an integral prime ($a + bi$, $b = 0$) is prime in G. Then the same method would apply for $a + bi$ when $a = 0$, since i is a unit.

If an integral prime p does not remain prime in G, then p can be written in the form $p = x^2 + y^2$ where $x,y \in Z$. This can be seen by letting $p = \alpha \cdot \beta$ where α,β are not units and $\alpha = a + bi$. Then $N(p) = N(\alpha) \cdot N(\beta)$ implies $p^2 = N(\alpha) \cdot N(\beta)$. As a result, $p = N(\alpha)$, since p is prime in Z. Hence, $p = a^2 + b^2$. As a consequence of this result, note, for example, 2, 5, 13, and 29 are not prime in G and $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, and $29 = 5^2 + 2^2$. On the other hand, 3, for example, is prime in G and $3 \neq x^2 + y^2$ for any $x,y \in Z$.

A sufficient condition for $p \in Z$ to be prime in G is $p \equiv 3 \pmod 4$. To see why this is the case, let $p = 4n + 3$ for some $n \in Z$. Assume p is not prime in G. By the result just established above, $p = x^2 + y^2$. Thus $x^2 + y^2 = 4n + 3$ implies $x^2 + y^2 \equiv 3 \pmod 4$. Now if $x^2 + y^2 \equiv 3 \pmod 4$, x and y cannot both be even or odd. Therefore, without loss of generality, let $x = 2m + 1$ be odd and $y = 2r$ be even. Then $(2m + 1)^2 + (2r)^2 \equiv 3 \pmod 4$. But this implies $2(m^2 + m + r^2) \equiv 1 \pmod 2$, which is absurd. Hence, p is prime in G. As examples, note 3, 7, 11, and 19 are all congruent to 3 (mod 4) and 3, 7, 11, and 19 are primes in Z that are also prime in G.

It turns out that $p \equiv 3 \pmod 4$ is also a necessary condition for an integral prime to be prime in G. If p is an integral prime and either $p \equiv 1 \pmod 4$ or $p \equiv 2 \pmod 4$, then p is not prime in G. For if $p \equiv 2 \pmod 4$, then p is even and equals 2. But $2 = (1 + i)(1 - i)$ and hence is not prime in G. In order to establish the remaining case, the result "If $p \equiv 1 \pmod 4$, then there exists an $x \in Z$ such that $x^2 \equiv -1 \pmod p$" will be used without proof (see Schockley, p. 139). Let p be an integral prime and $p \equiv 1 \pmod 4$. Therefore, there exists an $x \in Z$ such that $x^2 + 1 \equiv 0 \pmod p$. But this implies that $p \mid (x + i)(x - i)$. Moreover, if p is prime in G, then either $p \mid (x + i)$ or $p \mid (x - i)$. In either case, $p = \pm 1$, a contradiction. Hence p is not prime in G. As a consequence of this result, integral primes such as 5, 13, and 29 are not prime in G since 5, 13, and 29 are all congruent to 1 (mod 4).

If p is prime in Z and $p \equiv 1 \pmod 4$, then p is not prime in G and $p = x^2 + y^2$; this being a consequence of the above remarks. Now $x + iy$ is prime in G since $N(x + iy) = x^2 + y^2 = p$, which is prime in Z. Therefore, to determine a factorization of an integral prime p in G, one needs only obtain the perfect squares contained in p and test pairwise sums of squares. For example, consider 29, which is not prime in G. The perfect squares contained in 29 are 1, 4, 9, 16, and 25. Since $29 = 4 + 25$, $29 = (2 + 5i)(2 - 5i)$.

REFERENCE

James E. Shockley. *Introduction to Number Theory*. New York: Holt, Rinehart, and Winston, Inc., 1967.

*****

A NOTE ON ORDERING THE COMPLEX NUMBERS

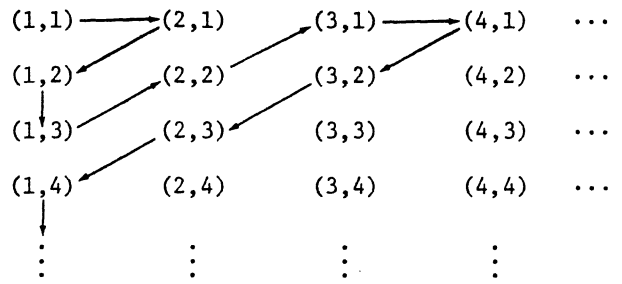
RICHARD C. WEIMER
Frostburg State College, Frostburg, Maryland

Many order relations can be defined on C. One of the most common orderings is the dictionary or lexicographical ordering. This order behaves in much the same way that the words are arranged in the dictionary. If the symbol "$\textcircled{<}$" is used to denote this order ("$\textcircled{<}$" is read "less than"), then $(a,b) \textcircled{<} (c,d)$ iff $a < c$, or $a = c$ and $b < d$. One can easily verify that $\textcircled{<}$ satisfies the definition of an order relation on C. Thus, $0 \textcircled{<} i$, $2 + 3i \textcircled{<} 3 + 16i$, $2 + 7i \textcircled{<} 2 + 10i$, $-3 - i \textcircled{<} 4$, etc.

Another ordering of C closely related to the dictionary ordering is the antilexicographical ordering. This ordering ($\boxed{<}$) is defined as: $(a,b) \boxed{<} (c,d)$ iff $b < d$ or $b = d$ and $a < c$. It is also an easy matter to verify that $\boxed{<}$ is an order relation on C.

As another illustration, one can show that Δ defined by $(a,b) \Delta (c,d)$ iff $\sqrt{a^2 + b^2} < \sqrt{c^2 + d^2}$, or $\sqrt{a^2 + b^2} = \sqrt{c^2 + d^2}$ and $\tan^{-1}(b/a) < \tan^{-1}(d/c)$ is an ordering of C. Thus $(1,2) \Delta (2,3)$ since $\sqrt{1^2 + 2^2} < \sqrt{2^2 + 3^2}$, and $(\sqrt{3},1) \Delta (\sqrt{2},\sqrt{2})$ since $\sqrt{(\sqrt{3})^2 + 1^2} = \sqrt{(\sqrt{2})^2 + (\sqrt{2})^2}$ and $\tan^{-1}(1/\sqrt{3}) = \pi/6$ $\tan^{-1}(\sqrt{2}/\sqrt{2}) = \pi/4$.

As a final illustration, any one-to-one correspondence between C and the members of an ordered set can be used to establish an order relation on C or any infinite subset of C, such as $G^+ = \{(a,b) \in Z \times Z \mid a,b > 0\}$. For example, consider the natural numbers with the usual ordering and the following list:



By using the above process, it is clear that there is a one-to-one correspondence between G^+ and the natural numbers. Thus, this correspondence induces the following order relation $\square$ on G^+: $(1,1) \square (2,1) \square (1,2) \square (1,3) \square (2,2) \square (3,1) \square \cdots$. Here $(1,3) \square (3,1)$ since $4 < 6$ (as natural numbers). Note that this ordering is not the dictionary ordering restricted to $G^+ \times G^+$ since $(2,2) \square (1,4)$ and $(1,4) \textcircled{<} (2,2)$.

It might also be observed that a field can be ordered as an ordered field if and only if no sum of squares of nonzero elements is zero (see Jacobson, p. 269). Since i and 1 are not zero and $i^2 + 1^2 = 0$, it follows that C with the usual operations can never be ordered as an ordered field.

Although C can be ordered, one should note that C with the order relation $\textcircled{<}$ does not satisfy the completeness property of the reals. The set

$$S = \{(3,1), (3.1,1), (3.14,1), (3,141,1), (3.1415,1), (3.14159,1), \ldots\},$$

for example, has $(\pi,1)$ as an upper bound. But $(\pi,.9)$ is also an upper bound and $(\pi,.9) \textcircled{<} (\pi,1)$. In fact, $(\pi,x) \textcircled{<} (\pi,1)$ if $x \textcircled{<} 1$. Since $\{x \in R | x < 1\}$ has no lower bound, S cannot have a least upper bound.

It can also be demonstrated that C with the order relation $\textcircled{<}$ does not possess the "Archimedean" property: If $(0,0) \textcircled{<} (a,b)$ and $(0,0) \textcircled{<} (c,d)$, then there exists a positive integer n such that $(c,d) \textcircled{<} n(a,b)$. For consider $(1,0)$ and $(0,1)$. Clearly $(0,1) \textcircled{<} (1,0)$, $(0,0) \textcircled{<} (1,0)$, and $(0,0) \textcircled{<} (0,1)$; but for no positive integer n can $(1,0) \textcircled{<} n(0,1)$.

It is interesting to note that C possesses a subset $G = \{a + bi | a,b \in Z\}$ that behaves in a similar fashion to the set $Z \times Z$ of pairs of integers; both structures are integral domains.

It is well known that Z with respect to $<$ (the usual order) is not dense, i.e., between any two integers there is not always another integer. This same result holds true for G. For example, consider (a,b) and $(a,b+1)$. Since there is no integer between b and $b+1$, G is not dense.

Between any two integers there is always a finite number of integers under the usual order. But this is not necessarily the case with the Gaussian integers, G. It is easily demonstrated that there are an infinite number of Gaussian integers (with respect to $\textcircled{<}$) between (a,b) and $(a+1,b)$ where a,b are positive integers. Thus, one can easily deduce that G^+ under $\textcircled{<}$ is not well ordered, i.e., not every nonempty subset of G possesses a smallest element. On the other hand, by considering the ordering of G^+ induced by the above list which establishes a one-to-one correspondence between the natural numbers and G^+, one notes that G^+ is well ordered with respect to this order.

For the natural numbers, if $a < b$ then $a + 1 \leq b$. This property does not carry over to G^+. This can be seen by considering $(1,2) \textcircled{<} (1,3)$. $(1,2) + (1,0) = (2,2)$ and $(1,3) \textcircled{<} (2,2)$.

REFERENCE

N. Jacobson. *Lectures in Abstract Algebra.* Vol. II: *Theory of Fields.* Princeton: Van Nostrand, 1951.

*****