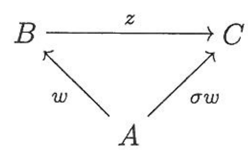
so u is anisotropic (and nonzero since y, w are independent). Consequently, $\tilde{\sigma}(u)$ is orthogonal to u, which means that

$$\begin{aligned} 0 &= B(\tilde{\sigma}(y+\varepsilon w),\, y+\varepsilon w) \\ &= B(\tilde{\sigma}y,\, y) + \varepsilon(B(\tilde{\sigma}w,\, y) + B(\tilde{\sigma}y,\, w)) + \varepsilon^2 B(\tilde{\sigma}w,\, w), \end{aligned}$$

where the last term is zero. Since $\varepsilon \in \dot{F}$ is arbitrary (and $|F| > 2$), we conclude that $B(\tilde{\sigma}y,\, y) = 0$, proving (7.9) in all cases. Applying Lemma 7.7 to the statement (7.9), we see that $\mathrm{Im}(\tilde{\sigma})$ is totally isotropic. But now (7.6)(2) gives $\tilde{\sigma}^2 = 0$, in contradiction to the hypothesis of Lemma 7.8. This establishes (1) of Lemma 7.8. It only remains to prove (2). Suppose $z = \widetilde{\sigma}(w) \neq 0$ and $\sigma_1 = \tau_z\sigma$. The claim $w \in L(\sigma_1)$ is clear from geometrical consideration of the "isosceles triangle" ABC:



This completes the proof. □

Remark 7.10. In (2) of Lemma 7.8, the conclusion can actually be strengthened to

$$L(\sigma_1) \supseteq L(\sigma) + F\cdot w \supsetneq L(\sigma),$$

although we did not need it in this form.

Exercises for Chapter I

1. Show that the group of self-isometries of the n-dimensional quadratic space $n\langle 1\rangle$ is isomorphic to the group $\mathrm{O}(n)$ of $n \times n$ orthogonal matrices over F.
2. Let $V = \mathbb{M}_n(F)$, viewed as a vector space (of dimension n^2) over F. Show that $B(X,Y) = \mathrm{tr}(XY)$ (for $x, y \in \mathbb{M}_n(F)$) defines a regular quadratic space $(V,\, B)$. Show that $(V,\, B)$ is isometric to $n\langle 1\rangle \perp m\mathbb{H}$ where $m = n(n-1)/2$, and find an orthogonal basis for $(V,\, B)$. Do the same problem for the new form $B'(X,Y) = \mathrm{tr}(X \cdot Y^t)$, and show that $(V,\, B')$ is isometric to $n^2\langle 1\rangle$. (For more background information on trace forms on algebras, see Exercise 29 below.)
3. On $V = \mathbb{M}_n(F)$, define $B_U(X,Y) = \mathrm{tr}(X\cdot UY^tU^{-1})$, where $X,\, Y \in V$, and U is a fixed nonsingular symmetric matrix. Show that B_U defines a nonsingular symmetric bilinear form on V. If U has a diagonalization $\langle a_1, \ldots, a_n\rangle$, show that $(V,\, B_U)$ has a diagonalization $\perp_{i,j} \langle a_ia_j\rangle$ (i.e. isometric to $\langle a_1, \ldots, a_n\rangle \otimes \langle a_1, \ldots, a_n\rangle$).

4. Let $a, b \in \dot{F}$, and let f be a regular quadratic form. Show that $f \perp \langle a \rangle$ represents $-b$ iff $f \perp \langle b \rangle$ represents $-a$.

5. 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 hyperbolic.

6. (Extending 3.6.) For (regular) quadratic forms $q_1, \ldots, q_n$, show that the orthogonal sum $q_1 \perp \cdots \perp q_n$ is isotropic iff there exist $a_i \in D(q_i)$ $(1 \leq i \leq n)$ such that $\langle a_1, \ldots, a_n \rangle$ is isotropic.

7. Let f be a regular isotropic diagonal quadratic form over a field of more than five elements. Show that f admits an isotropic vector whose coordinates are *all* nonzero.

8. (This exercise will be used at least a few times in the sequel.)
(1) Show that, if $\{F_i : i \in I\}$ is a family of subfields of a field K and $F = \bigcap_{i \in I} F_i \subseteq K$, then the natural map $\dot{F}/\dot{F}^2 \to \prod_i \dot{F}_i/\dot{F}_i^2$ is one-to-one.
(2) Deduce from (1) that, if $|I| < \infty$ and $|\dot{F}_i/\dot{F}_i^2| < \infty$ for all i, then $|\dot{F}/\dot{F}^2| < \infty$.

9. Let A be a UFD, whose group of units is U. If F is the quotient field of A, show that $\dot{F}/\dot{F}^2$ is the direct product of U/U^2 and a $\mathbb{Z}_2$-vector space whose basis consists of the prime elements of A (taken up to associates). If $A = \mathbb{Z}$, and $\{p_1, \ldots, p_n\}$, $\{q_1, \ldots, q_n\}$ are sets of distinct primes, show that $\langle p_1, \ldots, p_n \rangle \cong \langle q_1, \ldots, q_n \rangle$ over $\mathbb{Q}$ iff $p_i = q_i$ for all i (after a permutation).

10. Show that the following conditions are equivalent:

    (1) Every 4-dimensional form over F of determinant -1 is isotropic.
    (2) Every even-dimensional form over F of determinant -1 is isotropic.
    (3) Every 3-dimensional form over F represents its own determinant.
    (4) Every odd-dimensional form over F represents its own determinant.

    (For more information on the four equivalent conditions above, see Ch. X, Exercise 11.)

11. Prove the following "Witt's Extension Theorem." Let V be a regular quadratic space, and U_1, U_2 be two subspaces. If there exists a (bijective) isometry $\sigma : U_1 \to U_2$, show that there exists an isometry σ' of V onto V such that $\sigma' | \, U_1 = \sigma$. (This is essentially an equivalent version of 4.2.)

12. In a hyperbolic space V, a maximal totally isotropic subspace is sometimes called a *Lagrangian*. Show that V is always the sum of two Lagrangians.

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

14. Let U be a (possibly not regular) subspace of dimension $m+r$ in a hyperbolic space $m\,\mathbb{H}$. Show that $i(U)$ (the Witt index of U) is at least r. (In particular, $\dim U > m \Longrightarrow U$ is isotropic.)
15. Let U be a (possibly not regular) quadratic space of dimension k. Use the last exercise to show that U can be embedded (as a quadratic space) into the hyperbolic space $m\,\mathbb{H}$ iff $i(U) \geq k-m$.
16. For regular quadratic forms σ and φ, show that
    (1) $i\,(\sigma \otimes \varphi) \geq i\,(\sigma) \cdot \dim\,\varphi$;
    (2) $i\,(\sigma \perp \varphi) \leq i\,(\sigma) + \dim\,\varphi$; and
    (3) if σ is isometric to a subform of a regular form τ, then
    $$\dim\,\tau - i\,(\tau) \geq \dim\,\sigma - i\,(\sigma).$$
    (This is essentially a slight reformulation of (2).) Deduce that, if $\dim\,\sigma > \dim\,\tau - i\,(\tau)$, then σ must be isotropic.
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 $T\big(\sum_{g\in G} a_g g\big) = a_1$, 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. (**Hint.** The answer is $\big(|G| - r\big)/2$, where $r = \text{Card}\,\{g \in G:\ g^2 = 1\}$.)
18. Let φ be a regular group form. Show that for any regular form σ, $D(\varphi) \cdot D(\varphi \otimes \sigma) = D(\varphi \otimes \sigma)$.
19. (*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
    $$\langle a_2, \ldots, a_n\rangle \cong \langle a,\, c_3, \ldots, c_n\rangle\,, \qquad \langle b_2, \ldots, b_n\rangle \cong \langle b,\, c_3, \ldots, c_n\rangle\,,$$
    and $\langle a_1,\, a\rangle \cong \langle b_1,\, b\rangle$.
20. (*Inductive Description of Value Sets.*) 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
    $$D(\langle a\rangle \perp \tau) = \bigcup \{D\,(\langle a,\, t\rangle) :\ t \in D(\tau)\}.$$
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. (For instance, $1 \in D_{\mathbb{Q}}\langle 17,\, 13\rangle$.)
22. (The Seven-Eleven Problem) What integers from 1 to 20 are represented by $\langle 7,\, 11\rangle$ over $\mathbb{Q}$?
23. Show that $q = \langle 2,\, 3,\, 6\rangle$ does not represent 7 over $\mathbb{Q}$. (**Hint.** Find a chain equivalence from q to the form $\langle 1,\, 1,\, 1\rangle$. The isometry $\langle 2,\, 3,\, 6\rangle \cong \langle 1,\, 1,\, 1\rangle$ also reoccurs in a later calculation over the rationals: see the Example following II.3.3.)

24. For $a,\ b \in \dot{F}$, show that
    (1) $b \in D(\langle 1,\ a\rangle) \iff b \cdot \langle 1,\ a\rangle \cong \langle 1,\ a\rangle$, and
    (2) $D(\langle 1,\ a\rangle) \cap D(\langle 1,\ b\rangle) \subseteq D(\langle 1,\ -ab\rangle)$.
25. Let $a,\ b \in \dot{F}$. If $\langle 1,\ -a\rangle$ is universal, show that
$$D(\langle 1,\ b\rangle) = D(\langle 1,\ ab\rangle).$$
26. Show that a binary form $\langle 1,\ -a\rangle$ over $\mathbb{Q}$ is universal iff $a \in \dot{\mathbb{Q}}^2$.
27. 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.
28. Let $q = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ $(a_{ij} = a_{ji})$ be a quadratic form over a field. The rank of q is defined to be the rank of the symmetric matrix (a_{ij}). Show that rank(q) is the largest integer k such that, upon setting a suitable set of $n-k$ of the variables equal to 0, we get a *regular* quadratic form in the remaining k variables.
29. For any finite-dimensional F-algebra A, let $\mathrm{tr}_A : A \to F$ denote the algebra trace on A. Then
$$(x,\ y) \mapsto \mathrm{tr}_A(xy) \quad (x,\ y \in A)$$
defines a symmetric bilinear form on A, denoted by $(A,\ \mathrm{tr}_A)$ (or more precisely, $(A,\ \mathrm{tr}_{A/F})$). (This is called the *trace form* on the F-algebra A.) If B is another finite-dimensional F-algebra, show that:
    (1) $(A \times B,\ \mathrm{tr}_{A\times B}) \cong (A,\ \mathrm{tr}_A) \perp (B,\ \mathrm{tr}_B)$; and
    (2) $(A \otimes B,\ \mathrm{tr}_{A\otimes B}) \cong (A,\ \mathrm{tr}_A) \otimes (B,\ \mathrm{tr}_B)$
30. Let K be a finite field extension of F. If K/F is an inseparable extension, show that the trace form $\mathrm{tr}_{K/F}$ is identically zero. On the other hand, if K/F is a separable extension, show that $\mathrm{tr}_{K/F}$ is a *nonsingular* symmetric bilinear form; in particular, this is always the case if $\mathrm{char}(F) = 0$, or if $\mathrm{char}(F)$ is prime to $[K : F]$. (**Aside.** From the second part, it follows that $\mathrm{tr}_{A/F}$ is a nonsingular symmetric bilinear form for any commutative étale algebra A over the field F.)
31. Find diagonalizations over $\mathbb{Q}$ for the trace forms on the following number fields:
    (1) $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$;
    (2) $K_2 = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{2+\sqrt{2}}$;
    (3) $K_3 = \mathbb{Q}(\zeta)$, where ζ is a primitive 5th root of unity;
    (4) $K_4 = \mathbb{Q}(\sqrt[3]{2})$;
    (5) $K_5 =$ the splitting field of $X^3 - 2$ over $\mathbb{Q}$; and
    (6) $K_6 =$ the splitting field of $X^3 + 3X^2 - X - 1$ over $\mathbb{Q}$.