Some remarks on factorization

To discuss factorization of ideals into maximal ideals inside a ring $\mathcal{O}_K$ of algebraic integers inside an algebraic number field K, we recall some basic facts.

–Inside $\mathcal{O}_K$, maximal ideals are exactly the non-zero prime ideals. In general rings, maximal ideals are prime, but not every non=zero primes ideal is maximal.

–A *principal ideal* is an ideal generated by a single element, so we write such an ideal as $I = (r)$ for some element r. To spell this out, this means every element $x \in I$ is divisible by r inside $\mathcal{O}_K$. For example, inside the ring $\mathbb{Z}[2^{1/3}]$, the ideal $(5, 2^{1/3} - 3)$, that is, the ideal of all elements of the form $a5 + b(2^{1/3} - 3)$ for $a, b \in \mathbb{Z}[2^{1/3}]$, ends up being a principal ideal $(2(2^{1/3})^2 + 2^{1/3} - 2)$.

–The norm of a non-zero ideal $I \subset \mathcal{O}_K$ is the number of elements $|\mathcal{O}_K/I|$ in the quotient ring $\mathcal{O}_K/I$. For example, the norm of the ideal (3) in the ring $\mathbb{Z}$ is $|\mathbb{Z}/3| = 3$. However, note that if we write (3) in the ring $\mathbb{Z}[i]$, then the ideal consists of all elements of the form $(a + bi)3$ for $a, b \in \mathbb{Z}$, so $N((3)) = 3^2 = 9$. To calculate norms of ideals inside rings $\mathbb{Z}[\alpha]$ for an algebraic integer α with minimal polynomial $p(x)$, the presentation $\mathbb{Z}[x]/(p(x)) \simeq \mathbb{Z}[\alpha]$ is often useful. This isomorphism takes x to α and elements $f(x)$ go to $f(\alpha)$. Therefore,

$$\mathbb{Z}[x]/(p(x), f_1(x), \cdots, f_k(x)) \simeq \mathbb{Z}[\alpha]/(f_1(\alpha), \cdots, f_k(\alpha))$$

We will see an example of this below.

–Another convenient formula for norms of ideals is $N((r)) = |N(r)|$ (corollary 153).

Now, we know that every non-zero ideal in $\mathcal{O}_K$ can be uniquely factorized into maximal ideals (theorem 145). The basic maximal ideals arise as factors of the ideal (p) in $\mathcal{O}_K$, where p is a prime of $\mathbb{Z}$. The method for finding these factorizations and the maximal ideals involved is in Dedekind's factorization theorem (theorem 160). Note also the important fact that the values of the norms that occur in these factorizations is included in the theorem and actually uses one of the remarks above. (Which one?)

All of the preceding facts need to be learned completely. Lectures 16 to 21 should be reviewed thoroughly.

Here is a concrete example of factorization using them.

Consider inside the ring $\mathbb{Z}[\alpha]$ for $\alpha = \sqrt{-26}$ the ideal $I = (6, 2 + \alpha)$. To calculate the norm use

$$\mathbb{Z}[\alpha]/(6, 2 + \alpha) \simeq \mathbb{Z}[x]/(x^2 + 26, 6, 2 + x) \simeq (\mathbb{Z}/6)[x]/(x^2 + 26, 2 + x)$$

$$\simeq \mathbb{Z}/2[x]/(x^2, x) \times \mathbb{Z}/3[x]/(x^2 + 2, x + 2)$$

So

$$N(I) = |\mathbb{Z}/2[x]/(x^2, x)||\mathbb{Z}/3[x]/(x^2 + 2, x + 2)|$$

Now,

$$\mathbb{Z}/2[x]/(x^2, x) = \mathbb{Z}/2[x]/(x) \simeq \mathbb{Z}/2$$

and

$$\mathbb{Z}/3[x]/(x^2 + 2, x + 2) \simeq \mathbb{Z}/3[x]/(x^2 - 1, x - 1) \simeq \mathbb{Z}/3[x]/(x - 1) \simeq \mathbb{Z}/3$$

Therefore,

$$N(I) = 6 = 2 \cdot 3$$

This tells us that the maximal ideals dividing I must divide 2 and 3. So these must be factorized. Since $x^2 + 26 \equiv x^2 \mod 2$, we get $(2) = \mathcal{P}_2^2$ where $\mathcal{P}_2 = (2, \alpha)$ and $N(\mathcal{P}_2) = 2$. Similarly, $x^2 + 26 \equiv x^2 - 1 = (x + 1)(x - 1) \mod 3$, so $(3) = \mathcal{P}_3\mathcal{P}_3'$ where $\mathcal{P}_3 = (3, \alpha + 1)$ and $\mathcal{P}_3' = (3, \alpha - 1)$. Comparison of norms then tells us that the only possibility for the factorization of I is $I = \mathcal{P}_2\mathcal{P}_3$ or $I = \mathcal{P}_2\mathcal{P}_3'$. To find out which is correct, we need to find out which one of $I \subset \mathcal{P}_3$ and $I \subset \mathcal{P}_3'$ is true. Clearly, the element 6 is inside both ideals, so we have to check $2 + \alpha$ for membership in $\mathcal{P}_3$ or $\mathcal{P}_3'$. But clearly, $2 + \alpha = 3 + (\alpha - 1) \in \mathcal{P}_3'$. Therefore,

$$I = \mathcal{P}_2\mathcal{P}_3' = (2, \alpha)(3, \alpha - 1)$$