Security proof for the one-time pad

Theorem.
The one-time pad is perfectly secret, that is: for every probability distribution for M, every message $m \in \mathcal{M}$ and every $c \in \mathcal{C}$ such that $\Pr[C = c] > 0$, $\Pr[M = m|C = c] = \Pr[M = m]$.

Proof. First write the definition :

$$\Pr[M = m|C = c] = \frac{\Pr[M = m \wedge C = c]}{\Pr[C = c]}.$$

We want to compute both probabilites.
First, since $C = K \oplus M$, we have $\Pr[M = m \wedge C = c] = \Pr[M = m \wedge K \oplus M = c]$. And $K \oplus M = c$ is equivalent to $K = M \oplus c$ and since in the probability, we have $M = m$, we can replace it by $K = m \oplus c$. Therefore, $\Pr[M = m \wedge C = c] = \Pr[M = m \wedge K = m \oplus c]$. Now, K and M are independent, therefore $\Pr[M = m \wedge K = m \oplus c] = \Pr[M = m]\Pr[K = m \oplus c]$. Since finally K is uniform, $\Pr[K = m \oplus c] = \frac{1}{2^\ell}$ (where ℓ is the common length of the messages, ciphertexts and keys). Altogether,

$$\Pr[M = m \wedge C = c] = \frac{1}{2^\ell}\Pr[M = m].$$

Second, we compute $\Pr[C = c]$ using the law of total probability:

$$\Pr[C = c] = \sum_{x \in \{0,1\}^\ell} \Pr[C = c \wedge M = x].$$

We can redo the same argument and rewrite $\Pr[C = c \wedge M = x] = \Pr[M = x]\Pr[K = x \oplus c] = \frac{1}{2^\ell}\Pr[M = x]$.
Therefore,

$$\Pr[C = c] = \sum_{x \in \{0,1\}^\ell} \frac{1}{2^\ell}\Pr[M = x] = \frac{1}{2^\ell}$$

since the sum over all possibilities x for M of $\Pr[M = x]$ equals 1.
The result follows.

Remark. In the slides, and during the class, the second part used the following “equality”: $\Pr[C = c] = \Pr[K = m \oplus c]$. This is nonsense since m does not appear in the left-hand side. Therefore, one needs to use the law of total probability to be able to introduce values for M. Note that the sum is over all $x \in \{0,1\}^\ell$, not the specific m from the statement.