Homework 14

1. To show that $Q[\sqrt{d}]$ is a Field, we must show that $Q[\sqrt{d}]$ is a commutative division ring.

First observe that it is commutative:

$$\text{Let } (a+b\sqrt{d}),\ (x+y\sqrt{d}) \in Q[\sqrt{d}].$$

$$\begin{aligned}(a+b\sqrt{d})\cdot(x+y\sqrt{d}) &= ax + (bx+ay)\sqrt{d} + byd \\ &= xa + (xb+ya)\sqrt{d} + ybd \\ &= (x+y\sqrt{d})\cdot(a+b\sqrt{d})\end{aligned}$$

as $Q[\sqrt{d}]$ is a ring under the same operations as Q, which includes commutative multiplication.

To show that it is a field, we must show that every nonzero element is a unit, and therefore is multiplicatively invertible:

$\neq 0$

Let $q \in Q(\sqrt{d}) = a + b\sqrt{d}$. Then

$\frac{1}{q} = \frac{1}{a+b\sqrt{d}}$, which $a - b\sqrt{d} \in Q(\sqrt{a})$ follows

$$\frac{1}{q} = \frac{a-b\sqrt{d}}{(a+b\sqrt{d})(a-b\sqrt{d})} = \frac{a}{a^2-b^2d} - \frac{b}{a^2-b^2d}\sqrt{d},$$

Finally $\left(\frac{a}{a^2-b^2d}\right), \left(-\frac{b}{a^2-b^2d}\right) \in Q$ and so $1/q \in Q[\sqrt{a}]$, and $Q(\sqrt{a})$ is a field.

2. First we show that ϕ is a homomorphism:

Let $x, y \in Q[\sqrt{d}]$.

$$
\begin{aligned}
\phi(x+y) &= \phi((a_1+a_2)+(b_1+b_2)\sqrt{d}) \\
&= (a_1+a_2)-(b_1+b_2)\sqrt{d} \\
&= (a_1-b_1\sqrt{d})+(a_2-b_2\sqrt{d}) \\
&= \phi(x)+\phi(y)
\end{aligned}
$$

$$
\begin{aligned}
\phi(xy) &= \phi((a_1+b_1\sqrt{d})(a_2+b_2\sqrt{d})) \\
&= \phi(a_1a_2+(a_1b_2+a_2b_1)\sqrt{d}+b_1b_2d) \\
&= \phi((a_1a_2+b_1b_2d)+(a_1b_2+a_2b_1)\sqrt{d}) \\
&= (a_1a_2+b_1b_2d)-(a_1b_2+a_2b_1)\sqrt{d} \\
&= a_1a_2-(a_1b_2+a_2b_1)\sqrt{d}+b_1b_2d \\
&= (a_1-b_1\sqrt{d})(a_2-b_2\sqrt{d}) \\
&= \phi(x)\cdot\phi(y).
\end{aligned}
$$

Furthurmore, consider any $q \in Q[\sqrt{d}]$ such that $\phi(q) = a - b\sqrt{d}$. Then, as $a \in Q$ and $(-b) \in Q$, $\phi(q) \in Q[\sqrt{d}]$ and so $\mathrm{Im}(\phi) = Q[\sqrt{d}]$, ϕ is surjective.

Finally consider $\phi(x) = \phi(y)$. Then

$$a_1 - b_1\sqrt{d} = a_2 - b_2\sqrt{d}.$$

~~But because $a_1 - b\sqrt{d} \in Q$ and $a_2 - b_2\sqrt{d} \in Q$,~~
~~then $a_1 - b_1\sqrt{d} = a_2 - b_2\sqrt{d}$~~ as Then $a_1 = a_2$ and $b_1 = b_2$, and so $x = a_1 + b_1\sqrt{d} = y = a_2 + a_2\sqrt{d}$
Thus ϕ is injective and an automorphism.

Homework 14

3a) Let $\alpha, \beta \in R$ such that

$\alpha = a + b\sqrt{d}$ and
$\beta = x + y\sqrt{d}$.

Then $\alpha \cdot \beta = (a+b\sqrt{d})(x+y\sqrt{d})$
$= ax + (ay+bx)\sqrt{d} + byd$.

We want to show that $N(\alpha \cdot \beta) = N(\alpha) N(\beta)$:

$$N(\alpha) = N(a+b\sqrt{d}) = a^2 - db^2$$

$$N(\beta) = N(x+y\sqrt{d}) = x^2 - dy^2$$

$$\begin{aligned} N(\alpha \cdot \beta) &= N(ax+byd+(ay+bx)\sqrt{d}) \\ &= (ax+byd)^2 - d(ay+bx)^2 \\ &= (ax)^2 + 2abxyd + (byd)^2 - d(ay)^2 \\ &\quad - 2abxyd - d(bx)^2 \\ &= (ax)^2 - (ay+bx)^2 d + (byd)^2 \end{aligned}$$

and finally

$$\begin{aligned} N(\alpha) \cdot N(\beta) &= (a^2 - db^2)(x^2 - dy^2) \\ &= (ax)^2 - d(bx)^2 - d(ay)^2 + (byd)^2 \\ &= (ax)^2 - (ay+bx)^2 d + (byd)^2 \\ &= N(\alpha \cdot \beta). \end{aligned}$$

3b) Suppose N did not have the property where $N(\alpha) = 0$ if and only if $\alpha = 0$.

Then there must exist some $r \in R$ where $r \neq 0$ and $N(r) = 0$. Thus

$$r = m + n\sqrt{d} \neq 0, \quad m, n \in \mathbb{Z} \text{ and}$$
$$N(r) = m^2 - dn^2 = 0, \quad m, n \in \mathbb{Z}.$$

Because $N(r) = 0$, either m and n are both zero (and thus $N(r) = 0 - 0$) or their terms ~~equ~~ cancel to give zero. Because we have stated that $r \neq 0$, the only possibility is the latter, and thus

$$m^2 - dn^2 = 0 \quad \Rightarrow m^2 = dn^2$$
$$\Rightarrow d = m^2/n^2.$$

However, this is a contradiction as d is an integer divisible by n^2 when $n \neq 1$ and d is an integer divisible by m^2 when $n = 1$. In both cases d violates being a square-free number, and so the assumption is false and $r = 0$.

Finally, consider $r = 0$; $m + n\sqrt{d} = 0$ can only be true when either m and n are both zero or when their terms cancel. However, similarly, $d = (-m/n)^2$ implies the same contradiction. Thus $N(\alpha) = 0$ if and only if $\alpha = 0$.

Homework 14

3c) Let $\alpha \in U(R)$. Then there exists some $\beta \in R$ such that $\alpha \cdot \beta = 1$ (β is also a unit in R). Now consider

$$N(1) = N(1 + 0\sqrt{d}) = 1^2 - d0^2 = 1.$$

Because $N(\alpha \cdot \beta) = N(\alpha) N(\beta)$ and $\alpha \cdot \beta = 1$, it must follow $N(\alpha) N(\beta) = 1$.

However, because $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ maps R to the integers, neither $N(\alpha)$ nor $N(\beta)$ can be a fractional inverse of the othere. Therefore both are 1, and hence for any unit α, $N(\alpha) = 1$.

For the other way, consider any $r \in R$ such that $N(r) = 1$. ~~Because Then for $r^{-1} \in R$, $N(r \cdot r^{-1}) = N(1) = 1$~~

Then $r = m + n\sqrt{d}$ has $m^2 - dn^2 = 1$.

~~But then~~

4a) The norm function of $\mathbb{Z}[\sqrt{-6}]$ is given by the following:

$N : \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z}$ where
$N(m+n\sqrt{-6}) = m^2 + 6n^2$.

But observe that the norms are always positive, as $m, n \in \mathbb{Z}$ and $m^2 \geq 0$ and $n^2 \geq 0$. Furthermore, because $\sqrt{2}$ and $\sqrt{3}$ are not integers, and because any addition of $6n^2$ for $n \in \mathbb{Z}$ is at least 6 or greater, neither 2 nor 3 can be in the image of N:

m \ n	0	±1	±2
0	0	6	24
±1	1	7	25
±2	4	10	28
	⋮		

[see how each sum is given by addition and can only increase]

4b) Observe that $6 \in \mathbb{Z}[\sqrt{-6}]$. For $\mathbb{Z}[\sqrt{-6}]$ to be a UFD, then, as $6 = 2 \times 3$ and $6 = (\sqrt{-6})(-\sqrt{-6})$, at least some of $2, 3, \pm\sqrt{-6}$ should reduce such that there is only one unique factorization.

4b) Consider the assumption that 2 is reducible. Then $2 = xy$ for some nonzero nonunit elements in $\mathbb{Z}[\sqrt{-6}]$. Given the norm function in part A:

$$N(2) = 2^2 + 6 \cdot 0^2 = 4$$

And given the properties in question 3:

$$\begin{aligned} N(x)N(y) &= N(xy) \\ &= N(2) \\ &= 4. \end{aligned}$$

Because neither x nor y are units, neither $N(x)$ nor $N(y)$ can be 1, and therefore $N(x) | 4$ but $N(x) \neq 1$ and $N(x) \neq 4$ (as this implies $N(y)=1$). Thus $N(x) = 2$, ~~and so $a^2 + 6b^2 = 2$ for some~~ which from part A is impossible. Thus 2 is irreducible.

Likewise consider $3 = xy$. Then

$N(3) = 3^2 = 9$ and similarly

$N(x) | 9$ but $N(x) \neq 1$ and $N(x) \neq 9$. Thus $N(x) = 3$ and from part A this is also impossible. Therefore $6 \in \mathbb{Z}[\sqrt{-6}]$ can be factorized in nonunique ways, as $2 \times 3 = 6$ is irreducible but $(\sqrt{-6})(-\sqrt{-6})$ is another solution. Hence $\mathbb{Z}[\sqrt{-6}]$ is not an UFD.

4c) $30 \in \mathbb{Z}[\sqrt{-30}]$ can be factorized as

$$30 = 2 \cdot 3 \cdot 5 \quad \text{and}$$

$$30 = (\sqrt{-30}) \cdot (-\sqrt{-30}).$$

By the same reasonings as in 4b, the norm function $N(a+b\sqrt{-30}) = a^2 + 30b^2$ does not have any reducible elements for 2, 3, or 5 as

$$a^2 + 30b^2 = 2$$
$$a^2 + 30b^2 = 3$$
$$a^2 + 30b^2 = 5$$

have no integer solutions. Therefore we must consider $\pm\sqrt{-30}$:

If $\pm\sqrt{-30}$ were reducible, then $\pm\sqrt{-30} = xy$ and similar to the integers

$$N(\pm\sqrt{-30}) = 30.$$

$N(x) \mid 30$ and $N(x) \neq 1$ and $N(x) \neq 30$, so $N(x)$ must be $2, 3, 5, 6, 10, 15$.

However for $a^2 + 30b^2$ these are all ~~possib~~ not possible as each is less than 30 and none are squares. Thus 30 has two factorizations of different lengths.

Homework 14

5a) Let $P \subseteq R$ be a nonzero prime ideal.

Because R is a PID, P is also a principle ideal, and therefore P is generated by a single element $p \in R$.

Now suppose P was not maximal, or

$$P \subseteq I \subseteq R \quad \text{for some } I < R.$$

Then, as both P and I are principle, for $P = (p)$ and $I = (i)$ it must follow $p \in I$, and so p must be generated by i. Therefore

$$ai = p \quad \text{for some } a \in R.$$

Because $p \in P$ and P is prime, then

$$ai \in P \iff a \in P \text{ or } i \in P.$$

If $i \in P$ then $P = I$ and thus P is maximal. However if $a \in P$, then by the same reasoning, a must be generated by p and thus

$$bp = a \quad \text{for some } b \in R.$$

Thus $p = ai = bpi$, and since R is commutative $p = bip$ and thus ~~b~~ is a unit.

Because $I = (i)$ and i is a unit,

$I = R$ and so P is also maximal.