

## 8. Polynomial rings and unique factorization

### One variable polynomials over a field

**Lemma:** If  $f(x) \in F[x]$ , and  $r \in F$ , then  $f(r) = 0$  if and only if  $(x - r)$  divides  $f$ .

**Proposition:** A polynomial of degree  $n$  over a field  $F$  has at most  $n$  roots in  $F$ .

### Finite subgroups of fields

**Proposition:** Let  $U \in F^\times$  be a finite subgroup of a field  $F$ . Then  $U$  is cyclic.

**Corollary:**  $\mathbb{Z}/p\mathbb{Z}^\times$  is cyclic. Note: the number theorists call a generator of  $\mathbb{Z}/p\mathbb{Z}^\times$  a *primitive root* modulo  $p$ . There are  $\phi(p - 1)$  primitive roots modulo  $p$ .

### More discussions of quadratic rings

**Proposition:** (Fermat) A prime number is the sum of two squares if and only if it is 2 or is congruent to 1 mod 4.

**Lemma:** The congruence  $x^2 \equiv -1 \pmod{p}$  has a solution modulo a prime  $p$  if and only if  $p = 2$  or  $p \equiv 1 \pmod{4}$ .

**Proof:** If  $p = 2$ , 1 is a solution. If  $p$  is odd, and  $x^2 = -1$  has a solution, then  $(\mathbb{Z}/p\mathbb{Z})^*$  has an element of order 4, so  $4 \mid (p - 1)$ . Notice that  $(\mathbb{Z}/p\mathbb{Z})^*$  has only two elements of order dividing 2, because of  $x^2 \equiv 1 \pmod{p}$  then  $p \mid (x^2 - 1)$ , so  $p \mid (x + 1)(x - 1)$ , so either  $x \equiv 1 \pmod{p}$  or  $x \equiv -1 \pmod{p}$ . If  $4 \mid (p - 1)$  then let  $H$  be the Sylow 2-subgroup of  $(\mathbb{Z}/p\mathbb{Z})^*$ . If  $H$  were not cyclic, then there would be too many elements of order 2 in  $H$ . So  $H$  must be cyclic and therefore there is an element of order 4.

Now suppose that  $p \equiv 1 \pmod{4}$ . Let  $u$  be a solution to  $x^2 + 1 \equiv 0 \pmod{p}$ . Consider the ideal  $I = (p, u + i) \subset \mathbb{Z}[i]$ . This is a maximal ideal. If  $\pi = a + bi$  is a generator of this ideal, then  $p = x\pi$ . If  $x$  were a unit, then  $u + i$  would have to be a multiple of  $p$ , which it visibly isn't. Therefore  $N(\pi)$  must be  $p$ . But  $N(\pi) = a^2 + b^2$ , so we've found our representation.

**Proposition:** The ring  $\mathbb{Z}[\sqrt{-5}]$  is not a Euclidean ring. In fact, the ideal  $(3, 1 + \sqrt{-5})$  is not principal. It is a proper ideal, because the quotient of  $\mathbb{Z}[\sqrt{-5}]$  by this ideal is  $\mathbb{Z}/3\mathbb{Z}$ . If  $\pi$  were a generator of this ideal, then  $3 = x\pi$  means

that either  $N(\pi) = 3$  or  $N(\pi) = 9$ . Also  $(1 + 5i) = y\pi$  means that  $N(\pi)$  divides 6. Since  $\pi$  is not a unit,  $N(\pi) = 3$ . But the equation  $x^2 + 5y^2 = 3$  has no integer solutions, so there is no element of norm 3 in this ring.

**Proposition:**  $\mathbb{Z}[\sqrt{2}]$  is Euclidean with respect to the norm. It has an infinite unit group.

**Proposition:** Let  $\rho = e^{2\pi/3}$ . Then  $\mathbb{Z}[\rho]$  is Euclidean (and it has six units).

## Back to the Gaussian integers

The irreducibles in  $\mathbb{Z}[i]$  are: -  $(1 + i)$  -  $p \in \mathbb{Z}$  with  $p \equiv 3 \pmod{4}$  -  $a \pm bi$  where  $a^2 + b^2 = p$  for  $p \in \mathbb{Z}$  and  $p \equiv 1 \pmod{4}$ .

A positive integer is a sum of two squares if and only if it factors

$$n = 2^k p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_r^{f_r}$$

where the  $p_i \equiv 1 \pmod{4}$  and the  $q_i \equiv 3 \pmod{4}$  and all the  $f_i$  are even.

The proof follows from the question of when is  $n = N(x)$  for some  $x \in \mathbb{Z}[i]$ .