Appendix A. A missing Lemma

Let K be a finite field extension of $\mathbb{Q}$. Let $w_1, \ldots, w_r$ be a basis of K as a vector space over $\mathbb{Q}$. Let M be the subgroup of K generated by the w_i's. Let R be the collection of all elements α in K such that $\alpha \cdot M \subset M$. Let M^{-1} be the collection of all α in K such that $\alpha \cdot M \subset R$. We had claimed in an earlier version of these notes that $M \cdot M^{-1} = R$.

However this statement is false in general. As we show below this can be reduced to the case when $M = \check{R}$. In which case what is being asserted is that R is Gorenstein. But one can give an example of a non-Gorenstein number ring R.

Let Trace : $K \to \mathbb{Q}$ denote the trace map. The $\mathbb{Q}$-linear symmetric form $(\alpha, \beta) = \text{Trace}(\alpha\beta)$ is non-degenerate. Let $\check{M}$ denote the collection of all α in K such that $(\alpha, M) \subset \mathbb{Z}$; similarly, let $\check{R}$ denote the collection of all α in K such that $(\alpha, R) \subset \mathbb{Z}$. Let $C_R = (\check{R})^{-1}$ be the collection of all elements α in K such that $\alpha \cdot \check{R} \subset R$. We claim that:

$$\begin{aligned} M \cdot \check{M} &= \check{R} \\ C_R \cdot \check{R} &= R \end{aligned}$$

Together these conditions imply that $M \cdot \check{M} \cdot C_R = R$. It follows that $\check{M} \cdot C_R \subset M^{-1}$ and hence $M \cdot M^{-1} = R$.

Let $v_1, \ldots, v_r$ be elements of K such that $(v_i, w_j) = \delta_{ij}$, where the latter is the Kronecker delta; $\check{M}$ is the group generated by the v_i's. To every element α of K we can associate a matrix $A(\alpha)$ by putting $A(\alpha)_{ij} = (\alpha, w_i v_j)$ and then $\alpha w_i = \sum_j A(\alpha)_{ij} w_j$. This gives a homomorphism from K to $r \times r$ matrices over $\mathbb{Q}$ such that R is precisely the collection of elements whose images are matrices with entries in $\mathbb{Z}$. Moreover, $\text{Trace}(\alpha) = \text{Trace}(A(\alpha))$, where the latter is the trace $\sum_i A(\alpha)_{ii}$ in the usual sense, of the matrix A. For any matrix S we can define an element $r(S)$ by the condition $(r(S), \beta) = \text{Trace}(S \cdot A(\beta))$. It follows that $r(A(\alpha)) = \alpha$.

Now, the group D of integer matrices is self-dual under the pairing $(T, S) = \text{Trace}(TS)$. The image of R in this group D is "saturated", i. e. if T is a matrix such that nT is in the image of R for some non-zero integer n, then T is in the image of R. It follows that $r(D) = \check{R}$. Now, D is the free group on the elementary matrices E_{kl} whose only non-zero entry is a "1" in the (k, l)-th place. For any matrix S we have $(E_{kl}, S) = S_{kl}$. In particular, for any element α in K we have $(E_{kl}, A(\alpha)) = (\alpha, w_k v_l)$. Thus $r(E_{kl}) = w_k v_l$ which is in $M \cdot \check{M}$. It follows that $M \cdot \check{M}$ is $r(D)$ which is $\check{R}$, thus proving the first equality above.

A.1. **Counterexample.** Let R be a subring of a number field K and suppose that R is finitely generated as an abelian group. Let $(\alpha, \beta) = \text{Trace}(\alpha\beta)$ denote the non-degenerate symmetric form on K as above. Also let $\check{R}$ be the collection of elements α in K such that $(\alpha, R) \subset \mathbb{Z}$. Now let α be any element of K such that $\alpha\check{R} \subset \check{R}$. Then we have $(\alpha, \check{R}) \subset \mathbb{Z}$. By the non-degeneracy of the pairing we see that α lies in R. Thus by putting $M = \check{R}$ we see that R is precisely the ring associated by M in the leading paragraph of this section. Thus to provide a counterexample to the stated result it is enough to show that there is an R such that $\check{R}^{-1} \cdot \check{R}$ is strictly smaller than R.

Let b be an integer which is not a cube. Let K be the field obtain by adjoining a cube root β of b to $\mathbb{Q}$. Let a be any non-zero integer and let R be the subring of

K generated by $w_1 = 1$, $w_2 = a\beta$ and $w_3 = a\beta^2$. We have the identities

$$w_1^2 = w_1; w_1 w_2 = w_2; w_1 w_3 = w_3; w_2^2 = a w_3; w_2 w_3 = a^2 b; w_3^2 = a b w_1$$

It follows that $\mathrm{Trace}(w_1) = 3$ and $\mathrm{Trace}(w_1) = \mathrm{Trace}(w_2) = 0$. Thus if $\alpha = a_1 w_1 + a_2 w_2 + a_3 w_3$ is such that $(\alpha, R) \subset \mathbb{Z}$ we obtain the conditions

$$3a_1 \in \mathbb{Z}; 3a^2 b a_3 \in \mathbb{Z}; 3a^2 b a_2 \in \mathbb{Z}$$

Thus a basis for $\check{R}$ is given by $u_1 = w_1/3$, $u_2 = w_2/(3a^2 b)$ and $u_3 = w_3/(3a^2 b)$. Now suppose that $\alpha = a_1 w_1 + a_2 w_2 + a_3 w_3$ is such that $\alpha \check{R} \subset R$. We obtain the conditions

$$a_1 \in 3a^2 b \cdot \mathbb{Z}; a_2 \in 3ab \cdot \mathbb{Z}; a_3 \in 3a \cdot \mathbb{Z};$$

A basis for $\check{R}^{-1}$ is thus given by $v_1 = 3a^2 b w_1$, $v_2 = 3ab w_2$ and $v_3 = 3a w_3$. We then compute

$$u_1 v_1 = a^2 b w_1; u_2 v_3 = a w_1; u_3 v_2 = a b w_1$$

It follows that $a w_1$ is in the product $\check{R}^{-1} \cdot \check{R}$ but w_1 is not. Hence the product is strictly smaller than R.