Looking at how linear feedback shift registers (LFSRs) are implemented, one can notice that the tap coefficients feeding into the XOR have to be from an irreducible polynomial in the polynomial ring GF$(2)[x]$. Why is this?

Suppose we have polynomials modulo $x^2 + x + 1$. These polynomials form the Galois field GF(2^2). An LFSR shifts, which means it takes a polynomial $p(x) = p_0 + p_1 x$ representing the current 2–bit state vector, and multiplies it by x. After shifting, the highest order term $p_1 x^2$ needs to be folded back into the representation by eliminating x^2 using the equation $x^2 + x + 1 = 0$, which follows from modulo arithmetic. Hence, LFSR is shift followed by conditional XOR, which means addition of $x + 1$ if $p_1 = 1$.

So, the shift represents multiplication by the generator polynomial x which produces a sequence of all elements of the field's cyclic multiplicative group. The XOR computes the modulo operation after multiplication, and is there to keep the representation contained in the minimal amount of bits.