ALGEBRA HW 8

CLAY SHONKWILER

1

Let $p > 2$ be a prime number and let $f(x) = x^{\frac{p-1}{2}} - 1$.

(a): Show that every square in $(\mathbb{Z}/p)^*$ is a root of $f(x) \in (\mathbb{Z}/p)[x]$.

(b): Deduce that $f(x) = \prod_{i=1}^{r}(x - a_i)$, where f is as in (a) and where $\{a_1, \ldots, a_r\}$ is the set of squares in $(\mathbb{Z}/p)^*$.

(c): Show that -1 is a square in $(\mathbb{Z}/p)^*$ if and only if $p \equiv 1 \mod 4$.

Proof. Suppose -1 is a square in $(\mathbb{Z}/p)^*$. Then, by part (a),

$$0 = f(-1) = (-1)^{\frac{p-1}{2}} - 1 \quad \Rightarrow (-1)^{\frac{p-1}{2}} \equiv 1 \mod p.$$

Now, since $(-1)^k = \pm 1$, with $(-1)^k = 1$ exactly when k is even, we see that $\frac{p-1}{2}$ is even (since $1 \neq -1$ in $(\mathbb{Z}/p)^*$). Hence, $p - 1$ must be divisible by 4, which is to say that $p \equiv 1 \mod 4$.

On the other hand, if $p \equiv 1 \mod 4$, then $\frac{p-1}{2}$ is even and so

$$f(-1) = (-1)^{\frac{p-1}{k}} - 1 = 1 - 1 = 0.$$

By part (b), the roots of $f(x)$ are precisely the squares in $(\mathbb{Z}/p)^*$, so we see that -1 is a square in $(\mathbb{Z}/p)^*$. □

2

(a): Let $\alpha \in \mathbb{Z}[i]$. Show that if its norm $N(\alpha)$ is prime in $\mathbb{Z}$ then α is prime in $\mathbb{Z}[i]$.

Proof. Suppose $\alpha \in \mathbb{Z}[i]$ such that $N(\alpha) = \alpha\bar{\alpha}$ is prime in $\mathbb{Z}$. Suppose there exist $\beta, \gamma \in \mathbb{Z}[i]$ such that $\beta\gamma = \alpha$. Then, since norms are multiplicative, $N(\beta)N(\gamma) = N(\alpha)$. Since $N(\alpha)$ is prime in $\mathbb{Z}$, this implies that either $N(\beta)$ or $N(\gamma)$ is 1. However, the only elements of $\mathbb{Z}[i]$ with unit norm are $\pm 1, \pm i$, each of which is a unit in $\mathbb{Z}[i]$. Hence, either β or γ is a unit, so we conclude that α is prime in $\mathbb{Z}[i]$. □

(b): Show that the converse fails.

Proof. In PS 7 # 8, we saw that 3 is prime in $\mathbb{Z}[i]$; however, $N(3) = 9$, which is clearly not prime in $\mathbb{Z}$, so we see that the converse of the statement in (a) is false. □

3

In $\mathbb{Z}[\sqrt{n}]$, define the *conjugate* of $\alpha = a + b\sqrt{n}$ to be $\bar{\alpha} = a - b\sqrt{n}$. Define the *norm* of α to be $N(\alpha) = \alpha\bar{\alpha} = a^2 - nb^2$.

(a): Show that $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$ and that $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof. Let $\alpha = a + b\sqrt{n}$, $\beta = c + d\sqrt{n}$. Then

$$\alpha\beta = (a + b\sqrt{n})(c + d\sqrt{n}) = ac + nbd + (ad + bc)\sqrt{n},$$

so

$$\overline{\alpha\beta} = (ac + nbd) - (ad + bc)\sqrt{n} = (a - b\sqrt{n})(c - d\sqrt{n}) = \bar{\alpha}\bar{\beta}.$$

Hence,

$$N(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta).$$

□

(b): For which $n < 0$ is there a division algorithm in $\mathbb{Z}[\sqrt{n}]$, relative to $\alpha \mapsto N(\alpha)$?

4

(a): Show that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units, whereas $\mathbb{Z}[\sqrt{-2}]$ has only finitely many.

(b): Can you make a general conjecture about the number of units in $\mathbb{Z}[\sqrt{n}]$?

5

Let $p > 0$ be a prime number in $\mathbb{Z}$.

(a): Show that if $p \equiv 1 \mod 4$ then p is not prime in $\mathbb{Z}[i]$, but instead splits as the product of two distinct primes.

(b): Show that if $p \equiv 3 \mod 4$ the p remains prime in $\mathbb{Z}[i]$.

(c): Show that if $p = 2$ then up to a unit, p is the square of a prime in $\mathbb{Z}[i]$.

Proof. Note that

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

Now, $N(1 + i) = 1^1 + 1^1 = 2$. If $\alpha\beta = 1 + i$, then $N(\alpha)N(\beta) = 2$; since 2 is prime in $\mathbb{Z}$, either $N(\alpha)$ of $N(\beta)$ is 1. The only elements in $\mathbb{Z}[i]$ with unit norm are $\pm 1, \pm i$, each of which is a unit, so we see that, in fact, $1 + i$ is prime in $\mathbb{Z}[i]$ so, up to a unit, 2 is the square of a prime in $\mathbb{Z}[i]$. □

6

Suppose α is prime in $\mathbb{Z}[i]$ and let $p_1 \cdots p_r$ be the prime factorization of $N(\alpha)$ in $\mathbb{Z}$.

(a): Show that $\alpha | p_j$ for some j.

(b): Deduce that if $\alpha \notin \mathbb{Z} \cup i\mathbb{Z}$, then $N(\alpha)$ is prime.

7

Show that $\alpha \in \mathbb{Z}[i]$ is prime if and only if either

(i): $\alpha = \epsilon p$ where $\epsilon \in \{\pm 1, \pm i\}$ and $p > 0$ is a prime in $\mathbb{Z}$ with $p \equiv 3 \mod 4$; or

(ii): $N(\alpha)$ is prime in $\mathbb{Z}$.

8

Let R be a commutative ring.

(a): Let $I_1, \ldots, I_n$ be ideals in R, and let $\mathfrak{p} \subset R$ be a prime ideal containing $I_1 \cap \cdots \cap I_n$. Show that $I_i \subset \mathfrak{p}$ for some i.

(b): Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals in R, and let $I \subset R$ be an ideal that is contained in $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. Show that $I \subset \mathfrak{p}_i$ for some i.

(c): Explain the content of (a) and (b) geometrically.

DRL 3E3A, University of Pennsylvania
E-mail address: shonkwil@math.upenn.edu