Notes on the MA160a Final

Question 3
Finding the class group of \( \mathbb{Q}(\sqrt{79}) \) is a little bit tricky. Here’s a brief sketch of how I would do it.

1. Compute \( \lambda \) (the “Minkowski Bound”): this is just under 11, so we consider the ideals lying over (2), (3), (5) and (7).

2. We find that
\[
(2) = (2, 1 + \sqrt{79})^2 \\
(3) = (3, \sqrt{79} - 1) \cdot (3, \sqrt{79} + 1) \\
(3) = (5, \sqrt{79} + 2) \cdot (5, \sqrt{79} - 2) \\
(3) = (7, \sqrt{79} + 3) \cdot (7, \sqrt{79} - 3)
\]

3. We check that \( (2, 1 + \sqrt{79}) = (9 + \sqrt{79}) \), and that neither of the ideals above 3 is principal.

4. Checking directly that the ideals above 5 are not principal is hard. One reason is that there is a solution in integers to
\[
x^2 - 79y^2 = 5z^2 \quad (x, y, z) = (19, 2, 3).
\]

5. Therefore one has to check in a cunning way. We will consider the ideal \( P := (3, \sqrt{79} - 1) \), and its powers.

6. We look at \( P^3 = (27, 5 + \sqrt{79}) \). This can be seen to be principal by noting that \( 5 + \sqrt{79} \) has norm 54, and by recalling that \( 9 + \sqrt{79} \) has norm 2. We check that \( P^3 = (-17 + 2\sqrt{79}) \); hence \( P^3 \) is principal.

7. We see that \( [P] \) does not have order 1; hence it has order 3. Similarly, let \( Q := (3, \sqrt{79} + 1) \) has order 3 also, because \( [PQ] = 1 \) and hence \( [Q] = [P^2] \). Hence the class group contains the cyclic group of order 3 as a subgroup.

8. We will now show that this is in fact the entire class group, by multiplying the ideals above 5 and 7 with \( P \) and \( Q \) and observing that these are principal. We can do this by noticing that there are elements of norm \(-15\) and \(21\): \(\pm 4 \pm \sqrt{79}\) and \(\pm 10 \pm \sqrt{79}\).

9. For example: \( P \cdot (5, 3 + \sqrt{79}) = (8 + \sqrt{79}) \). We can see this because when we multiply out the product of ideals we find that it is generated by \((15, 10 + 5\sqrt{79}, 9 + 3\sqrt{79})\). We notice that \(2(9 + 3\sqrt{79}) - (10 + 5\sqrt{79}) = 8 + \sqrt{79} \), and we check by hand that \((8 + \sqrt{79})\) is the same as \((P \cdot (5, 3 + \sqrt{79}))\).
10. Therefore, the two prime ideals above 5 are represented in the class group by \([P]\) and \([P^2]\). Notice that we have indirectly shown that these two ideals are not principal.

11. Similarly, \( P \cdot (7, 4 + \sqrt{79}) = (21, 12 + 3\sqrt{79}, 14 + 7\sqrt{79}) \), and we see that this ideal is in fact generated by \((10 - \sqrt{79})\).

12. So the class group is \( \mathbb{Z}/3\mathbb{Z} \).