## Math 115. A Rephrased Theorem 3.10

This handout gives a more detailed variant of Theorem 3.10.

**Theorem.** *Let*

$$f(x,y) = ax^2 + bxy + cy^2$$

*be a nonzero binary quadratic form with integer coefficients, and let* $d = b^2 - 4ac$ *be its discriminant.*

(a). *If $d$ is a perfect square (including $0$), then $f$ can be factored into two linear factors with integer coefficients (note Exercise 9).*

(b). *If $d$ is not a perfect square, then $f$ cannot be factored into linear factors with rational coefficients.*

*Proof.* (a). Assume that $d$ is a perfect square.

**Case I:** $a = 0$**.** Then $f(x,y) = bxy + cy^2 = (bx + cy)y$ can be factored, and $d = b^2$ is a perfect square.

**Case II:** $a \neq 0$**.** By algebra we know that $az^2 + bz + c$ has rational roots $r_1$ and $r_2$ (possibly equal), so $f(x,y) = a(x - r_1y)(x - r_2y)$. Write $r_1 = h_1/k_1$ and $r_2 = h_2/k_2$ as fractions in lowest terms. Then

$$f(x,y) = \frac{a}{k_1k_2}(k_1x - h_1y)(k_2x - h_2y)\ ,$$

where

$$\frac{a}{k_1k_2}(-k_1h_2 - h_1k_2) = b \in \mathbb{Z} \qquad \text{and} \qquad \frac{a}{k_1k_2}h_1h_2 = c \in \mathbb{Z}\ .$$

It will suffice to show that $k_1k_2 \mid a$, since then $\frac{a}{k_1k_2} \in \mathbb{Z}$, and the factor $\frac{a}{k_1k_2}(k_1x - h_1y)$ has integer coefficients.

Let $p$ be a prime and let $\alpha, \beta$ be such that $p^\alpha \parallel k_1$ and $p^\beta \parallel k_2$. We want to show that $p^{\alpha+\beta} \mid a$.

**Case IIa:** $p \mid h_1$ **and** $p \mid h_2$**.** Then $\alpha = \beta = 0$, so there is nothing to prove.

**Case IIb:** $p \nmid h_1$ **and** $p \nmid h_2$**.** Since $c \in \mathbb{Z}$, we have $k_1k_2 \mid ah_1h_2$, hence $p^{\alpha+\beta} \mid ah_1h_2$. This implies $p^{\alpha+\beta} \mid a$ (since $p \nmid h_1h_2$), so we are done.

**Case IIc:** $p \mid h_1$ **but** $p \nmid h_2$**.** Then $p \nmid k_1$, so $p \nmid k_1h_2$. But $p \mid h_1k_2$, so $p \nmid (-k_1h_2 - h_1k_2)$, therefore (since $b \in \mathbb{Z}$) $k_1k_2 \mid a(-k_1h_2 - h_1k_2)$, and therefore $p^{\alpha+\beta} \mid a(-k_1h_2 - h_1k_2)$, so $p^{\alpha+\beta} \mid a$.

**Case IId:** $p \nmid h_1$ **but** $p \mid h_2$**.** This is similar to Case IIc (interchange the indices $1$ and $2$).

Therefore $f$ factors into linear factors with integer coefficients.

(b). We will prove the contrapositive: If $f$ can be factored into linear factors with rational coefficients, then $d$ is a perfect square.

First, if $a = 0$ then $d = b^2$ is a perfect square.

Otherwise, by assumption $f(x,y) = (k_1x + h_1y)(k_2x + h_2y)$ with $k_1, h_1, k_2, h_2 \in \mathbb{Q}$, and $k_1k_2 \neq 0$ since $a \neq 0$. Therefore the quadratic polynomial $az^2 + bz + c$ has rational roots $-h_1/k_1$ and $-h_2/k_2$, so $\sqrt{d} \in \mathbb{Q}$. As was noted earlier (in class on September 10), this implies that the integer $d = b^2 - 4ac$ is the square of an integer. $\square$