MAT 150C - Homework 4

Markus Tran

1. (a) Let $\mathbb{F}$ be a field with characteristic $p$, and $a, b \in \mathbb{F}$. Then

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + \left( \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \right) + b^p.$$

Since the characteristic $p$ must be prime, we have $p \Big| \binom{p}{k}$ for $0 < k < p$ which means $\binom{p}{k} = np = 0$. Thus $(a+b)^p = a^p + b^p$

.

(b) $\Phi_{p^r}(x)$ is irreducible if $\Phi_{p^r}(x+1)$ is irreducible. Note that

$$(x+1)^{p^n} = \sum_{k=0}^{p^n} \binom{p^n}{k} x^k.$$

Since $p$ is prime, we have $p \Big| \binom{p^n}{k}$ for $0 < k < p^n$. This means that in $\mathbb{F}_p[x]$ with characteristic $p$,

$$(x+1)^{p^{r-1}} = x^{p^{r-1}} + 1,$$

and $$\Phi_{p^r}(x+1) = \frac{\left(x^{p^{r-1}} + 1\right)^p - 1}{x^{p^{r-1}} + 1 - 1} = \frac{\left(x^{p^{r-1}}\right)^p}{x^{p^{r-1}}} = x^{p^{r-1}(p-1)}.$$

Back in $\mathbb{Z}[x]$, this implies that all the terms of $\Phi_{p^r}$ are divisible by the prime $p$ except for the term of the highest degree of $p^{r-1}(p-1)$. By looking at the terms of smallest degree in the numerator and denominator, we see

$$\Phi_{p^r}(x+1) = \frac{(x+1)^{p^r} - 1}{(x+1)^{p^{r-1}} - 1} = \frac{\cdots + p^r x}{\cdots + p^{r-1} x}.$$

Thus the constant term is $p^r x / p^{r-1} x = p$ and is not divisible by $p^2$. By **Eisenstein's criterion**, $\Phi_{p^r}(x+1)$ is irreducible, and thus so is $\Phi_{p^r}(x)$

2. (a) Let $a = \alpha_1 + \alpha_2\sqrt{-n}$ and $b = \beta_1 + \beta_2\sqrt{-n}$ so that

$$ab = (\alpha_1\beta_1 - \alpha_2\beta_2 n) + (\alpha_1\beta_2 + \alpha_2\beta_1)\sqrt{-n}.$$

Then

$$\begin{aligned} N(ab) &= (\alpha_1\beta_1 - \alpha_2\beta_2 n)^2 + n(\alpha_1\beta_2 + \alpha_2\beta_1)^2 \\ &= (\alpha_1^2 + n\alpha_2^2)(\beta_1^2 + n\beta_2^2) \\ &= N(a)N(b). \end{aligned}$$

(b) Suppose $a$ is a unit, and let $ab = 1$. Then $N(a)N(b) = N(1) = 1$. Since $N$ is nonnegative, it must be that $N(a) = N(b) = 1$.

Suppose $N(a) = 1$, and let $a = \alpha + \beta\sqrt{-n}$. Since $n > 2$, we must have $\beta^2 = 0$ and also $\alpha^2 = 1$. Thus $a = \pm 1$ and $a$ is a unit.

Altogether, this means that the only units $\mathbb{Z}[\sqrt{-n}]$ are $1, -1$

.

(c) Suppose $2$ is reducible and $2 = ab$ where $a, b$ are not units. Then $N(2) = N(a)N(b)$. Since $N$ is nonnegative, either $N(a) = 1$ or $N(b) = 1$, and by (b), either $a$ or $b$ is a unit which is a contradiction. Thus $2$ is irreducible.

(d) Let $n$ be odd. Then $N(1 + \sqrt{-n}) = 1 + n$ is even.

Let $a = 1 + \sqrt{-n}$ and $b = 1 - \sqrt{-n}$. Then $ab = 1 + n > 2$ is divisible by $2$, but $2$ does not divide $a$ nor $b$. Thus $2$ is irreducible but not prime, which means $\mathbb{Z}[\sqrt{-n}]$ cannot be a UFD.