Primes - Problem Sheet 7

Composition of quadratic forms

Q1) Let $f = (a, b, c)$ be a primitive form, and M any integer. Show that f represents some integer coprime to M. Show also that we can assume f properly represents some integer coprime to M.

Q2) Suppose that F is (a) direct composition of f and g. If $f \sim f'$ and $g \sim g'$, and $F' \sim F$, show that F' is a direct composition of f' and g'. So we can use the Dirichlet composition to find the direct composition with explicit bilinear forms.

Q3) Suppose that $pq = X^2 + 14Y^2$ and $q = 2a^2 + 7b^2$. By considering the composition

$$\begin{aligned} p(2a^2 + 7b^2)(2a^2 + 7b^2) &= (X^2 + 14Y^2)(2a^2 + 7b^2) \\ &= 2(aX + 7bY)^2 + 7(-bX + 2aY)^2 \,. \end{aligned}$$

By reducing $2a^2 + 7b^2$, and $X^2 + 14Y^2$ modulo q, show that we may choose the sign $\pm a, \pm b, \pm X, \pm Y$, so that

$$q \mid aX + 7bY, -bX + 2aY \,,$$

hence conclude that p is represented by $2x^2 + 7y^2$.

Q4) Suppose that $F = (A, B, C)$ is the composition of $f = (a, b, c)$ and $g = (a', b', c')$ via

$$\begin{aligned} f(x, y)g(z, w) = F(&a_1xz + b_1xw + c_1yz + d_1yw, \\ &a_2xz + b_2xw + c_2yz + d_2yw) \,. \end{aligned}$$

Suppose all 3 forms have the same discriminant $D \neq 0$.

i) By specialising variables x, y, w, z prove that

$$\begin{aligned} aa' &= Aa_1^2 + Ba_1a_2 + Ca_2^2 \\ ac' &= Ab_1^2 + Bb_1b_2 + Cb_2^2 \\ ab' &= 2Aa_1b_1 + B(a_1b_2 + a_2b_1) + 2Ca_2b_2 \,. \end{aligned}$$

Hint: try $x = z = 1, y = w = 0$ for the first.

ii) Prove that $a^2(b'^2 - 4a'c') = (a_1b_2 - a_2b_1)^2(B^2 - 4AC)$, hence conclude

$$f(1, 0) = a = \pm(a_1b_2 - a_2b_1) \,.$$

iii) Prove that

$$g(1, 0) = a' = \pm(a_1c_2 - a_2c_1)$$

Q5) Recall that a group of order 4 is is isomorphic to either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or to $\mathbb{Z}/4\mathbb{Z}$. Determine the class group $\mathcal{C}(D)$ for $D = -56$, $D = -68$, $D = -84$, $D = -96$. Do you see any connection between $\mathcal{C}(D)$ and when genus theory works? Hint: to distinguish between $\mathbb{Z}/\mathbb{Z}2 \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ you only need to check whether some form is not properly equivalent to its inverse. Why? This is easy to do using reduced forms.

Q6) It is known that any *ternary* quadratic form $f(x,y,z)$ of determinant $\det(f) = 1$ is properly equivalent to $x^2+y^2+z^2$. (See Corollary 2 [Cassels 2008, p. 138].) Assuming this, show that there is no (nice!) notion of composition of integral ternary quadratic forms of fixed determinant. Hint: we would (want to) have

$$(x^2+y^2+z^2)(u^2+v^2+w^2) = (B_1(x,y,z;u,v,w))^2+(B_2(x,y,z;u,v,w))^2+(B_3(x,y,z;u,v,w))^2\,,$$

where $B_i(x,y,z;u,v,w) = a_{1,1}xu + \cdots + a_{3,3}zw$ are integral bilinear forms. Consider representations of $15 = 3 \times 5$ by $x^2+y^2+z^2$.

Q7) Suppose $D < 0$ is a discriminant, and that q is a prime such that $\left(\frac{D}{q}\right) = 1$. Show that

$$h(D) \geq \log\left(\frac{1}{4}(|D|)\right) / \log q\,.$$

Hint: some $g(x,y)$ of discriminant D represents q. If g has order M in the class group, then q^M is represented by the principal form. Put a bound on q^M.
Remark: With slightly stronger analysis, one can prove the bound

$$h(D) - 1 \geq \log\left(\frac{1}{4}(|D|+1)\right) / \log(q)\,.$$

For this, see the paper “Über die Klassenzahl imaginär-quadratischer Zahlkörper”, Nagel 1922.