1.4. **If K is a finite separable extension of F, show that $B(x, y) = \mathrm{tr}_{K/F}(xy)$ defines a regular quadratic space (K, B) over F. For $F = \mathbb{Q}$ and $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$, what is the diagonalization of (K, B)?**

Solution by Kendra Lockman, kendra (at) math:

Solution. By Dedekind's theorem on the independence of characters, $\mathrm{tr}_{K/F} = \sum_i \sigma_i$ is nonzero (here the σ_i are the distinct embeddings of K into an algebraic closure of F). Thus the bilinear form B is regular. Using the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ for the above particular example of K and F, the matrix for B is

$$\begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{bmatrix}.$$

Moreover, $\mathrm{span}\{\sqrt[3]{2}, \sqrt[3]{4}\}$ is hyperbolic since $\sqrt[3]{2}$ is an isotropic vector. Hence $K \cong \mathbb{Q} \cdot 1 \oplus \mathbb{H}$, and the Witt index of B is 1. A diagonalization of B is given by the basis $\{1, \sqrt[3]{2} + \sqrt[3]{4}, \sqrt[3]{2} - \sqrt[3]{4}\}$, with respect to which B has the diagonal matrix $\mathrm{diag}(3, 12, -12)$. □

1.6. **If $a, b \in F$ are such that $a^2 + b^2 = c \neq 0$, show that the 4-dimensional form $\langle 1, 1, -c, -c\rangle$ is hyberbolic.**

Solution by David Zywina, zywina@math.berkeley.edu:

$\langle 1, 1, -c\rangle$ represents $c = a^2 + b^2$, so $\langle 1, 1, -c\rangle \cong \langle c, d, e\rangle$ for some $d, e \in \dot{F}$. Taking determinants we see that $de = -1 \cdot \dot{F}^2$, hence $\langle d, e\rangle \cong \langle 1, -1\rangle$. Combining we get $\langle 1, 1, -c\rangle \cong \langle c, 1, -1\rangle$. By the Witt cancellation theorem, $\langle 1, -c\rangle \cong \langle c, -1\rangle$.

$\langle 1, 1, -c, -c\rangle$

$\cong \langle 1, -c\rangle \perp \langle 1, -c\rangle$

$\cong \langle 1, -c\rangle \perp \langle c, -1\rangle \cong \langle 1, -1\rangle \perp \langle c, -c\rangle \cong \mathbb{H} \perp \mathbb{H}$

1.7. Solution by Soroosh Yazdani, syazdani@math.berkeley.edu:

We want to prove that if $a_1 x_1^2 + \cdots + a_n x_n^2 = 0$ has a non-trivial solution, then it has a solution where none of the x_i's are zero. For the rest of this problem, I say a solution is nonzero, if none of its terms are zero. First, we will prove that $ax_1^2 - ax_2^2 + b_3x_3^2 + \cdots + b_kx_k^2$ has a nonzero solution. This is implied by showing that there is a non-zero solution to $x^2 - y^2 = c$ for some $c \in F$, since we can just take $x_3 = x_4 = \cdots = x_k = 1$, and take $c = -\frac{b_3+\cdots+b_k}{a}$. To show that $x^2 - y^2 = c$ has a nonzero solution, let $x = a + b$ and $y = a - b$. Then we are looking for $a \neq \pm b$ such that $4ab = c$. For any $a \neq 0$ there is a b satisfying the above equation. The number of such solutions with $a = b$ is at most two, since $a^2 = \frac{c}{4}$ has at most two solutions. Similarly, the number of solutions with $a = -b$ is at most two. So the number of solutions with $a \neq 0, \pm b$ is 5, so as long as $|F| > 5$ we can find a nonzero solution to $x^2 - y^2 = c$.

Now we proceed to prove that if $a_1x_1^2 + \cdots + a_nx_n^2 = 0$ has a non-trivial solution, then it has a nonzero solution. Let $(z_1, \ldots, z_n)$ be a non-trivial solution, with $z_1, \ldots, z_k$ nonzero and $z_{k+1} = \cdots = z_n = 0$. Without loss of generality, we can assume that $z_1 = 1$. Therefore $a_2x_2^2 + \cdots + a_kz_k^2 = -a_1$. Now consider the quadratic form $< a_1, -a_1, a_{k+1}, \ldots, a_n >$. We already showed that this has a nonzero solution. Let $(y_1, y_2, y_{k+1}, \ldots, y_n)$ be such a nonzero solution. Then

$$\begin{aligned} a_1(z_1y_1)^2 + a_2(z_2y_2)^2 + a_3(z_3y_2)^2 + \cdots + a_k(z_ky_2)^2 + a_{k+1}y_{k+1}^2 + \cdots + a_ny_n^2 \\ = a_1y_1^2 + (a_2z_2^2 + \cdots + a_kz_k^2)y_2^2 + a_{k+1}y_{k+1}^2 + \cdots + a_ny_n^2 \\ = a_1y_1^2 - a_1y_2^2 + a_{k+1}y_{k+1}^2 + \cdots + a_ny_n^2 = 0. \end{aligned}$$

Therefore $(z_1y_1, z_2y_2, z_3y_2, \ldots, z_ky_2, z_{k+1}y_{k+1}, \ldots, z_ny_n)$ is a solutions to $< a_1, \ldots, a_n >$, and since every element is nonzero, it is the desired solution.

1.10. **Show that the following conditions are equivalent:**

(a) Every 4-dimensional form over F of determinant -1 is isotropic.

(b) Every even-dimensional form over F of determinant -1 is isotropic.

(c) Every 3-dimensional form over F represents its own determinant.

(d) Every odd-dimensional form over F represents its own determinant.

Solution by Dave Freeman, `dfreeman@math`.

Solution. $(2 \Rightarrow 4)$: Let n be odd, and suppose $q = \langle a_1, \ldots, a_n \rangle$. Let q' be the $n+1$-dimensional form $q' = \langle a_1, \ldots, a_n, -\prod a_i \rangle$; q' has determinant -1. By hypothesis, q' is isotropic, so we may find a nonzero vector $(x_1, \ldots, x_{n+1})$ such that $q'(x_1, \ldots, x_{n+1}) = 0$. If $x_{n+1} \neq 0$ then we have

$$q\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right) = \prod_{i=1}^{n} a_i = d(q).$$

If $x_{n+1} = 0$ then q is isotropic and thus universal.

$(4 \Rightarrow 2)$: Let n be odd. Any $(n+1)$-dimensional form of determinant -1 can be written as $q = \langle a_1, \ldots, a_n, -\prod a_i \rangle$, where the a_i are all nonzero. By hypothesis, we can find $(x_1, \ldots, x_n)$ such that $a_1 x_1^2 + \cdots + a_n x_n^2 = \prod a_i$. Then

$$q(x_1, \ldots, x_n, 1) = \prod_{i=1}^{n} a_i - \prod_{i=1}^{n} a_i = 0.$$

Since $\prod a_i \neq 0$, at least one of x_i must be nonzero, so q is isotropic.

$(1 \Leftrightarrow 3)$ follows by the same arguments as above, taking $n = 3$.

$(4 \Rightarrow 3)$ is obvious.

$(3 \Rightarrow 4)$: Let n be odd; we induct on n. The case $n = 1$ is trivial, and the case $n = 3$ is our hypothesis. Let $q = \langle a_1, \ldots, a_n \rangle$. By hypothesis, $\langle a_{n-2}, a_{n-1}, a_n \rangle \cong \langle a_{n-2}a_{n-1}a_n, t, 1/t \rangle$ for some t, so we have

$$q \cong \langle a_1, \ldots, a_{n-3}, a_{n-2}a_{n-1}a_n, t, 1/t \rangle. \tag{1}$$

By the inductive hypothesis, $q' = \langle a_1, \ldots, a_{n-3}, a_{n-2}a_{n-1}a_n \rangle$ represents $\prod a_i = d(q')$. Suppose $q'(\vec{x}) = \prod a_i$. Then if we write q in the form (1), we have $q(\vec{x}, 0, 0) = \prod a_i = d(q)$. □

1.13. **Show that a regular quadratic space is isotropic iff it has a basis consisting of isotropic vectors.**

Solution by David Zywina, zywina@math.berkeley.edu:

$(\Leftarrow)$ If a quadratic space has a basis of isotropic vectors then clearly it is isotropic.

(⇒) Suppose we have a regular isotropic quadratic space (V, B, q) of dimension n. V is isotropic so there is a nonzero isotropic $w_1 \in V$. Now suppose we have linearly independent isotropic vectors $w_1, \cdots, w_k \in V$. If $k = n$ then we are done, so assume that $k < n$.

Let $W = span\{w_1, \cdots, w_k\}$.

Claim: There exists $v \in V \setminus W$ such that $B(v, w_1) \neq 0$.

Proof: Suppose the contrary (ie. $B(v, w_1) = 0$, for all $v \in V \setminus W$). Since B is regular, $B(V, w_1) \neq \{0\}$. Therefore $B(W, w_1) = B(V, w_1) \neq \{0\}$.
So there is a w_i, $1 \leq i \leq k$, such that $B(w_i, w_1) \neq 0$.
Pick any $v \in V \setminus W$, we then have $v + w_i \in V \setminus W$.
$B(v + w_i, w_1) = B(v, w_1) + B(w_i, w_1) = 0 + B(w_i, w_1) \neq 0$
This is a contradiction in our original assumption, and the claim is proved.

Take $v \in V \setminus W$ as in the claim above. For any $c \in \dot{F}$, $v + cw_1 \in V \setminus W$.

$$q(v + cw_1) = q(v) + 2cB(v, w_1) + c^2 q(w_1) = q(v) + 2cB(v, w_1)$$

Now take $c = \frac{-q(v)}{2B(v,w_1)}$, which is well defined since $B(v, w_1) \neq 0$. We then have $q(v + cw_1) = 0$, where $v + cw_1 \in V \setminus W$.

So define $w_{k+1} = v + cw_1$, and we get a linearly independent set $\{w_1, \cdots, w_k, w_{k+1}\}$ of isotropic vectors in V. Continuing by induction on the number of vectors, we get the desired basis.

1.14. **Let U be a (possibly not regular) subspace of dimension $m+r$ in a hyperbolic space $m\mathbb{H}$. Show that the Witt index of U is at least r. (In particular, $\dim U > m \implies U$ is isotropic.)**

Solution by Kendra Lockman, kendra (at) math:

Proof. Write $m\mathbb{H} = V \oplus V'$, with V totally isotropic, $\dim V = m$. Then $V \cap U$ is a maximal isotropic subspace of U, so the Witt index

$w.i.(U)$ must equal $\dim(V \cap U)$. Now

$$\begin{aligned} 2m &\geq \dim(V+U) \\ &= \dim V + \dim U - \dim(V \cap U) \\ &= m + (m+r) - w.i.(U), \end{aligned}$$

so $w.i.(U) \geq r$. □

1.17. **Let G be a finite group and $V = FG$ be the group ring of G over F. Let $T : V \to F$ be the linear functional defined by $T\left(\sum_{g \in G} a_g g\right) = a_1$, and let q be the quadratic form on V associated with the (symmetric) bilinear form $(\alpha, \beta) \mapsto T(\alpha\beta)$. Compute the Witt index of q.**

Solution by Dave Freeman, `dfreeman@math`.

Solution. The group elements of G form a basis of V over F. With respect to this basis, the matrix of q has entries $\{a_{gh}\}_{g,h \in G}$, where $a_{gh} = 1$ if $gh = 1$ and $a_{gh} = 0$ otherwise. In particular, $a_{gg} = 1$ if and only if $g^2 = 1$. If we order the basis of V so that every group element is next to its inverse, then the matrix is in block diagonal form and consists of an $r \times r$ identity matrix, where $r = \#\{g \in G \colon g^2 = 1\}$, followed by $(|G| - r)/2$ blocks of the form $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Since $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cong \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \cong \mathbb{H}$, the Witt index of q is thus $(|G| - r)/2$ plus the Witt index of $r\langle 1 \rangle$. In particular, if F is formally real, then the Witt index of q is $(|G| - r)/2$. □

1.18. **(Inductive Description of Isometry) For $n \geq 3$, show that $\langle a_1, \ldots, a_n \rangle \cong \langle b_1, \ldots, b_n \rangle$ iff there exist $a, b, c_3, \ldots, c_n \in \dot{F}$ such that $\langle a_2, \ldots, a_n \rangle \cong \langle a, c_3, \ldots, c_n \rangle$, $\langle b_2, \ldots, b_n \rangle \cong \langle b, c_3, \ldots, c_n \rangle$ and $\langle a_1, a \rangle \cong \langle b_1, b \rangle$.**

Solution by David Zywina, zywina@math.berkeley.edu:

($\Leftarrow$) Suppose we have $a, b, c_3, \ldots, c_n \in \dot{F}$ such that $\langle a_2, \ldots, a_n \rangle \cong \langle a, c_3, \ldots, c_n \rangle$, $\langle b_2, \ldots, b_n \rangle \cong \langle b, c_3, \ldots, c_n \rangle$ and $\langle a_1, a \rangle \cong \langle b_1, b \rangle$.

Using these isometries we get: $\langle a_1, a_2, a_3, \ldots, a_n \rangle \cong \langle a_1, a, c_3, \ldots, c_n \rangle \cong \langle b_1, b, c_3, \ldots, c_n \rangle \cong \langle b_1, b_2, b_3, \ldots, b_n \rangle$

($\Rightarrow$) Suppose that $\langle a_1, \ldots, a_n \rangle \cong \langle b_1, \ldots, b_n \rangle$.

Lemma: There exist $a, b, c_3, \ldots, c_n \in \dot{F}$ such that $\langle a_2, \ldots, a_n\rangle \cong \langle a, c_3, \ldots, c_n\rangle$, and $\langle a_1, a\rangle \cong \langle b_1, b\rangle$.

Proof: We have $b_1 \in D(\langle b_1, \ldots, b_n\rangle) = D(\langle a_1, \ldots, a_n\rangle)$, so there are $x_1, \ldots, x_n \in F$ such that $b_1 = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$. Let $a = a_2x_2^2 + \ldots + a_nx_n^2$

If $a = 0$, then b_1 and a_1 are equal upto a square of $\dot{F}$. So we have $\langle a_2, \ldots, a_n\rangle \cong \langle b_2, \ldots, b_n\rangle$. The lemma is easily shown to hold with the following values: $a = b = a_2$, $c_3 = a_3, \ldots, c_n = a_n$.

If $a \neq 0$, then let $b = a_1a/b_1$. The binary forms $\langle a_1, a\rangle$ and $\langle b_1, b\rangle$ both represent b_1, and both have the same determinant. Therefore, $\langle a_1, a\rangle \cong \langle b_1, b\rangle$.

The form $\langle a_2, \ldots, a_n\rangle$ represents a, so there are $c_3, \ldots, c_n \in \dot{F}$ such that $\langle a_2, \ldots, a_n\rangle \cong \langle a, c_3, \ldots, c_n\rangle$.

Take $a, b, c_3, \ldots, c_n$ as in the lemma above. All we have left to verify is that $\langle b_2, \ldots, b_n\rangle \cong \langle b, c_3, \ldots, c_n\rangle$.

$\langle b_1\rangle \perp \langle b, a_2, \ldots, a_n\rangle \cong \langle b_1, b\rangle \perp \langle a_2, \ldots, a_n\rangle \cong \langle a_1, a\rangle \perp \langle a_2, \ldots, a_n\rangle \cong \langle a\rangle \perp \langle a_1, \ldots, a_n\rangle \cong \langle a\rangle \perp \langle b_1, \ldots, b_n\rangle \cong \langle b_1\rangle \perp \langle a, b_2, \ldots, b_n\rangle$

By the Witt cancellation theorem we have:

$$\langle a\rangle \perp \langle b_2, \ldots, b_n\rangle \cong \langle b\rangle \perp \langle a_2, \ldots, a_n\rangle$$

So $\langle a\rangle \perp \langle b_2, \ldots, b_n\rangle \cong \langle b\rangle \perp \langle a_2, \ldots, a_n\rangle \cong \langle b\rangle \perp \langle a, c_3, \ldots, c_n\rangle$. Applying the Witt cancellation theorem again, we get $\langle b_2, \ldots, b_n\rangle \cong \langle b, c_3, \ldots, c_n\rangle$ as desired.

1.19. **Let φ be a regular group form. Show that for any regular form σ, $D(\varphi) \cdot D(\varphi \otimes \sigma) = D(\varphi \otimes \sigma)$.**

Solution by Dave Freeman, `dfreeman@math`.

Solution. Suppose φ is a form on V, and σ is a form on W. Pick diagonal bases $\{v_i\}, \{w_j\}$ for φ and σ respectively, and write $\varphi = \langle a_1, \ldots, a_n\rangle$ and $\sigma = \langle b_1, \ldots, b_m\rangle$. Let $x = \sum_i x_iv_i \in V$, $y = \sum_{i,j} y_{ij}v_i\otimes$

$w_j \in V \otimes W$ be arbitrary vectors. Then we have,

$$\begin{aligned}
\varphi(x) \cdot (\varphi \otimes \sigma)(y) &= \left(\sum_i a_i x_i^2\right)\left(\sum_{j,k} a_j b_k y_{jk}^2\right) \\
&= \sum_{i,j,k} a_i a_j b_k x_i^2 y_{jk}^2 \\
&= \sum_k b_k \left(\sum_i a_i x_i^2\right)\left(\sum_j a_j y_{jk}^2\right) \\
&= \sum_k b_k \varphi(x)\varphi(y_k),
\end{aligned}$$

where $y_k = \sum_j y_{jk} v_j$. Since φ is a group form, for each k there is some $z_k \in V$ such that $\varphi(x)\varphi(y_k) = \varphi(z_k)$. Let $z_k = \sum_l z_{lk} v_l$, and define $z \in V \otimes W$ by $z = \sum_{k,l} z_{lk} v_l \otimes w_k$. Then from above we have,

$$\begin{aligned}
\varphi(x) \cdot (\varphi \otimes \sigma)(y) &= \sum_k b_k \left(\sum_l a_l z_{lk}^2\right) \\
&= \sum_{k,l} a_l b_k z_{lk}^2 \\
&= (\varphi \otimes \sigma)(z).
\end{aligned}$$

We conclude that $D(\varphi) \cdot D(\varphi \otimes \sigma) \subset D(\varphi \otimes \sigma)$. Since φ is a group form it must represent 1, so we have $D(\varphi \otimes \sigma) \subset D(\varphi) \cdot D(\varphi \otimes \sigma)$, and thus equality holds. □

Remark 0.1. *The proof above doesn't appear to make use of the fact that φ and σ are regular. Is this hypothesis really necessary?*

1.20. **For $\varphi = \sigma \perp \tau$, show that**

$$D(\varphi) = \bigcup \{D(\langle s, t \rangle) \,:\, s \in D(\sigma),\ t \in D(\tau)\}.$$

From this, deduce that

$$D(\langle a \rangle \perp \tau) = \bigcup \{D(\langle a, t \rangle) \,:\, t \in D(\tau)\}.$$

Solution by Kendra Lockman, kendra (at) math:

Solution. Take an element a from the right-hand side of the equation, so we can write $a = sx^2 + ty^2$ for $x, y \in F$ and, say, $s = \sigma(v)$, $t = \tau(w)$. Then

$$\begin{aligned} a &= x^2\sigma(v) + y^2\tau(w) \\ &= \sigma(xv) + \tau(yw) \\ &= \sigma \perp \tau(xv + yw) \in D(\varphi). \end{aligned}$$

Conversely, take $a \in D(\varphi)$. Then we can find vectors v, w for which $a = \sigma \perp \tau(v + w) = \sigma(v) + \tau(w) \in D(\langle\sigma(v), \tau(w)\rangle)$. □

1.21. **If $0 \neq a^2 + b^2 \neq c^2$ in a field F, show that $\langle a^2 + b^2, a^2 + b^2 - c^2\rangle$ always represents 1 over F.**

Solution by Dave Freeman, `dfreeman@math`.

Solution. Let $q = \langle a^2 + b^2, a^2 + b^2 - c^2\rangle$. We have

$$\begin{aligned} q(a - c, b) &= (a^2 + b^2)(a - c)^2 + (a^2 + b^2 - c^2)b^2 \\ &= a^4 - 2a^3c + a^2c^2 + a^2b^2 - 2ab^2c + b^2c^2 + a^2b^2 + b^4 - b^2c^2 \\ &= a^4 - 2a^3c + a^2(2b^2 + c^2) - 2ab^2c + b^4 \\ &= (a^2 - ac + b^2)^2, \end{aligned}$$

so if $a^2 - ac + b^2 \neq 0$, then q represents 1.

If $a^2 + b^2 = ac$, then

$$\begin{aligned} q = \langle ac, ac - c^2\rangle &\cong \langle acb^2, ac - c^2\rangle \cong \langle ac(ac - a^2), ac - c^2\rangle \\ &\cong \langle a^2(c^2 - ac), ac - c^2\rangle \cong \langle c^2 - ac, ac - c^2\rangle. \end{aligned}$$

If $ac \neq c^2$ then this is a hyperbolic plane, which is universal. If $ac = c^2$ then $a = c$ (since $c \neq 0$), so $q = \langle a^2 + b^2, b^2\rangle$, which obviously represents 1 in both the cases $b = 0$ and $b \neq 0$. □

1.22. **(The Seven-Eleven Problem) What integers from 1 to 20 are represented by $\langle 7, 11\rangle$ over the rationals?**

Solution by David Zywina, zywina@math.berkeley.edu:

Suppose that we have a rational solution (x, y) to $7x^2 + 11y^2 = \alpha$, where $\alpha \in \{1, \cdots, 20\}$.

Then we can find $a, b, c \in \mathbb{Z}$, $c \neq 0$, such that $7a^2 + 11b^2 = \alpha c^2$ and a, b, and c are relatively prime.

Case 1: Suppose $\alpha \not\equiv 0 \pmod 7$.

If $c \equiv 0 \pmod 7$, then we would have $11b^2 \equiv 0 \pmod 7$. So $c \equiv b \equiv 0 \pmod 7$. So 7^2 divides $\alpha c^2 - 11b^2 = 7a^2$, which implies that 7 divides a. Now a, b, and c are all divisible by 7, which is impossible since they are relatively prime. Therefore, $c \not\equiv 0 \pmod 7$.

$\alpha c^2 = 7a^2 + 11b^2 \equiv 4b^2 \equiv (2b)^2 \pmod 7$

So $\alpha \equiv (2bc^{-1})^2 \pmod 7$. Therefore α is a quadratic residue modulo 7.

$\Rightarrow \alpha \equiv 1, 2, 4 \pmod 7$

Case 2: Suppose $\alpha \not\equiv 0 \pmod{11}$.

Similar to the last case, we can show that $c \not\equiv 0 \pmod{11}$.

$\alpha c^2 = 7a^2 + 11b^2 \equiv -4a^2 \equiv -(2a)^2 \pmod{11}$

So $\alpha \equiv -(2ac^{-1})^2 \pmod{11}$. Therefore $-\alpha$ is a quadratic residue modulo 11.

$\Rightarrow \alpha \equiv 2, 6, 7, 8, 10 \pmod{11}$

Case 1 $\Rightarrow \alpha \in \{1, 2, 4, 8, 9, 11, 15, 16, 18\} \cup \{7, 14\}$

Case 2 $\Rightarrow \alpha \in \{2, 6, 7, 8, 10, 13, 17, 18, 19\} \cup \{11\}$

Combining these, we get that $\alpha \in \{2, 7, 8, 11, 18\}$.

These in fact have solutions:

$$2 = 7(\frac{1}{3})^2 + 11(\frac{1}{3})^2$$

$$7 = 7 \cdot 1^2 + 11 \cdot 0^2$$

$$8 = 7(\frac{2}{3})^2 + 11(\frac{2}{3})^2$$

$$11 = 7 \cdot 0^2 + 11 \cdot 1^2$$

$$18 = 7 \cdot 1^2 + 11 \cdot 1^2$$

Therefore, in the range 1 to 20, only 2,7,8,11, and 18 are represented by $\langle 7, 11 \rangle$.

1.23. **For $a, b, \in \dot{F}$, show that**

$$D(\langle 1, a\rangle) \bigcap D(\langle 1, b\rangle) \subset D(\langle 1, -ab\rangle).$$

Solution by Soroosh Yazdani, syazdani@math.berkeley.edu: Recall that $\alpha \in D(\langle 1, \beta\rangle)$ if and only if $-\beta \in D(\langle 1, -\alpha\rangle)$. One can verify this fact by noting that

$$\begin{aligned} \alpha \in D(\langle 1, \beta\rangle) &\iff \alpha = x^2 + \beta y^2 \\ &\iff -\beta y^2 = x^2 - \alpha \\ &\iff -\beta y^2 \in D(\langle 1, -\alpha\rangle) \\ &\iff -\beta \in D(\langle 1, -\alpha\rangle). \end{aligned}$$

Therefore, if we have $\gamma \in D(\langle 1, a\rangle) \bigcap D(\langle 1, b\rangle)$, then $-a \in D(\langle 1, -\gamma\rangle)$ and $-b \in D(\langle 1, -\gamma\rangle)$. Recall that $\langle 1, -\gamma\rangle$ is a norm form, and hence a group form. Therefore $D(\langle 1, -\gamma\rangle)$ is a subgroup of $\dot{F}$. Therefore $(-a)(-b) = ab \in D(\langle 1, -\gamma\rangle)$, which implies $\gamma \in D(\langle 1, -ab\rangle)$ as was desired.

1.24. **Let $a, b, \in \dot{F}$. If $\langle 1, a\rangle$ is universal, show that**

$$D(\langle 1, b\rangle) = D(\langle 1, -ab\rangle).$$

Solution by Soroosh Yazdani, syazdani@math.berkeley.edu: Note that by problem 23 we have that

$$D(\langle 1, b\rangle) \subset D(\langle 1, -ab\rangle)$$

for all $b \in \dot{F}$ (since $D(\langle 1, a\rangle) = \dot{F}$). If we apply this to $-ab$ we get that

$$D(\langle 1, -ab\rangle) \subset D(\langle 1, -a(-ab)\rangle) = D(\langle 1, b\rangle).$$

Therefore

$$D(\langle 1, b\rangle) = D(\langle 1, -ab\rangle).$$

1.26. **Give an example of a regular ternary quadratic form** $q(x, y, z)$ **over a field for which each of the forms** $q(0, y, z), q(x, 0, z)$**, and** $q(x, y, 0)$ **has rank 1.**

Solution by David Zywina, zywina@math.berkeley.edu:

For any field of characteristic $\neq 2$, define:

$$q(x, y, z) = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

The matrix above has determinant 4, so q is regular.

Setting the variables to zero we get:

$$q(0, y, z) = \begin{pmatrix} y & z \end{pmatrix} \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} y \\ z \end{pmatrix}$$

$$q(x, 0, z) = \begin{pmatrix} x & z \end{pmatrix} \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} x \\ z \end{pmatrix}$$

$$q(x, y, 0) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Therefore $q(0, y, z), q(x, 0, z)$, and $q(x, y, 0)$ each have rank 1.