < z < (1)w$. Since $z \in \alpha$ then $(-m)z \in \alpha$. From the finite set $S = \{-m, -m+1, \ldots, 0, 1\}$, choose $n \in S$ to be the largest integer such that $nw \in \alpha$, and so $(n+1)w \notin \alpha$.

In Rudin's proof, note that $nw + p = nw - (n+2)w = -2w = v \in 0^*$.

Step 5

If $\alpha, \beta, \gamma \in R$ and $\beta < \gamma$, then $\alpha + \beta < \alpha + \gamma$.

Proof: Let $p \in \alpha + \beta$. $\therefore \exists a \in \alpha$ and $b \in \beta$ such that $p = a + b$. Since $\beta < \gamma$, by definition, $b \in \gamma$ since $\beta \subset \gamma$. $\therefore a \in \alpha$ and $b \in \gamma \Rightarrow p = a + b \in \alpha + \gamma$. $\therefore \alpha + \beta \subset \alpha + \gamma$. Rudin clearly shows $\alpha + \beta = \alpha + \gamma$ is not a possibility, so $\alpha + \beta$ is a proper subset of $\alpha + \gamma$, which means $\alpha + \beta < \alpha + \gamma$.

$0^* < \alpha \iff -\alpha < 0^*$ and $0^* > \alpha \iff -\alpha > 0^*$

Proof: $0^* < \alpha \Rightarrow (-\alpha) + 0^* < (-\alpha) + \alpha \Rightarrow -\alpha < 0^*$, using (A5), (A4), and the above statement. Likewise, $-\alpha < 0^* \Rightarrow \alpha + (-\alpha) < \alpha + 0^* \Rightarrow 0^* < \alpha$.

$0^* > \alpha \Rightarrow (-\alpha) + 0^* > (-\alpha) + \alpha \Rightarrow -\alpha > 0^*$, using (A5), (A4), and the above statement. Likewise, $-\alpha > 0^* \Rightarrow \alpha + (-\alpha) > \alpha + 0^* \Rightarrow 0^* > \alpha$.

Step 6

The proofs for (M1) through (M5) and (D) are provided below for completeness.

Note that $\alpha \in R^+$ means there is an $r \in Q, r > 0$ such that $r \in \alpha$.

(M1) $\alpha \in R^+, \beta \in R^+ \Rightarrow \alpha\beta \in R^+$

Must show $\alpha\beta$ is a cut as defined and then a member of R^+.

(I) $\alpha\beta \neq \emptyset$, since $\alpha \neq \emptyset$ and $\beta \neq \emptyset$. $\therefore$ If $r \in \alpha, s \in \beta$ with $r > 0, s > 0$, by definition, $rs \in \alpha\beta$ as $rs \leq rs$. Note that $0 < rs$ so that $0^* < \alpha\beta$.

$\alpha\beta \neq Q$: There exists $r', s' \in Q$ such that $r' \notin \alpha, s' \notin \beta$. $\therefore$ For all $r \in \alpha$ such that $r > 0$, $0 < r < r'$, and for all $s \in \beta$ such that $s > 0$, $0 < s < s'$. $\therefore 0 < rs < r's' \Rightarrow r's' \notin \alpha\beta$.

(II) Let $p \in \alpha\beta, q \in Q$, and $q < p$. $\therefore \exists r \in \alpha, s \in \beta$ such that $r > 0, s > 0$ and $p \leq rs$. $\therefore q < rs \Rightarrow q \in \alpha\beta$.

(III) Let $p \in \alpha\beta$. We need to find a p' such that $p < p'$ and $p' \in \alpha\beta$.

For p, there exists $r \in \alpha, s \in \beta, r > 0, s > 0$ such that $p \leq rs$. Since α is a cut, $\exists r' \in \alpha$ such that $0 < r < r'$. Similarly, $\exists s' \in \beta$ such that $0 < s < s'$. $\therefore 0 < rs < r's'$. Let $p' = r's'$. $\therefore p < p'$.

Now since $r' \in \alpha, s' \in \beta$, $\exists r'' \in \alpha$ such that $0 < r' < r''$. Similarly, $\exists s'' \in \beta$ such that $0 < s' < s''$. $\therefore 0 < p' = r's' < r''s'' \Rightarrow p' \in \alpha\beta$.

Thus, for any $p \in \alpha\beta$ there is a p' such that $p < p'$ and $p' \in \alpha\beta$. So, (III) is satisfied.

(I) showed that $0^* < \alpha\beta$ for $\alpha \in R^+, \beta \in R^+$. Thus $\alpha\beta$ is a cut and a member of R^+, so the second requirement of Definition 1.17 holds: If $\alpha > 0^*$ and $\beta > 0^*$ then $\alpha\beta > 0^*$.

(M2) $\alpha\beta = \beta\alpha$.

Must show $\alpha\beta \subset \beta\alpha$ and $\beta\alpha \subset \alpha\beta$.

(i) $\alpha\beta \subset \beta\alpha$: Let $p \in \alpha\beta$. $\therefore p \leq rs$ for some $r \in \alpha, s \in \beta, 0 < r, 0 < s$. Since $rs = sr$, then $p \leq sr \Rightarrow p \in \beta\alpha$.

(ii) $\beta\alpha \subset \alpha\beta$: Let $p \in \beta\alpha$. $\therefore p \leq sr$ for some $s \in \beta, r \in \alpha, 0 < s, 0 < r$. Since $sr = rs$, then $p \leq rs \Rightarrow p \in \alpha\beta$.

(M3) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$

Must show $\alpha(\beta\gamma) \subset (\alpha\beta)\gamma$ and $(\alpha\beta)\gamma \subset \alpha(\beta\gamma)$.

(i) $\alpha(\beta\gamma) \subset (\alpha\beta)\gamma$: Let $p \in \alpha(\beta\gamma)$. $\therefore p \leq rs'$ for some $r \in \alpha, s' \in \beta\gamma, 0 < r, 0 < s'$.

$s' \in \beta\gamma \Rightarrow \exists s \in \beta, t \in \gamma, 0 < s, 0 < t$, and $0 < s' \leq st \Rightarrow p \leq rs' \leq r(st)$.

Since $r(st) = (rs)t$, then $p \leq (rs)t$. Define $r' = rs$ so that $0 < r'$. Thus, $r' \in \alpha\beta$. $\therefore p \leq r't \Rightarrow p \in (\alpha\beta)\gamma$.

(ii) $(\alpha\beta)\gamma \subset \alpha(\beta\gamma)$: Let $p \in (\alpha\beta)\gamma$. $\therefore p \leq r't$ for some $r' \in \alpha\beta, t \in \gamma, 0 < r', 0 < t$.

$r' \in \alpha\beta \Rightarrow \exists r \in \alpha, s \in \beta, 0 < r, 0 < s$, and $0 < r' \leq rs \Rightarrow p \leq r't \leq (rs)t$.

Since $(rs)t = r(st)$, then $p \leq r(st)$. Define $s' = st$ so that $0 < s'$. Thus, $s' \in \beta\gamma$. $\therefore p \leq rs' \Rightarrow p \in \alpha(\beta\gamma)$.

(M4) $1^* \in R^+, 1^* \neq 0^*$ and $1^*\alpha = \alpha$ for every $\alpha \in R^+$.

Since $1/2 \in 1^*$ and $1/2 \notin 0^*$, then $1^* \neq 0^*$ and in fact $0^* \subset 1^* \Rightarrow 0^* < 1^*$.

(i) $1^*\alpha \subset \alpha$

Let $p \in 1^*\alpha$. $\therefore p \leq rs$ for some $r \in 1^*, s \in \alpha, 0 < r < 1, 0 < s$. $\therefore rs < s \Rightarrow p < s \Rightarrow p \in \alpha$.

(ii) $\alpha \subset 1^*\alpha$

Let $p \in \alpha$.

Suppose $p \leq 0$. By definition of $1^*, \frac{1}{2} \in 1^*$. Since $\alpha \in R^+, \exists r \in \alpha$ such that $0 < r$. Since $0 < \frac{1}{2}r$, we have $p < \frac{1}{2}r \Rightarrow p \in 1^*\alpha$.

Suppose $p > 0$. Since $p \in \alpha$ and $\alpha \in R^+$, there exists a $p' \in \alpha$ such that $0 < p < p'$. Thus, $0 < \frac{p}{p'} < 1 \Rightarrow \frac{p}{p'} \in 1^*$. $\therefore p = (\frac{p}{p'})p' \in 1^*\alpha$.

Thus, (i) and (ii) show $1^*\alpha = \alpha$.

(M5) For every $\alpha \in R^+, \alpha \neq 0^*$, there is an element $\beta \in R^+$ such that $\alpha\beta = 1^*$.

For $\alpha = 1^*$, $\beta = 1^*$, since by (M4), $1^*1^* = 1^*$, so we can exclude $\alpha = 1^*$ in the below proofs.

Using Step 4 and Rudin's definition for an additive inverse cut as a template, we use the following definition for a multiplicative inverse cut.

To understand the intuition for the following definition, take a concrete example. Let $\alpha = \{a \in Q, a < 3\}, \beta = \{b \in Q, b < \frac{1}{3}\}$. Ignoring the negative numbers, multiplying the positive numbers from each cut gives us $\{c \in Q, 0 < c < 1\}$. We can add $c \leq 0$ to make it the cut 1^*. Note that the reciprocal of the positive members in β are those numbers greater than 3, which is the "upper" cut using 3 as the boundary (i.e., all numbers not in α). Upper cuts have no smallest number (like no largest number for lower cuts). Thus, we have a criterion showing we can "squeeze" in a number and still stay above the boundary of 3. Dividing the reciprocal of a possible positive number for β by r with $r > 1$ assures a resulting smaller number, so if this resulting smaller number is still above the boundary of 3 (i.e., still not in α), then the original number must be less than $\frac{1}{3}$ (i.e., in β).

Definition: Fix $\alpha \in R^+$ and let $\beta = \alpha^{-1}$ be the set of all $p \in Q$ with the following properties:

(1) If $p \leq 0$ then $p \in \beta$.

(2) If $p > 0$ and there exists an $r \in Q$ such that $r > 1$ and $\dfrac{1}{p} \cdot \dfrac{1}{r} \notin \alpha$, then $p \in \beta$.

We need to show $\beta \in R^+$ and $\alpha\beta = 1^*$.

(a) $\beta \in R^+$

(I) If $1^* < \alpha$, let $s \notin \alpha$ so that $1 < s$. Let $p = \dfrac{1}{2s}$ and let $r = 2$, so $p > 0$.

$\therefore \dfrac{1}{p} \cdot \dfrac{1}{r} = 2s \cdot \dfrac{1}{2} = s \notin \alpha$. By (2) in the definition, $p \in \beta$ (and $p > 0$), so $\beta \neq \emptyset$.

If $\alpha < 1^*$, let $p \in 1^*$ and $p \notin \alpha$ (α is a proper subset of 1^*). Note $1 \notin \alpha$.

$\therefore 0 < p < 1 \Rightarrow 1 < \dfrac{1}{p}$. Let $r = \dfrac{1}{p} \Rightarrow r > 1$. $\therefore \dfrac{1}{p} \cdot \dfrac{1}{r} = \dfrac{1}{p} \cdot p = 1 \notin \alpha$.

By (2) in the definition, $p \in \beta$ (and $p > 0$), so $\beta \neq \emptyset$.

If $q \in \alpha$ and $q > 0$, then $1/q \notin \beta$, for if $1/q \in \beta$, then there is an $r > 1$ such that $\dfrac{1}{1/q} \cdot \dfrac{1}{r} = \dfrac{q}{r} \notin \alpha$. But $r > 1 \Rightarrow \dfrac{q}{r} < q \Rightarrow \dfrac{q}{r} \in \alpha$, a contradiction.

$\therefore 1/q \notin \beta$, so $\beta \neq Q$.

$\therefore \beta \neq \emptyset$ and $\beta \neq Q$ so (I) is satisfied.

(II) Let $p \in \beta$ and suppose $q \in Q$ is such that $q < p$.

If $q \leq 0$ then by (1) in the Definition, $q \in \beta$.

If $0 < q < p$, then by (2) in the Definition, there is an $r > 1$ such that $\dfrac{1}{p} \cdot \dfrac{1}{r} \notin \alpha$.

Also, $\dfrac{1}{p} < \dfrac{1}{q} \Rightarrow \dfrac{1}{p} \cdot \dfrac{1}{r} < \dfrac{1}{q} \cdot \dfrac{1}{r}$. Since $\dfrac{1}{p} \cdot \dfrac{1}{r} \notin \alpha$ then $\dfrac{1}{q} \cdot \dfrac{1}{r} \notin \alpha \Rightarrow q \in \beta$.

(III) Need to show that if $p \in \beta, \exists q \in \beta$ such that $p < q$.

Let $p \in \beta$ such that $p > 0$ by (I) above. $\therefore$ There is an $r > 1$ such that $\dfrac{1}{p} \cdot \dfrac{1}{r} \notin \alpha$.

We need to find some $r' > 1$ so that $q = pr'$, which will give $p < q$, and some factor $x > 1$ so that $\dfrac{1}{pr'} \cdot \dfrac{1}{x} = \dfrac{1}{p} \cdot \dfrac{1}{r}$, which will mean $pr' \in \beta$ by our Definition. Thus, we want $r'x = r$ and $x > 1$. Thus, we need an $r' > 1$ such that $r/r' > 1$, which means $r > r' > 1$.

$\therefore$ Let $r' = \dfrac{r+1}{2}$. This satisfies $r > r' > 1$. $\therefore x = r/r' = \dfrac{2r}{r+1} > 1$.

In summary, given $r > 1$ from $p \in \beta$, define $r' = \left(\dfrac{r+1}{2}\right)$. This $r' > 1$ since $\left(\dfrac{r+1}{2}\right) > 1$. $\therefore$ Let $q = r'p$, so that $q > p$. Also, since $r/r' > 1$, then

$$\frac{1}{q} \cdot \frac{1}{r/r'} = \frac{1}{pr'} \cdot \frac{1}{r/r'} = \frac{1}{p} \cdot \frac{1}{r} \notin \alpha$$

Thus, $q \in \beta$ as it satisfies our Definition for β above, and so (III) is satisfied.

Thus, with (I),(II),(III) satisfied and (I) showing $\beta > 0^*$, then $\beta \in R^+$.

(b) $\alpha\beta \subset 1^*$

Let $p \in \alpha\beta$. If $p < 0$ then $p \in 1^*$.

Assume $p > 0$. Then $p \leq ab$ for some $a > 0, a \in \alpha, b > 0, b \in \beta$.

But $b \in \beta \Rightarrow \exists r > 1$ such that $\dfrac{1}{b} \cdot \dfrac{1}{r} \notin \alpha$. $\therefore$ Since $a \in \alpha, a < \dfrac{1}{b} \cdot \dfrac{1}{r} \Rightarrow ab < \dfrac{1}{r} \Rightarrow ab \in 1^*$ since $\dfrac{1}{r} < 1$. Since $p \leq ab$, then $p \in 1^*$.

$\therefore p \in \alpha\beta \Rightarrow p \in 1^*$.

(c) $1^* \subset \alpha\beta$

This is a lot harder to prove. Let $p \in 1^*$. If $p \leq 0$ then $p \in \alpha\beta$.

What we will try to do is find an $x \in \alpha$ and a $p/x \in \beta$ so that $p = (x)(p/x)$.

Assume $p > 0$. $\therefore 0 < p < 1 \Rightarrow 0 < 1 - p < 1$.

Since $\alpha \in R^+$, let $a \in \alpha$ such that $0 < a$. $\therefore 0 < a(1-p) < a$. Also, let $z \in Q$ such that $z \notin \alpha$. Therefore, we have

$$0 < a(1-p) < a < z \qquad [1]$$

Using the Archimedean Property for Q proved above in (A5)(3), there is an integer $n > 0$ such that $z < n[a(1-p)]$. From the finite set $\{1, 2, \ldots, n\}$, choose the largest integer m such that $m[a(1-p)] \in \alpha$. Such an m exists since for $m = 1$, $m[a(1-p)] \in \alpha$ as we can see from equation [1] since $a(1-p) < a$. $\therefore (m+1)[a(1-p)] \notin \alpha$.

$$\begin{aligned} \therefore (m+1)[a(1-p)] &= a(1-p) + m[a(1-p)] \notin \alpha \\ \text{Let } a_1 &= m[a(1-p)], \qquad a_1 \in \alpha \\ b &= a_1 + a(1-p), \qquad b \notin \alpha \qquad [2] \end{aligned}$$

Note from equation [2], $b - a_1 = a(1-p)$.

Let $a_2 = \max\{a, a_1\}$, so $a_2 \in \alpha$. Also, $a_1 \leq a_2$ so $-a_2 \leq -a_1 \Rightarrow b - a_2 \leq b - a_1$.

$\therefore b - a_2 \leq a(1-p)$. Since $0 < a < b$, then $a(1-p) < b(1-p)$, as $0 < 1 - p$.

Thus $b - a_2 < b(1-p)$, so

$$\begin{aligned} b - a_2 + pb &< b(1-p) + pb \Rightarrow \\ b - a_2 + pb &< b \Rightarrow \\ pb &< a_2 \Rightarrow \\ 1 &< \frac{a_2}{pb} \qquad [3] \end{aligned}$$

Noting that $p = a_2(p/a_2)$ and $a_2 \in \alpha$, can we demonstrate that $p/a_2 \in \beta$? Indeed, it is as $b = \dfrac{1}{p/a_2} \cdot \dfrac{1}{a_2/pb}$ and $b \notin \alpha$. That is, we found an $r > 1$ by using $r = \dfrac{a_2}{pb}$ from equation [3], so that $\dfrac{1}{p/a_2} \cdot \dfrac{1}{r} \notin \alpha$. From the Definition of β, $p/a_2 \in \beta$.

$\therefore p = a_2(\dfrac{p}{a_2})$, where $a_2 \in \alpha, \dfrac{p}{a_2} \in \beta$. $\therefore p \in 1^* \Rightarrow p \in \alpha\beta$.

(b),(c) mean $\alpha\beta = 1^*$ and this completes the proof of (M5).

(D) The Distributive Law

Let $\alpha, \beta, \gamma \in R^+$. Then $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

We need the following lemma because so far multiplication has only been established for R^+, and the proofs below depend on properties of addition.

Lemma: If $\alpha \in R^+, \beta \in R^+$, then $\alpha + \beta \in R^+$

Proof: (A1) showed that $\alpha + \beta$ is a cut. Let $a \in \alpha, b \in \beta, a > 0, b > 0$. $\therefore 0 < a + b \in \alpha + \beta$. $\therefore \alpha + \beta \neq 0^*$ and it can't be true that $\alpha + \beta < 0^*$. Thus $\alpha + \beta > 0^* \Rightarrow \alpha + \beta \in R^+$.

(1) $\alpha(\beta + \gamma) \subset \alpha\beta + \alpha\gamma$

Let $p \in \alpha(\beta + \gamma)$. Then there exists $a \in \alpha, z \in \beta + \gamma, a > 0, z > 0$, such that $p \leq az$.

However, $z \in \beta + \gamma \Rightarrow \exists b \in \beta, c \in \gamma$ such that $z = b + c$. Since $\beta \in R^+, \gamma \in R^+$, let $b' \in \beta, c' \in \gamma, b' > 0, c' > 0$ such that $b < b', c < c'$. $\therefore z = b + c < b' + c'$. Note that $0 < b' + c' \in \beta + \gamma$.

$\therefore p \leq az \Rightarrow p \leq a(b + c) < a(b' + c') = ab' + ac'$. But since $0 < ab' \leq ab'$ and $0 < ac' \leq ac'$, then $ab' \in \alpha\beta$ and $ac' \in \alpha\gamma$. So $ab' + ac' \in \alpha\beta + \alpha\gamma$.

$\therefore p < ab' + ac' \Rightarrow p \in \alpha(\beta + \gamma)$.

(2) $\alpha\beta + \alpha\gamma \subset \alpha(\beta + \gamma)$

Let $p \in \alpha\beta + \alpha\gamma$. Then there exists $v \in \alpha\beta, w \in \alpha\gamma$ such that $p = v + w$.

$v \in \alpha\beta$ and $\alpha\beta \in R^+ \Rightarrow \exists r \in \alpha, s \in \beta, 0 < r, 0 < s$ such that $v \leq rs$.

$w \in \alpha\gamma$ and $\alpha\gamma \in R^+ \Rightarrow \exists x \in \alpha, y \in \gamma, 0 < x, 0 < y$ such that $w \leq xy$.

$\therefore v + w \leq rs + xy$. Let $a = \max\{r, x\}$. $\therefore 0 < a \in \alpha$ and $rs + xy \leq as + ay$.

$\therefore p = v + w \leq rs + xy \leq as + ay = a(s + y)$. $\therefore p \leq a(s + y)$ and note $0 < s + y \in \beta + \gamma$, and $\beta + \gamma \in R^+$. Since $0 < a$ and $a(s + y) \leq a(s + y)$, then $a(s + y) \in \alpha(\beta + \gamma)$.

$\therefore p \leq a(s + y) \Rightarrow p \in \alpha(\beta + \gamma)$.

$(1), (2) \Rightarrow \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Step 7

Since $0^* \notin R^+$, multiplying 0^* with α has so far been undefined, and so $\alpha 0^* = 0^*\alpha = 0^*$ is needed at this point. Note $0^* \in R$.

Proofs of (M1) - (M5) and (D) are now given for all cuts in R, using Rudin's definition for negative cuts. Extensive use of Proposition 1.14 is made with all its consequences, such as $x = y \iff -x = -y$ and $-x - y = -(x + y)$, for $x, y \in F$, a field. Use is also made of, from 1.14(d) and Step 5, $\alpha < 0^* \iff (-\alpha) > 0^*$.

(M1) If $\alpha \in R$ and $\beta \in R$, then $\alpha\beta \in R$.

Step 6 already showed this for $\alpha > 0^*, \beta > 0^*$.

(1) $\alpha < 0^*, \beta > 0^*$

By definition, $\alpha\beta = -[(-\alpha)\beta]$.

But $(-\alpha) > 0^*$ so $(-\alpha)\beta \in R^+ \subset R \Rightarrow (-\alpha)\beta \in R$. By (A5), $-[(-\alpha)\beta] \in R$.

$\therefore \alpha\beta \in R$.

(2) $\alpha < 0^*, \beta < 0^*$

By definition, $\alpha\beta = (-\alpha)(-\beta)$. But $(-\alpha) \in R^+, (-\beta) \in R^+ \Rightarrow (-\alpha)(-\beta) \in R^+$.

$\therefore \alpha\beta \in R^+ \subset R \Rightarrow \alpha\beta \in R$.

(3) $\alpha > 0^*, \beta < 0^*$

By definition, $\alpha\beta = -[\alpha(-\beta)]$.

But $(-\beta) > 0^* \Rightarrow \alpha(-\beta) \in R^+ \subset R \Rightarrow \alpha(-\beta) \in R$. By (A5), $-[\alpha(-\beta)] \in R$.

$\therefore \alpha\beta \in R$.

(4) If $\alpha = 0^*$ or $\beta = 0^*$ then $\alpha\beta = 0^* \in R$ by definition.

(M2) If $\alpha \in R, \beta \in R$, then $\alpha\beta = \beta\alpha$.

Step 6 already showed this for $\alpha > 0^*, \beta > 0^*$. We use below the result from Step 5: $\alpha < 0^* \iff (-\alpha) > 0^*$.

(1) If $\alpha = 0^*$ or $\beta = 0^*$, then $\alpha\beta = \beta\alpha = 0^*$.

(2) $\alpha < 0^*, \beta > 0^*$

By definition, $\alpha\beta = -[(-\alpha)\beta]$.

But $(-\alpha) > 0^* \Rightarrow (-\alpha)\beta = \beta(-\alpha)$ using (M2) for $(-\alpha) \in R^+, \beta \in R^+$.

$\therefore \alpha\beta = -[(-\alpha)\beta] = -[\beta(-\alpha)]$. But by definition, $\beta\alpha = -[\beta(-\alpha)]$.

$\therefore \alpha\beta = \beta\alpha$.

(3) $\alpha < 0^*, \beta < 0^*$

By definition, $\alpha\beta = (-\alpha)(-\beta)$.

But $(-\alpha)(-\beta) = (-\beta)(-\alpha)$ using (M2) for $(-\alpha) \in R^+, (-\beta) \in R^+$.

$\therefore \alpha\beta = (-\alpha)(-\beta) = (-\beta)(-\alpha)$. But by definition, $\beta\alpha = (-\beta)(-\alpha)$.

$\therefore \alpha\beta = \beta\alpha$.

(4) $\alpha > 0^*, \beta < 0^*$

By definition, $\alpha\beta = -[\alpha(-\beta)]$.

But $(-\beta) > 0^* \Rightarrow \alpha(-\beta) = (-\beta)\alpha$ using (M2) for $\alpha \in R^+, (-\beta) \in R^+$.

$\therefore \alpha\beta = -[\alpha(-\beta)] = -[(-\beta)\alpha]$. But by definition, $\beta\alpha = -[(-\beta)\alpha]$.

$\therefore \alpha\beta = \beta\alpha$.

(M3) If $\alpha, \beta, \gamma \in R$, then $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Step 6 already showed this for $\alpha > 0^*, \beta > 0^*$.

In several of the steps below, we make use of Proposition 1.14 and its consequences, such as $x = y \iff -x = -y$ when $x, y \in F$, F a field. It is tempting to use 1.16(c) in which, for $x, y \in F$, $(-x)y = -(xy) = x(-y)$. However, examination of Rudin's proof of 1.16(c) shows that it depends on the distributive property for R, which we have not proved yet (only for R^+ so far in Step 6). Thus, to avoid circular reasoning, we prove

the following Lemma, which is the equivalent to 1.16(c), and only depends on properties proved so far. Note, from this Lemma, as in Rudin, we can state $(-x)(-y) = xy$ for R. For ease, in this Lemma x and y represent cuts in R. Note (M1) of Step 7 states $xy, (-x)y, x(-y), -(xy), (-x)(-y)$ are all cuts in R.

Lemma For $x, y \in R, (-x)y = -(xy) = x(-y)$.

(a) $x = 0^*$ or $y = 0^*$

First we prove $0^* = -0^*$.

$$\begin{aligned} -0^* + 0^* &= -0^* && \text{using (A4)} \\ 0^* + (-0^*) &= 0^* && \text{using (A5)} \\ -0^* + 0^* &= 0^* + (-0^*) && \text{using (A2)} \\ \therefore 0^* &= -0^* \end{aligned}$$

If $x = 0^*, (-x)y = (-0^*)y = 0^*y = 0^* = -0^* = -(0^*y) = -(xy)$ and $x(-y) = 0^*(-y) = 0^*$. $\therefore 0^* = (-x)y = -(xy) = x(-y)$.

If $y = 0^*, (-x)y = (-x)0^* = 0^* = -0^* = -(x0^*) = -(xy)$ and $x(-y) = x(-0^*) = x0^* = 0^*$. $\therefore 0^* = (-x)y = -(xy) = x(-y)$.

(b) $x > 0^*, y > 0^*$

Note $-x < 0^*, -y < 0^*$.

$$\begin{aligned} (-x)y &= -[(-(-x))y] && \text{Rudin definition of multiplication} \\ &= -[xy] && \text{1.14(d) stating } -(-x) = x \\ x(-y) &= -[x[-(-y)]] && \text{Rudin definition of multiplication} \\ &= -[xy] && \text{1.14(d) stating } -(-y) = y \end{aligned}$$

$\therefore (-x)y = -(xy) = x(-y)$.

(c) $x > 0^*, y < 0^*$

$$\begin{aligned} xy &= -[x(-y)] && \text{Rudin definition of multiplication} \\ \therefore -(xy) &= x(-y) && w = v \iff -w = -v \text{ and } 1.14(d) \\ x > 0^* &\Rightarrow -x < 0^* && \text{Step 5} \\ \therefore (-x)y &= [-(-x)](-y) && \text{Rudin definition of multiplication} \\ &= x(-y) && \text{1.14(d)} \end{aligned}$$

$\therefore (-x)y = -(xy) = x(-y)$.

(d) $x < 0^*, y > 0^*$

$$\begin{aligned} y > 0^* &\Rightarrow -y < 0^* && \text{Step 5} \\ x(-y) &= (-x)[-(-y)] && \text{Rudin definition of multiplication} \\ &= (-x)y && \text{1.14(d)} \\ xy &= -[(-x)y] && \text{Rudin definition of multiplication} \\ -(xy) &= (-x)y && w = v \iff -w = -v \text{ and } 1.14(d) \end{aligned}$$

$\therefore (-x)y = -(xy) = x(-y)$.

(e) $x < 0^*, y < 0^*$

$$\begin{aligned}
x < 0^* &\Rightarrow -x > 0^* && \text{Step 5}\\
(-x)y &= -[(-x)(-y)] && \text{Rudin definition of multiplication}\\
y < 0^* &\Rightarrow -y > 0^* && \text{Step 5}\\
x(-y) &= -[(-x)(-y)] && \text{Rudin definition of multiplication}\\
xy &= (-x)(-y) && \text{Rudin definition of multiplication}\\
-(xy) &= -[(-x)(-y)] && w = v \iff -w = -v
\end{aligned}$$

$\therefore (-x)y = -(xy) = x(-y) = -[(-x)(-y)]$.

For all cases, $(-x)y = -(xy) = x(-y)$ has been proved without using the distributive property.

Now to prove (M3) for R.

(1) $\alpha = 0^*$ or $\beta = 0^*$ or $\gamma = 0^*$.

If $\alpha = 0^*$ then $\alpha\beta = 0^*$, so $(\alpha\beta)\gamma = 0^*\gamma = 0^*$, and $\alpha(\beta\gamma) = 0^*(\beta\gamma) = 0^*$. Therefore, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

If $\beta = 0^*$ then $\alpha\beta = 0^*$, so $(\alpha\beta)\gamma = 0^*\gamma = 0^*$, and $\beta\gamma = 0^*$, so $\alpha(\beta\gamma) = \alpha 0^* = 0^*$. Thus, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

If $\gamma = 0^*$ then $(\alpha\beta)\gamma = (\alpha\beta)0^* = 0^*$, and $\beta\gamma = 0^*$ so $\alpha(\beta\gamma) = \alpha 0^* = 0^*$. Therefore, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

(2) $\alpha > 0^*, \beta < 0^*, \gamma > 0^*$

By definition, $\alpha\beta = -[\alpha(-\beta)]$, so $-(\alpha\beta) = \alpha(-\beta) > 0^*$. By (M1) in Step 7, $\alpha\beta \in R$, and since $\gamma \in R$, then $(\alpha\beta)\gamma \in R$. Therefore,

$$\begin{aligned}
-[(\alpha\beta)\gamma] &= -(\alpha\beta)\gamma && \text{using the Lemma: } -[(x)y] = (-x)y\\
&= (\alpha(-\beta))\gamma && \text{using the Lemma: } -(xy) = x(-y)\\
&= \alpha[(-\beta)\gamma] && \text{using (M3) for } \alpha, (-\beta), \gamma \in R^+\\
&= \alpha[-(\beta\gamma)] && \text{using the Lemma: } (-x)y = -(xy)\\
&= -[\alpha(\beta\gamma)] && \text{using the Lemma: } x(-y) = -(xy)
\end{aligned}$$

Since $-[(\alpha\beta)\gamma] = -[\alpha(\beta\gamma)]$ then $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

(3) $\alpha < 0^*, \beta > 0^*, \gamma > 0^*$

By definition, $\alpha\beta = -[(-\alpha)\beta]$, so $-(\alpha\beta) = (-\alpha)\beta > 0^*$. By (M1) in Step 7, $\alpha\beta \in R$, and since $\gamma \in R$, then $(\alpha\beta)\gamma \in R$. Therefore,

$$\begin{aligned}
-[(\alpha\beta)\gamma] &= -(\alpha\beta)\gamma && \text{using the Lemma: } -[(x)y] = (-x)y\\
&= ((-\alpha)\beta)\gamma && \text{using the Lemma: } -(xy) = (-x)y\\
&= (-\alpha)(\beta\gamma) && \text{using (M3) for } (-\alpha), \beta, \gamma \in R^+\\
&= -[\alpha(\beta\gamma)] && \text{using the Lemma: } (-x)y = -(xy)
\end{aligned}$$

Since $-[(\alpha\beta)\gamma] = -[\alpha(\beta\gamma)]$ then $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

(4) $\alpha < 0^*, \beta < 0^*, \gamma > 0^*$

By definition, $\alpha\beta = (-\alpha)(-\beta)$. By (M1) in Step 7, $\alpha\beta \in R$, and since $\gamma \in R$, then $(\alpha\beta)\gamma \in R$. Therefore,

$$\begin{aligned}
(\alpha\beta)\gamma &= [(-\alpha)(-\beta)]\gamma \\
&= (-\alpha)[(-\beta)\gamma] && \text{using (M3) for } (-\alpha), (-\beta), \gamma \in R^+ \\
&= (-\alpha)[-(\beta\gamma)] && \text{using the Lemma: } (-x)y = -(xy) \\
&= -[(-\alpha)(\beta\gamma)] && \text{using the Lemma: } x(-y) = -(xy) \\
&= -[-[\alpha(\beta\gamma)]] && \text{using the Lemma: } (-x)y = -(xy) \\
&= \alpha(\beta\gamma) && \text{using 1.14(d) } -[-x] = x
\end{aligned}$$

(5) $\gamma < 0^*$

If $\gamma < 0^*$ then $(-\gamma) > 0^*$. By (M1) in Step 7, $\beta\gamma \in R$, and since $\gamma \in R$, then $\alpha(\beta\gamma) \in R$.

$$\begin{aligned}
-[\alpha(\beta\gamma)] &= \alpha[-(\beta\gamma)] && \text{using the Lemma: } -(xy) = x(-y) \\
&= \alpha[\beta(-\gamma)] && \text{using the Lemma: } -(xy) = x(-y) \\
&= [\alpha\beta](-\gamma) && \text{using (1),(2),(3),(4) above for } \alpha, \beta \in R, (-\gamma) \in R^+ \\
&= -[(\alpha\beta)\gamma] && \text{using the Lemma: } x(-y) = -(xy)
\end{aligned}$$

Since $-[(\alpha\beta)\gamma] = -[\alpha(\beta\gamma)]$ then $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

(1) $\rightarrow$ (5) means for all cases, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

(M4) If $\alpha \in R$, then $1^*\alpha = \alpha$.

If $\alpha = 0^*$, then by definition, $1^*\alpha = 0^* = \alpha$.

If $\alpha < 0^*$, then $(-\alpha) > 0^*$, so $1^*(-\alpha) = -\alpha$, using (M4) in Step 6. Using the Lemma in (M3) above, since $1^* \in R, (-\alpha) \in R$, then $1^*(-\alpha) \in R$, so $1^*(-\alpha) = -(1^*\alpha)$. Therefore $-(1^*\alpha) = -\alpha \Rightarrow 1^*\alpha = \alpha$.

$1^*\alpha = \alpha$ was already proved for $\alpha > 0^*$ in (M4) of Step 6.

(M5) If $\alpha \in R$ and $\alpha \neq 0^*$, then there exists an element $\gamma \in R$ such that $\alpha\gamma = 1^*$.

This was already proved for $\alpha > 0^*$ in Step 6. $\therefore$ Suppose $\alpha < 0^*$. Then $-\alpha > 0^*$.

$\therefore$ There exists a $\beta \in R^+$ such that $(-\alpha)\beta = 1^*$. Since $R^+ \subset R$, then $\beta \in R$, and so by (A5), $-\beta \in R$. By (M1) above in Step 7, $\alpha(-\beta) \in R$, and by the Lemma in (M3) above, $(-\alpha)\beta = \alpha(-\beta)$. $\therefore \alpha(-\beta) = 1^*$. $\therefore$ Letting $\gamma = -\beta$, then there exists a $\gamma \in R$ such that $\alpha\gamma = 1^*$.

(D) If $\alpha, \beta, \gamma \in R$, then $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

The field properties for addition, which were proved in Step 4, and their consequences, such as Proposition 1.14 in Rudin, are used multiple times in the proofs below. One such consequence that is used is $-x - y = -(x + y)$. Also, use is made of the Lemma proved above in (M3) of Step 7: $(-x)y = -(xy) = x(-y)$. We will also use the distributive property for R^+ proved in Step 6 when all three elements are positive.

(1) $\alpha = 0^*$ or $\beta = 0^*$ or $\gamma = 0^*$

(a) If $\alpha = 0^*$, then $\alpha(\beta + \gamma) = 0^*$ by definition. Similarly, $\alpha\beta = 0^*$ and $\alpha\gamma = 0^*$.
$\therefore \alpha(\beta + \gamma) = 0^* = 0^* + 0^* = \alpha\beta + \alpha\gamma$.

(b) If $\beta = 0^*$, then $\beta + \gamma = 0^* + \gamma = \gamma$. $\therefore \alpha(\beta + \gamma) = \alpha\gamma$.

$\alpha\beta = \alpha 0^* = 0^*$ by definition. $\therefore \alpha\beta + \alpha\gamma = 0^* + \alpha\gamma = \alpha\gamma$.

$\therefore \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma = \alpha\gamma$.

(c) If $\gamma = 0^*$, then $\beta + \gamma = \beta + 0^* = \beta$. $\therefore \alpha(\beta + \gamma) = \alpha\beta$.

$\alpha\gamma = \alpha 0^* = 0^*$. $\therefore \alpha\beta + \alpha\gamma = \alpha\beta + 0^* = \alpha\beta$.

$\therefore \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma = \alpha\beta$.

(2) $\alpha > 0^*$ or $\beta > 0^*$ or $\gamma > 0^*$

$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ was proved in Step 6 (D) for this case.

(3) $\alpha > 0^*, \beta < 0^*, \gamma > 0^*$

$\therefore -\beta > 0^*$.

(a) $\beta + \gamma = 0^*$

$\therefore \gamma = (-\beta)$

$$\begin{aligned} \alpha(\beta + \gamma) &= \alpha 0^* = 0^* && \text{by definition} \\ &= \alpha\beta + [-(\alpha\beta)] && \text{using (A5)} \\ &= \alpha\beta + \alpha(-\beta) && \text{using } -(xy) = x(-y) \\ \therefore \alpha(\beta + \gamma) &= \alpha\beta + \alpha\gamma && \text{since } \gamma = (-\beta) \end{aligned}$$

(b) $\beta + \gamma > 0^*$

$$\begin{aligned} \alpha\gamma &= \alpha(0^* + \gamma) && \text{using (A4)} \\ &= \alpha([(-\beta) + \beta] + \gamma) && \text{using (A5)} \\ &= \alpha((-\beta) + [\beta + \gamma]) && \text{using (A3)} \\ &= \alpha(-\beta) + \alpha(\beta + \gamma) && \text{using Step 6 (D) as } (-\beta) > 0^* \\ &= -(\alpha\beta) + \alpha(\beta + \gamma) && \text{using } x(-y) = -(xy) \\ \therefore \alpha\beta + \alpha\gamma &= \alpha\beta + [-(\alpha\beta) + \alpha(\beta + \gamma)] && x = y \Rightarrow z + x = z + y \\ &= [\alpha\beta + [-(\alpha\beta)]] + \alpha(\beta + \gamma) && \text{using (A3)} \\ &= 0^* + \alpha(\beta + \gamma) && \text{using (A5)} \\ \therefore \alpha\beta + \alpha\gamma &= \alpha(\beta + \gamma) && \text{using (A4)} \end{aligned}$$

(c) $\beta + \gamma < 0^*$

$\therefore -(\beta + \gamma) > 0^*$

$$\begin{aligned} -(\alpha\beta) &= \alpha(-\beta) && \text{using } -(xy) = x(-y) \\ &= \alpha[0^* + (-\beta)] && \text{using (A4)} \\ &= \alpha[[\gamma + (-\gamma)] + (-\beta)] && \text{using (A5)} \\ &= \alpha[\gamma + [(-\gamma) + (-\beta)]] && \text{using (A3)} \end{aligned}$$

$$\begin{aligned}
\therefore -(\alpha\beta) &= \alpha[\gamma + [(-\gamma) + (-\beta)]] \\
&= \alpha[\gamma + [-(\gamma + \beta)]] && \text{using } (-x) + (-y) = -(x+y) \\
&= \alpha[\gamma + [-(\beta + \gamma)]] && \text{using (A2)} \\
&= \alpha\gamma + \alpha[-(\beta + \gamma)] && \text{using Step 6 (D)} \\
&= \alpha\gamma - \alpha[(\beta + \gamma)] && \text{using } x(-y) = -(xy) \\
\therefore -(\alpha\beta) + \alpha[(\beta + \gamma)] &= [\alpha\gamma - \alpha[(\beta + \gamma)]] + \alpha[(\beta + \gamma)] && x = y \Rightarrow x + z = y + z \\
&= \alpha\gamma + [-\alpha[(\beta + \gamma)] + \alpha[(\beta + \gamma)]] && \text{using (A3)} \\
&= \alpha\gamma + 0^* && \text{using (A5)} \\
&= \alpha\gamma && \text{using (A4)}
\end{aligned}$$

$$\begin{aligned}
\therefore -(\alpha\beta) + \alpha[(\beta + \gamma)] &= \alpha\gamma \\
\alpha\beta + [-(\alpha\beta) + \alpha[(\beta + \gamma)]] &= \alpha\beta + \alpha\gamma && x = y \Rightarrow z + x = z + y \\
[\alpha\beta + [-(\alpha\beta)]] + \alpha[(\beta + \gamma)] &= \alpha\beta + \alpha\gamma && \text{using (A3)} \\
0^* + \alpha[(\beta + \gamma)] &= \alpha\beta + \alpha\gamma && \text{using (A5)} \\
\alpha[(\beta + \gamma)] &= \alpha\beta + \alpha\gamma && \text{using (A4)}
\end{aligned}$$

$\therefore$ For $\alpha > 0^*, \beta < 0^*, \gamma > 0^*$, $\alpha[(\beta + \gamma)] = \alpha\beta + \alpha\gamma$.

(4) $\alpha > 0^*, \beta > 0^*, \gamma < 0^*$

$$\begin{aligned}
\alpha(\gamma + \beta) &= \alpha\gamma + \alpha\beta && \text{using result of (3) above} \\
&= \alpha\beta + \alpha\gamma && \text{using (A2)}
\end{aligned}$$

(5) $\alpha > 0^*, \beta < 0^*, \gamma < 0^*$

$$\begin{aligned}
-\alpha(\beta + \gamma) &= \alpha[-(\beta + \gamma)] && \text{using } -(xy) = x(-y) \\
&= \alpha[(-\beta) + (-\gamma)] && \text{using } -(x+y) = (-x) + (-y) \\
&= \alpha(-\beta) + \alpha(-\gamma) && \text{using Step 6 (D) as } (-\beta) > 0^*, (-\gamma) > 0^* \\
&= -\alpha\beta - \alpha\gamma && \text{using } x(-y) = -(xy) \\
&= -(\alpha\beta + \alpha\gamma) && \text{using } -x - y = -(x+y) \\
\therefore \alpha(\beta + \gamma) &= \alpha\beta + \alpha\gamma && \text{using } x = y \iff -x = -y
\end{aligned}$$

(6) $\alpha < 0^*$

$\therefore (-\alpha) > 0^*$.

$$\begin{aligned}
-[\alpha(\beta + \gamma)] &= (-\alpha)(\beta + \gamma) && \text{using } -(xy) = (-x)y \\
&= (-\alpha)\beta + (-\alpha)\gamma && \text{using cases (2),(3),(4),(5) above} \\
&= -(\alpha\beta) + [-(\alpha\gamma)] && \text{using } (-x)y = -(xy) \\
&= -[\alpha\beta + \alpha\gamma] && \text{using } (-x) + (-y) = -(x+y) \\
\therefore \alpha(\beta + \gamma) &= \alpha\beta + \alpha\gamma && x = y \iff -x = -y
\end{aligned}$$

$\therefore$ (1) $\rightarrow$ (6) show $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ for all cases, proving **(D)**.

Step 8

r^* is a cut.

Proof: (1) $r-1 \in Q$ and $r+1 \in Q$.

$r-1 < r < r+1 \Rightarrow r-1 \in r^*, r+1 \notin r^*$. $\therefore r^* \neq \emptyset, r^* \neq Q$.

(2) Let $p \in r^*$. $\therefore p < r$. Let $q \in Q$ such that $q < p$. $\therefore q < r \Rightarrow q \in r^*$.

(3) Let $p \in r^*$. $\therefore p < r$. So, $2p < p + r \Rightarrow p < \dfrac{p+r}{2}$.

Let $q = \dfrac{p+r}{2}$, so $p < q$. Therefore,

$$\begin{aligned} p &< r \Rightarrow \\ p + r &< 2r \Rightarrow \\ q = \frac{p+r}{2} &< r \Rightarrow \end{aligned}$$

Thus, $p < q < r \Rightarrow q \in r^*$. So, when $p \in r^*$, there is a $q > p$ with $q \in r^*$.

Note: this also proves that 0^* and 1^*, mentioned in Step 4 and Step 6, are cuts.

$r^* + s^* = (r+s)^*$

One may wonder how Rudin, in proving $(r+s)^* \subset r^* + s^*$, came up with $2t = r + s - p$.

$p \in (r+s)^*$ means $p < r + s$. We need to find an $r' \in r^*, s' \in s^*$ such that $p = r' + s'$.

$\therefore$ We need a $t > 0$ so that $r' = r - t < r$ and $s' = s - t < s$. Obviously, any positive t will do, but we also want $p = (r-t) + (s-t) = r + s - 2t$, which means $2t = r + s - p$.

Since $p < r + s$, then $0 < r + s - p$. Thus, $2t = r + s - p > 0$, or $t = \dfrac{r+s-p}{2} > 0$.

So, given $p \in (r+s)^*$, we choose t as above which gives us $r' < r$ and $s' < s$ and $p = r' + s'$ so that $p \in r^* + s^*$.

$r^* s^* = (rs)^*$

$(rs)^* = \{p \in Q$ such that $p < rs\}$, and as shown above $(rs)^*$ is a cut.

What does $r^* s^*$ mean? Rudin first defined multiplication of cuts in R^+ to prove field properties, followed by definition of cuts less than or equal to 0^*. So, we will first consider the case of $r^*, s^* \in R^+$ (so $r^* > 0^*$ and $s^* > 0^*$), followed by cases when either r^* or s^* is less than or equal to 0^*.

Note that the proof of (c) in Rudin, $r^* < s^* \iff r < s$, does not depend on this case (b), and so case (c) can be used in proving case (b).

Also, from case (a), $r^* + (-r)^* = 0^*$, so that $-(r^*) = (-r)^*$, using field property (A4).

(1) $r^* > 0^*, s^* > 0^*$

By definition, $r^* s^*$ is the set of all $p \in Q$ such that $p \leq uv$ for some choice of $u \in r^*, v \in s^*$ in which $0 < u, 0 < v$.

(a) $r^*s^* \subset (rs)^*$

Let $p \in r^*s^*$. $\therefore p \leq uv$ for some $u \in r^*, v \in s^*$. $\therefore 0 < u < r, 0 < v < s$ and so $uv < rs$. $\therefore p < rs \Rightarrow p \in (rs)^*$. $\therefore r^*s^* \subset (rs)^*$.

(b) $(rs)^* \subset r^*s^*$

If $p \leq 0$, then for some choice of $u \in r^*, v \in s^*$ in which $0 < u, 0 < v$, $p < uv$, so $p \in r^*s^*$.

Suppose $p > 0$. We need to find u, v such that $0 < u < r, 0 < v < s$ and $p \leq uv$.

Since $p \in (rs)^*$, then $0 < p < rs$. $\therefore 0 < \dfrac{p}{r} < s$. $\therefore \dfrac{p}{r} \in s^*$. Since s^* is a cut, there exists an $s' \in s^*$ such that $0 < \dfrac{p}{r} < s' < s$. Also, $0 < \dfrac{p}{r} < s' \Rightarrow 0 < \dfrac{p}{s'} < r$, so $\dfrac{p}{s'} \in r^*$. Note $p = \dfrac{p}{s'}s'$.

$\therefore$ Let $u = \dfrac{p}{s'} \in r^*, v = s' \in s^*$. $\therefore p \leq uv$, so $p \in r^*s^*$.

$\therefore$ For all cases, $p \in (rs)^* \Rightarrow p \in r^*s^* \Rightarrow (rs)^* \subset r^*s^*$.

(a),(b) mean $(rs)^* = r^*s^*$ for $r^* \in R^+, s^* \in R^+$.

(2) $r^* = 0^*$ or $s^* = 0^*$

By Rudin's definition, $r^*s^* = 0^*$. Also, $r^* = 0^*$ means $r = 0$ and $s^* = 0^*$ means $s = 0$. $\therefore rs = 0 \Rightarrow (rs)^* = 0^*$.

$\therefore r^*s^* = (rs)^* = 0^*$.

(3) $r^* < 0^*, s^* < 0^*$

By Rudin's definition in Step 7, $r^*s^* = [-(r^*)][-(s^*)]$.

But $-(r^*) = (-r)^*$ and $-(s^*) = (-s)^*$. $\therefore r^*s^* = (-r)^*(-s)^*$.

$r^* < 0^* \Rightarrow r < 0$ and $s^* < 0^* \Rightarrow s < 0$, using case (c) in Step 8. $\therefore -r > 0, -s > 0$. So by (1) above, $(-r)^*(-s)^* = [(-r)(-s)]^* = (rs)^*$.

$\therefore r^*s^* = (rs)^*$.

(4) $r^* < 0^*, s^* > 0^*$

By definition, $r^*s^* = -([-(r^*)]s^*)$.

But $-(r^*) = (-r)^*$. Also, $r^* < 0^* \Rightarrow r < 0 \Rightarrow -r > 0$.

$\therefore r^*s^* = -((-r)^*s^*) = -([(-r)s]^*) = -(-[rs]^*)$ using (1) above, and $(-r)s = -(rs)$ from 1.16(d) in Rudin, using the field properties for Q.

$\therefore r^*s^* = -(-(rs)^*) = (rs)^*$, using 1.14(d). Note the field properties for cuts has already been proved in Steps 4 - 7.

(5) $r^* > 0^*, s^* < 0^*$

$r^*s^* = s^*r^*$ by Step 7, (M2). From (4) above, $s^*r^* = (sr)^*$, and $sr = rs$ in Q, so $r^*s^* = (rs)^*$.

Cases (1) $\rightarrow$ (5) mean $r^*s^* = (rs)^*$ for all $r, s \in Q$.