CHAPTER 2, QUESTION 29

29. Use Question 12 to show that the irreducibles in $\mathbb{Z} + \mathbb{Z}i$ are $1 + i$ and its associates, $x \pm iy$ where $x^2 + y^2 = p$ (prime) $\equiv 1 \pmod 4$ and their associates, and q (prime) $\equiv 3 \pmod 4$ and its associates.

Solution. Let π be an irreducible in $\mathbb{Z} + \mathbb{Z}i$. Clearly, $\pi \mid \pi\bar{\pi}$ in $\mathbb{Z} + \mathbb{Z}i$, so that $\pi \mid a$ in $\mathbb{Z} + \mathbb{Z}i$ for some $a \in \mathbb{Z}$. As π (being an irreducible) is neither 0 nor a unit, it is clear that $a \neq 0, \pm 1$. Hence a has a nontrivial factorization into primes in $\mathbb{Z}$, say

$$a = p_1 \dots p_k,$$

where $k \in \mathbb{N}$ and each p_i is a prime in $\mathbb{Z}$. As $\mathbb{Z} + \mathbb{Z}i$ is a principal ideal domain (Theorem 2.2.3), π is a prime in $\mathbb{Z} + \mathbb{Z}i$ (Theorem 1.4.3). Hence, as $\pi \mid p_1 \dots p_k$, we deduce that $\pi \mid p_i$ for some $i \in \{1, 2, \dots, k\}$. We have shown the existence of a rational prime p such that $\pi \mid p$. Suppose there exists another prime $q \neq p$ such that $\pi \mid q$. As $\gcd(p, q) = 1$ there exist integers r and s such that

$$rp + sq = 1.$$

As $\pi \mid p$ and $\pi \mid q$, we see that $\pi \mid 1$, contradicting that π is an irreducible of $\mathbb{Z} + \mathbb{Z}i$. Hence, for each irreducible π in $\mathbb{Z} + \mathbb{Z}i$, there exist a unique prime p in $\mathbb{Z}$ such that $\pi \mid p$. Thus we can find all the irreducibles in $\mathbb{Z} + \mathbb{Z}i$ by factoring all the rational primes p into irreducibles in $\mathbb{Z} + \mathbb{Z}i$.

If $p = 2$ we have

$$2 = -i(1 + i)^2,$$

where $-i$ is a unit of $\mathbb{Z} + \mathbb{Z}i$. It is easily checked that $1 + i$ is an irreducible in $\mathbb{Z} + \mathbb{Z}i$ and if π is a prime dividing 2 then π is an associate of $1 + i$.

If $p \equiv 1 \pmod 4$ by Theorem 2.5.1 there are integers x and y such that $p = x^2 + y^2$. Hence

$$p = (x + iy)(x - iy)$$

in $\mathbb{Z} + \mathbb{Z}i$. It is easily checked that $x \pm iy$ are nonassociated irreducibles in $\mathbb{Z} + \mathbb{Z}i$, and that any prime π dividing p is an associate of $x + iy$ or $x - iy$.

Finally, if $p \equiv 3 \pmod 4$,it is easily verified using Question 12 that p is a prime in $\mathbb{Z} + \mathbb{Z}i$.

As $U(\mathbb{Z}+\mathbb{Z}i) = \{1, i, -1, -i\}$ (Exercise 1, Question 1) the irreducibles in $\mathbb{Z} + \mathbb{Z}i$ are

$1+i, \ -1+i, \ -1-i, \ 1-i;$
$x+iy, \ -y+ix, \ -x-iy, \ y-ix,$
$x-iy, \ y+ix, \ -x+iy, \ -y-ix,$ where $x^2+y^2 = p$ (prime) $\equiv 1 \pmod 4$;
$q, \ iq, \ -q, \ -iq,$ where q (prime) $\equiv 3 \pmod 4$. ∎

June 20, 2004