Discussion of 18.786 (Spring 2016) homework set #2

Darij Grinberg

March 24, 2016

1. Solution to problem 3

(b) We have $(-ab, b) = \underbrace{(a,b)}_{=-1} \underbrace{(-b,b)}_{\substack{=1 \\ \text{(well-known)}}} = -1$. Thus, neither $-ab$ nor b is a square in K.

We want to prove that every $d \in K$ admits a square root in $H_{a,b}$. So fix $d \in K$.

If d is a square in K, then we are done; hence, assume that it isn't. Thus, $d \in K^\times$ and $d \notin (K^\times)^2$.

We notice that

$$(xi + yj + zk)^2 = ax^2 + by^2 - abz^2 \qquad \text{for any } (x,y,z) \in K^3.$$

In particular, $(zk)^2 = -abz^2$ for any $z \in K$. Thus, if $-abd$ is a square – say, $-abd = \mu^2$ for some $\mu \in K$ –, then we have $d = -ab\left(\frac{\mu}{ab}\right)^2 = \left(\frac{\mu}{ab}k\right)^2$, which shows that d admits a square root in $H_{a,b}$. So we WLOG assume that $-abd$ is not a square.

Now, the projections of $-ab \in K^\times$ and $-abd \in K^\times$ onto the quotient group $K^\times / (K^\times)^2$ are distinct (since d is not a square) and both unequal to the identity element (since neither $-ab$ nor $-abd$ is a square). Since the quotient group $K^\times / (K^\times)^2$ is an $\mathbb{F}_2$-vector space (if we reframe its multiplication as addition), we thus conclude that the projections of $-ab \in K^\times$ and $-abd \in K^\times$ onto this $\mathbb{F}_2$-vector space $K^\times / (K^\times)^2$ are distinct and both nonzero, and thus $\mathbb{F}_2$-linearly independent (since any two distinct nonzero vectors in an $\mathbb{F}_2$-vector spaces are always $\mathbb{F}_2$-linearly independent). Since the Hilbert symbol is nondegenerate as an $\mathbb{F}_2$-bilinear form on $K^\times / (K^\times)^2$, we thus conclude the following: For any $\alpha \in \{1, -1\}$ and $\beta \in \{1, -1\}$, there exists some $\lambda \in K^\times$ such that $(-ab, \lambda) = \alpha$ and $(-abd, \lambda) = \beta$. Applying this to $\alpha = (a, b)$ and $\beta = (ab, d)$, we obtain the following: There exists some $\lambda \in K^\times$ such that $(-ab, \lambda) = (a, b)$ and $(-abd, \lambda) = (ab, d)$. Consider this λ.

Notice that $(-ab, ab) = 1$ (by the same well-known fact that gave us $(-b, b) = 1$).

Problem 4 on pset #1 now shows that $ax^2 + by^2 = \lambda$ has a solution (since $(-ab, \lambda) = (a, b)$). Consider these x and y.

Problem 4 on pset #1 (applied to ab, d, z and w instead of a, b, x and y) shows that $abz^2 + dw^2 = \lambda$ has a solution (since $(-abd, \lambda) = (ab, d)$). Consider these z and w.

If we had $w = 0$, then $abz^2 + dw^2 = \lambda$ would simplify to $abz^2 = \lambda$, which would entail that $\left(-ab, \underbrace{\lambda}_{=abz^2}\right) = \left(-ab, abz^2\right) = (-ab, ab) = 1$, which would contradict $(-ab, \lambda) = (a, b) = -1$. Hence, we cannot have $w = 0$. Thus, $w \neq 0$.

Now, $ax^2 + by^2 = \lambda = abz^2 + dw^2$. Solving this for d, we obtain

$$\begin{aligned} d &= \frac{ax^2 + by^2 - abz^2}{w^2} \qquad \text{(since } w \neq 0\text{)} \\ &= a\left(\frac{x}{w}\right)^2 + b\left(\frac{y}{w}\right)^2 - ab\left(\frac{z}{w}\right)^2 = \left(\frac{x}{w}i + \frac{y}{w}j + \frac{z}{w}k\right)^2, \end{aligned}$$

which shows that d has a square root in $H_{a,b}$. Part **(b)** is solved.