Algebraic number theory

Solutions sheet 3

March 17, 2011

1. (a) In the first case any additive subgroup of $\mathbb{Q}$ generated by finitely many elements will have only finitely many primes in denominators. This is also true in the second case. In the third case any finitely generated subgroup of $\mathbb{Q}/\mathbb{Z}$ is finite, and so is never equal to the whole group.

(b) For a factor group of G this is obvious: it is generated by the images of generators of G. Let M be a f.g. abelian group, and let $N \subset M$ be a subgroup. There exists a surjective homomorphism $f : \mathbb{Z}^n \rightarrow M$ for some n. By a theorem from lectures $f^{-1}(N)$ is isomorphic to $\mathbb{Z}^r$ for some r. Then N is generated by the images of the standard basis vectors of $\mathbb{Z}^r$.

2. The discriminant of the polynomial is -11, so $K = \mathbb{Q}(\sqrt{-11})$. Since -11 is 1 modulo 4, $p = 2$ is not ramified, so the only prime ramified in K is 11. The prime 2 is inert since -11 is 5 modulo 8. Gauss reciprocity implies that an odd $p \neq 11$ is split if and only if p is a square modulo 11, that is, 1, 3, 4, 5 or 9 modulo 11.

$p = 47$ is 3 modulo 11, so it is split in K. The minimal polynomial of $\delta = \frac{1}{2}(1 + \sqrt{-11})$ is $t^2 - t + 3$. Let's solve it modulo 47 using the standard formula. -11 is 6^2 modulo 47; note also that $\frac{1}{2}$ is 24. Hence the solutions are 27 and 21. (It's good to check here that $21 + 27$ is 1 mod 47, and 21×27 is 3 mod 47.) Therefore the ideals are $(47, \delta - 27)$ and $(47, \delta - 21)$.

There is a quicker way to find these ideals. Let d be a square-free integer congruent to 1 modulo 4, $\delta = \frac{1}{2}(1 + \sqrt{d})$, and let $p \neq 2$ be an odd prime that splits in $\mathbb{Q}(\sqrt{d})$. Let A be an integer such that $t^2 - t + \frac{1}{4}(1 - d) = (t - A)(t - 1 + A)$ modulo p. I claim that we have the equality of ideals

$$(p, \delta - A) = (p, \sqrt{d} - a),$$

where a is an integer such that $a^2 \equiv d \bmod p$. In fact, we can take $a = 2A-1$.

Since $\sqrt{d} = 2\delta - 1$ the displayed equality becomes

$$(p, \delta - A) = (p, 2(\delta - A)).$$

But $\delta - A \equiv (p+1)/2 \times 2(\delta - A) \bmod p$, so we are done.

Going back to the question we obtain $(47, \delta - 27) = (47, \sqrt{-11} - 6)$, and similarly $(47, \delta - 21) = (47, \sqrt{-11} + 6)$. Please bear in mind that this will only work for *odd* primes, and for 2 you will need the general formulae with δ given in lectures.

3. (a) If d is 2 or 3 mod 4, then 2 is ramified. If d is 1 mod 4, then $d \neq \pm 1$, so there is a odd prime p dividing d, which is ramified in $\mathbb{Q}(\sqrt{d})$.

(b) Let d be the product of all *odd* primes in S, and let $d^* = \pm d$, where the sign is chosen so that $d^* \equiv 1 \bmod 4$. If $S = \{2\}$ define $d^* = 1$. If S does not contain 2, then $\mathbb{Q}(\sqrt{d^*})$ does the job, and this is the only quadratic field ramified exactly at the primes of S. If S contains 2, then we have $\mathbb{Q}(\sqrt{-d^*})$, $\mathbb{Q}(\sqrt{2d^*})$, $\mathbb{Q}(\sqrt{-2d^*})$.

4. The linear span of $\sqrt[3]{d}$ and $\sqrt[3]{d}^2$; the linear span of $\sqrt{a}$, $\sqrt{b}$ and $\sqrt{ab}$. The calculation is straightforward.

5. Write $a = x + y\sqrt{d}$, then $x - y\sqrt{d} = (z_1 + z_2\sqrt{d})(x + y\sqrt{d})$ gives a system of two linear equations in x and y with zero determinant.

6. $-5 \equiv 3 \bmod 4$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. If $I = (a + b\sqrt{-5})$, a, $b \in \mathbb{Z}$, then $a^2 + 5b^2$ divides 4 and 6, so an easy calculation shows that $a + b\sqrt{-5}$ is a unit, hence $I = \mathcal{O}_K$. But I is a prime ideal over 2, so $I = \mathcal{O}_K$ is impossible. Therefore, I is not principal. We have $I^2 = 2\mathcal{O}_K$ which is clearly principal.

7. Consider $d = -1$, -2 and -3, and do an easy calculation using Gauss reciprocity. In the last case $-3 \equiv 1 \bmod 4$, and the norm looks like this:

$$N(a + b\delta) = a^2 + ab + b^2(1 - d)/4 = a^2 + ab + b^2.$$