Groups and Rings:
Solutions to Problem Sheet 6

Please email any questions or corrections to
hannah.tillmann-morris15@ic.ac.uk

December 2021

Question 1

Let $d < -1$ be an odd negative integer.

(a) Clearly 2 is not an invertible element of the ring $R := \mathbb{Z}[\sqrt{d}]$ since its inverse $\frac{1}{2}$ is not in R. We have to show that if $ab = 2$ for $a, b \in R$ then a or b is invertible in R.

Using the hint given in the question, consider the map $\varphi : R \to \mathbb{Z}_{\geq 0}$ given by $\varphi(m + n\sqrt{d}) = m^2 - n^2 d$. It's multiplicative - you can check that $\varphi((m + n\sqrt{d})(k + l\sqrt{d})) = \varphi(m + n\sqrt{d})\varphi(k + l\sqrt{d})$. Suppose for a contradiction that $2 = (m + n\sqrt{d})(k + l\sqrt{d})$ for some $n, m, k, l \in \mathbb{Z}$, where neither $m + n\sqrt{d}$ nor $k + l\sqrt{d}$ are invertible in R. Then, by the multiplicative property of φ, we have $\varphi(2) = 4 = (m^2 - n^2 d)(k^2 - l^2 d)$. Since both factors are positive integers, they are either equal to 1 and 4 or both equal to 2. If $m^{-}n^2 d = 1$, then $m + n\sqrt{d}$ is invertible in R as $(m + n\sqrt{d})(m - n\sqrt{d}) = 1$. So $m^2 - n^2 d$ must equal 2. m^2 and $-n^2 d$ are both positive integers, so either

1. $m^2 = 2$ and $-n^2 d = 0$. Clearly this can't be true since there's no integer m that squares to 2.
2. $m^2 = 0$ and $-n^2 d = 2$. Since n^2 is positive and can't equal 2, we must have $-d = 2$. This is a contradiction since d is odd.
3. $m^2 = 1$ and $-n^2 d = 1$. Since n^2 and $-d$ are both positive integers, they must both be 1. This is a contradiction since $d < -1$.

(b) Note $a = \frac{1-d}{2}$ is an integer since d is odd. If R were a unique factorisation domain, then since $2 \cdot a$ is a factorisation of $1 - d$ in R, with 2 irreducible, any other factorisation $\alpha \cdot \beta$ of $1 - d$ must have either $2|\alpha$ or $2|\beta$. But clearly 2 does not divide either $1 - \sqrt{d}$ or $1 + \sqrt{d}$.

Question 2

(a) R is clearly a subring of the field of complex numbers $\mathbb{C}$, and there are no zero divisors in $\mathbb{C}$. Alternatively, we could use the multiplicative property of φ again. Suppose $\exists x, y \in R$ such that $xy = 0$. Then $\varphi(xy) = \varphi(x)\varphi(y) = 0$. But $\varphi(x)$ and $\varphi(y)$ are integers, so one of them must be zero. $\varphi(x) = a^2 + b^2 = 0$ if and only if $a = b = 0$, i.e. $x = 0$.

(b) Suppose $r \in R^x$. Then $\exists s \in R$ such that $rs = 1$. Then $1 = \varphi(rs) = \varphi(r)\varphi(s)$, so $\varphi(r) = \varphi(s) = 1$ since they are both nonnegative integers whose product is 1.

(c) Clearly $\varphi(x) = 0$ iff $x = 0$ so φ is a function $R \to \mathbb{Z}_{\geq 0}$ such that

1. $\varphi(xy) \geq \varphi(x)$ for all $x, y \in R$.

   Indeed, $\varphi(xy) = \varphi(x)\varphi(y)$, and $\varphi(y) \geq 1$.

2. $\forall x, y \in R\ \exists q, r \in R$ such that $x = qy + r$ and either $r = 0$ or $\varphi(r) < \varphi(y)$.

   To prove this, we'll use the hint given in the question to approximate elements of $\mathbb{Q}(i)$ by elements of R. The point is, to get the remainder r as 'small' as possible (with respect to φ), we need to get the quotient q a close enough approximation to $\frac{x}{y}$.

   $\frac{x}{y}$ is in $\mathbb{Q}(i)$ so can be written as $u + vi$, where $u, v \in \mathbb{Q}$. So we need to pick $q = m + ni$ close enough to $u + vi$ such that

   $$\varphi(r) = \varphi(x - qy) = \varphi(y)\varphi\left(\frac{x}{y} - q\right) = \varphi(y)((u-m)^2 + (v-m)^2)$$

   is smaller than $\varphi(y)$. This can be achieved if $(u-m)^2 + (v-m)^2 < 1$. But we can pick $m \in (u - \frac{1}{2}, u + \frac{1}{2}) \cap \mathbb{Z}$ and $n \in (v - \frac{1}{2}, v + \frac{1}{2}) \cap \mathbb{Z}$, and then

   $$(u-m)^2 + (v-m)^2 < \frac{1}{4} + \frac{1}{4} < 1.$$

(d) Suppose that $\varphi(r) = p$ some prime number and $r = ab$ for some $a, b \in R$. Then $\varphi(r) = \varphi(a)\varphi(b) = p$, and since p is prime one of $\varphi(a)$ and $\varphi(b)$ is p and the other is 1. but in part (b) we showed that $\varphi(a) = 1$ if and only if a is a unit.

(e) Suppose for a contradiction that there are $a, b \in R \setminus R^\times$ such that $ab = p$. Then $\varphi(a)\varphi(b) = \varphi(p) = p^2$. But since neither a nor b is a unit, neither $\varphi(a)$ nor $\varphi(b)$ can equal 1, so $\varphi(a) = \varphi(b) = p$ since p is prime. But $p \equiv 3 \bmod 4$ and you can show that the sum of two squares is never congruent to 3 mod4. (Hint: show any square is congruent to either 0 or 1 mod4.)

Question 3

Question 3 is very similar to Question 2. Notice that φ is still the function that sends a complex number z to the square of its modulus $|z|^2 = z\bar{z}$.

(a) R is a subring of the field $\mathbb{C}$.

(b) φ is multiplicative and

$$r \in R^\times \quad \Longleftrightarrow \quad \varphi(r) = 1$$

still holds by the same argument as in Question 2(b). So the invertible elements of R are those with modulus 1 when considered as complex numbers. If you've noticed that ζ is a third root of unity, you can see that the elements of $R^\times$ are exactly the sixth roots of unity, ± 1, $\pm\zeta$ and $\pm\zeta^2$.

Alternatively, you could try to find the integer solutions to the equation

$$\varphi(a + b\zeta) = a^2 - ab + b^2 = 1.$$

Considering this as a quadratic equation for a in terms of b, it is easy to see from the discriminant $b^2 - 4(b^2 - 1)$ that there is a real solution a if and only if $b^2 \leq \frac{4}{3}$. But if b can only take values in $\mathbb{Z}$, then b must be 0, 1 or -1. Thus it is easy to check that the solutions (a, b) are

$$(\pm 1, 0),\ (0, \pm 1),\ (1, -1) \text{ and } (-1, 1).$$

(c) We use the same method as for Question 2(c), and approximate $\frac{x}{y} = u + v\zeta$, where $u, v \in \mathbb{Q}$ by some $q = m + n\zeta \in R$. This time the factor we need to bound, $\varphi(\frac{x}{y} - q)$, has the expression

$$(u - m)^2 - (u - m)(v - n) + (v - n)^2.$$

But as before, by picking $m \in (u - \frac{1}{2}, u + \frac{1}{2}) \cap \mathbb{Z}$ and $n \in (v - \frac{1}{2}, v + \frac{1}{2}) \cap \mathbb{Z}$, we get

$$\varphi\left(\frac{x}{y} - q\right) = (u - m)^2 - (u - m)(v - n) + (v - n)^2 < \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1.$$

(d) The exact same reasoning as for Question 2(d) holds.

(e) By the same reasoning as for Question 2, if $\exists x, y \in R$ such that $xy = p$, then $\varphi(x) = \varphi(y) = p$. But $p \equiv 2 \bmod 3$ and you can show that $a^2 - ab + b^2$ is never congruent to 2 mod3. (There are a finite number of cases to check.)

Question 4

From Problem Sheet 4 we know all elements of $\mathbb{H}$ have the form $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$, where $z, w \in \mathbb{C}$.

$$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}^2 = \begin{pmatrix} z^2 - \overline{w}w & zw + \overline{z}w \\ -z\overline{w} - \overline{z}\overline{w} & -\overline{w}w + \overline{z}^2 \end{pmatrix}$$

If z is purely imaginary, then $z + \overline{z} = 0$ and the two non-diagonal entries will be zero. We would also have $z^2 = \overline{z}^2$ and so to make the diagonal entries equal to -1, we can take any $w \in \mathbb{C}$ such that $|w|^2 = w\overline{w} = z^2 + 1$.

The fact that we've just found infinitely many elements of $\mathbb{H}$ which are roots of the polynomial $x^2 + 1$ does not contradict any theorem we know, since $\mathbb{H}$ is not a field.

Question 5

(a) To prove R is a ring you need to check the ring axioms. R is never an integral domain as long as neither R_1 nor R_2 are trivial: $(r_1, 0) \cdot (0.r_2) = (0, 0)$ for all $r_1 \in R_1$, $r_2 \in R_2$.

(b) Both projections are clearly surjective. To check each projection $\pi_i : R \longrightarrow R_i$ is a ring homomorphism, you need to check:

1. π_i is a homomorphism of additive groups.
2. $\pi_1((a, b) \cdot (c, d)) = \pi_1(a \cdot c, b \cdot d) = a \cdot c = \pi_1((a, b)) \cdot \pi_1((c, d))$, and similarly for pi_2.
3. $\pi_i(1_R) = \pi_i((1_{R_1}, 1_{R_2})) = 1_{R_i}$.

Question 6

(a) You need to check that

1. $I \cap J$ is an additive subgroup of R. This follows from the fact I and J are both additive subgroups of R.
2. If $x \in I \cap J$ and $r \in R$, then $rx \in I \cap J$. This is true because both I and J are ideals, so if $x \in I$ and $x \in J$, then $rx \in I$ and $rx \in J$ for any $r \in R$, and so $rx \in I \cap J$.

(b) Check that

1. IJ is an additive subgroup of R. 0_R is an element of both I and J so $0_R \cdot 0_R = 0_R \in IJ$. IJ is closed under addition since the sum of two finite sums $x_1y_1 + ... + x_ny_n$, $x'_1y'_1 + ... + x'_my'_m$ is another finite sum $x_1y_1 + ... + x_ny_n + x'_1y'_1 + ... + x'_my'_m$. Since I is closed under additive inverses $(-x)y = -xy \in IJ$ for any $xy \in IJ$.

2. For any $r \in R$ and $x_1y_1 + ... + x_ny_n \in IJ$, we have

$$r(x_1y_1 + ... + x_ny_n) = r(x_1y_1) + ... + r(x_ny_n) = (rx_1)y_1 + ... + (rx_n)y_n \in IJ.$$

(c) For any $x \in I$, $y \in J$, $xr \in I$ and $ry \in J$ for all $r \in R$. In particular $xy \in I$ and $xy \in J$, so $xy \in I \cap J$. We proved $I \cap J$ is an ideal, so we know it's closed under addition, and so any finite sum $x_1y - 1 + ...x_ny_n \in I \cap J$.

Let $R = \mathbb{Z}$ and $I = J = 2\mathbb{Z}$. Then $IJ = 4\mathbb{Z}$, which is a strict subset of $I \cap J = 2\mathbb{Z}$.

(d) You've seen in lectures that the maps $R \longrightarrow R/I$ and $R \longrightarrow R/J$ are homomorphisms of rings, with kernels I and J respectively. That $R/I \times R/J$ is a ring follows from Question 5 and the fact that f is a homomorphism follows by the definition of multiplcation and addition on the product ring. $f(a) = 0_{(R/I)\times(R/J)}$ if and only if $a + I = 0_{R/I} = I$ and $a + J = 0_{R/J} = J$, which is true if and only if $a \in I$ and $a \in J$, i.e. $a \in I \cap J$.

Question 7

(a) Suppose I and J are coprime, i.e. $I + J = R$. We already know from Question 6(c) that $IJ \subset I \cap J$, so it remains to show the other inclusion $I \cap J \in IJ$. Suppose $x \in I \cap J$. Since any $r \in R$ can be written as $r = a + b$ with $a \in I$ and $b \in J$, we have $1 = a + b$ in particular. So $x = x(a + b) = xa + xb$. Since R is commutative, $xa \in IJ$ and $xb \in IJ$, so $x = xa + xb \in IJ$.

(b) From Question 6(d) we know that $IJ = I \cap J$ is the kernel of $f : R \longrightarrow (R/I) \times (R/J)$, so f descends to an injective homomorphism $g : R/IJ \longrightarrow (R/I) \times (R/J)$. To show g is also surjective, it's enough to show f is surjective. Suppose $(x + I, y + J) \in (R/I) \times (R/J)$. We need to find some $r \in R$ such that $r + I = x + I$ and $r + J = y + J$. Again we use the fact that $1 = a + b$ for some $a \in I$, $b \in J$. Then $b = 1 - a$ and so $b + I = 1 + I$. Thus $bx + I = x + I$, and by the same reasoning $ay + J = y + J$. But $bx \in J$ and $ay \in I$ so $bx + ay + I = bx + I = x + I$ and $bx + ay + J = ay + J = y + J$.

(c) If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ are coprime in the usual integer sense of $(a, b) = 1$, then there exist $x, y \in \mathbb{Z}$ such that $1 = ax + by$. Thus 1 is an element of the ideal $a\mathbb{Z} + b\mathbb{Z}$, and therefore $R = a\mathbb{Z} + b\mathbb{Z}$. So the $a\mathbb{Z}$ and $b\mathbb{Z}$ are coprime in the sense of ideals, and the result follows from the previous part of the question.