Algebraic Number Theory - Assignment 2

Matteo Durante, 2303760, Leiden University

23rd September 2018

Please consider exercises 10 and 24.

Exercise 10

$$\begin{aligned}(H:I):J &= \{x \in \mathbb{K} \mid xJ \subset H:I\} \\ &= \{x \in \mathbb{K} \mid \forall j \in J \; xj \in H:I\} \\ &= \{x \in \mathbb{K} \mid \forall j \in J \; \forall i \in I \; xij \in H\} \\ &= \{x \in \mathbb{K} \mid xIJ \subset H\} \\ &= H:(IJ)\end{aligned}$$

$$\begin{aligned}(\bigcap_k I_k):J &= \{x \in \mathbb{K} \mid xJ \subset \bigcap_k I_k\} \\ &= \{x \in \mathbb{K} \mid \forall k \; xJ \subset I_k\} \\ &= \bigcap_k \{x \in \mathbb{K} \mid xJ \subset I_k\} \\ &= \bigcap_k (I_k : J)\end{aligned}$$

$$\begin{aligned}I:(\sum_k J_k) &= \{x \in \mathbb{K} \mid x(\sum_k J_k) \subset I\} \\ &= \{x \in \mathbb{K} \mid \sum_k xJ_k \subset I\} \\ &= \{x \in \mathbb{K} \mid \forall k \; xJ_k \subset I\} \\ &= \bigcap_k \{x \in \mathbb{K} \mid xJ_k \subset I\} \\ &= \bigcap_k (I:J_k)\end{aligned}$$

Indeed, let $x \in \mathbb{K}$ be s.t. $x(\sum_k J_k) \subset I$. Then, for every finite set of indexes and any choice of elements $f_{k_i} \in J_{k_i}$, $x(f_{k_1} + \cdots + f_{k_n}) = xf_{k_i} + \cdots + xf_{k_n} \in I$, hence $\sum_k xJ_k \subset I$. The proof in the opposite direction follows the steps backwords.

Exercise 12

We know that, given a domain R and fractional R-ideals I and J, $r(I) = I : I$ and $I = IR$.

Being a fractional ideal, I is an R-module and the same goes for $r(I)$, hence $\forall x \in R$ we have that $xI \subset I$, therefore $R \subset r(I)$. Now, let $x \in r(I)$. Then, $xI \subset I$, ergo $xII^{-1} \subset II^{-1}$, i.e. $xR \subset R$. In particular, $x = x1 \in R$, therefore $R = r(I)$.

Now, let R, R' be subrings (subdomains) of $\mathbb{K} = Q(R) = Q(R')$ (field) such that I is an invertible R-ideal and an invertible R'-ideal. Earlier we proved that, given these conditions, we should have $r(I) = R$ and $r(I) = R'$. Since the definition of $r(I) = \{x \in \mathbb{K} \mid xI \subset I\}$ is independent from the subring we are considering, we get that $R = R'$.

Exercise 13

First, we consider the ring homomorphism $\phi : \mathbb{Z}[\sqrt{-19}] \to \mathbb{F}_2$ defined as $\phi(a + b\sqrt{-19}) = a + b$. Let's prove that it is a homomorphism:

$$\begin{aligned}
\phi((a + b\sqrt{-19}) + (c + d\sqrt{-19})) &= \phi((a + c) + (b + d)\sqrt{-19}) \\
&= (a + c) + (b + d) \\
&= \phi(a + b\sqrt{-19}) + \phi(c + d\sqrt{-19}) \\
\phi((a + b\sqrt{-19})(c + d\sqrt{-19})) &= \phi((ac - 19bd) + (ad + bc)\sqrt{-19}) \\
&= ac - 19bd + ad + bc \\
&= ac + bd + ad + bc \\
&= (a + b)(c + d) \\
&= \phi(a + b\sqrt{-19})\phi(c + d\sqrt{-19})
\end{aligned}$$

Notice that $\ker \phi = (2, 1 + \sqrt{-19})$, hence it is a maximal ideal. We observe that $\frac{1-\sqrt{-19}}{2} \in r(\mathfrak{m})$ because $2\frac{1-\sqrt{-19}}{2} = 1-\sqrt{-19} \in \mathfrak{m}$ and $(1+\sqrt{-19})\frac{1-\sqrt{-19}}{2} = 10 \in \mathfrak{m}$, therefore $\frac{1-\sqrt{-19}}{2} \in r(\mathfrak{m}) \neq R$.

Observe that $\mathfrak{m}^2 = (2^2, 2(1 + \sqrt{-19}), (1 + \sqrt{-19})^2) = (4, 2 + 2\sqrt{-19}, -18 + 2\sqrt{-19}) = (4, 2 + 2\sqrt{-19}) = 2\mathfrak{m}$, hence, if it did have an inverse J, setting $R = \mathbb{Z}[\sqrt{-19}]$, we would have $I = IR = I^2J = 2IJ = 2R$, which is obviously false.

Let $2R = \mathfrak{p}\mathfrak{q}$ with $\mathfrak{p}$, $\mathfrak{q}$ prime ideals. Then, $2\mathfrak{m} = \mathfrak{m}^2 \subset \mathfrak{p}\mathfrak{q} \subset \mathfrak{p} \cup \mathfrak{q}$, hence $\mathfrak{m}^2$ is contained in $\mathfrak{p}$ or $\mathfrak{q}$; let's say $\mathfrak{m}^2 \subset \mathfrak{p}$. Then, being $\mathfrak{p}$ prime, $\mathfrak{m} \subset \mathfrak{p}$, thus $\mathfrak{m} = \mathfrak{p}$. Now we have that $2R = \mathfrak{m}\mathfrak{q}$, hence $2\mathfrak{m} = \mathfrak{m}^2\mathfrak{q}$, which implies that $\mathfrak{q} = R$. We have arrived at a contradiction.

Exercise 24

Let $\alpha \not\subset \mathfrak{p}_i \ \forall i \leq n$. We will prove that $\alpha \not\subset \bigcup_{i=1}^n \mathfrak{p}_i$.

For $n = 1$, the thesis is trivial.

Let's assume it is true for $n - 1$ $n > 1$. Then, for any choice of $n - 1$ indexes among those n, we may find an element $x_j \in (\alpha \setminus \bigcup_{i=1, i\neq j}^n \mathfrak{p}_i)$.

If there is an index j s.t. $x_j \notin \mathfrak{p}_j$, we are done.

Otherwise, having $x_j \in \mathfrak{p}_j \ \forall j$, consider $y = \sum_{j=1}^n \Pi_{i=1, i\neq j}^n x_i$. We have that $y \in \alpha$ and $y \notin \mathfrak{p}_j \ \forall j$.

Indeed, if this was not the case, then $\Pi_{i=1, i\neq j}^n x_i \in \mathfrak{p}_j$ for some j, hence $x_i \in \mathfrak{p}_j$ for some $i \neq j$ because $\mathfrak{p}_j$ is prime, which is absurd.