Math 120 Homework 8 Solutions

May 26, 2018

Exercise 7.1.26. Let \( K \) be a field. A discrete valuation on \( K \) is a function \( \nu : K^\times \to \mathbb{Z} \) satisfying

(i) \( \nu(ab) = \nu(a) + \nu(b) \) (i.e. \( \nu \) is a homomorphism from the multiplicative group of nonzero elements of \( K \) to \( \mathbb{Z} \)),

(ii) \( \nu \) is surjective, and

(iii) \( \nu(x + y) \geq \min\{\nu(x), \nu(y)\} \) for all \( x, y \in K^\times \) with \( x + y \neq 0 \).

The set \( R = \{ x \in K^\times | \nu(x) \geq 0 \} \cup \{0\} \) is called the valuation ring of \( \nu \).

(a) Prove that \( R \) is a subring of \( K \) which contains the identity. (In general, a ring \( R \) is called a discrete valuation ring if there is some field \( K \) and some discrete valuation \( \nu \) on \( K \) such that \( R \) is the valuation ring of \( \nu \)). (b) Prove that for each nonzero element \( x \in K \) either \( x \) or \( x^{-1} \) is in \( R \). (c) Prove that an element \( x \) is a unit in \( R \) if and only if \( \nu(x) = 0 \).

Proof. (a) It suffices to check that \( R \) contains 1 and is closed under addition, additive inverses, and multiplication.

Since

\[ \nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1) \]

by property (i), it follows that \( \nu(1) = 0 \), so \( 1 \in R \).

Suppose \( a, b \in R \) are nonzero elements (if either are zero the sum is obviously in \( R \)), so that \( \nu(a) \geq 0 \) and \( \nu(b) \geq 0 \). We would like to show \( a + b \in R \). If \( a + b = 0 \), we know \( 0 \in R \) so we’re done. Otherwise,

\[ \nu(a + b) \geq \min\{\nu(a), \nu(b)\} \geq 0, \]

so \( a + b \in R \) as well. Thus \( R \) is closed under addition.

Suppose \( a \in R \) is nonzero. Note that

\[ 0 = \nu(1) = \nu(-1 \cdot -1) = \nu(-1) + \nu(-1) \]

by property (i), so \( \nu(-1) = 0 \). Thus,

\[ \nu(-a) = \nu(-1 \cdot a) = \nu(-1) + \nu(a) = \nu(a) \geq 0. \]

Thus, \( -a \in R \) and \( R \) is closed under additive inverses.

Finally, if \( a, b \in R \) are nonzero elements (if either are zero the product is zero), then \( \nu(a) \geq 0 \) and \( \nu(b) \geq 0 \), so

\[ \nu(ab) = \nu(a) + \nu(b) \geq 0, \]

and so \( ab \in R \) as well. This shows \( R \) is closed under multiplication and finishes the proof.

(b) We have

\[ \nu(x) + \nu(x^{-1}) = \nu(x \cdot x^{-1}) = \nu(1) = 0, \]

so at least one of \( \nu(x), \nu(x^{-1}) \) is nonnegative.

(c) If \( x \) is a unit, by definition its inverse \( x^{-1} \) also lies in \( R \). But by the calculation in part (b), \( \nu(x^{-1}) = -\nu(x) \) so if they’re both nonnegative then \( \nu(x) = 0 \). Conversely, if \( \nu(x) = 0 \), \( \nu(x^{-1}) = 0 \) as well so its inverse lies in \( R \) and \( x \) is a unit in \( R \).

Exercise 7.3.29*. Let \( R \) be a commutative ring. Recall (cf. Exercise 13, Section 1) that an element \( x \in R \) is nilpotent if \( x^n = 0 \) for some \( n \in \mathbb{Z}^+ \). Prove that the set of nilpotent elements form an ideal – called the nilradical of \( R \) and denoted by \( \mathfrak{n}(R) \).
Proof. We need to check two things.

First, if \(x, y \in R\) are nilpotent, we need to check that \(x + y\) is as well. If \(x^n = 0\) and \(y^n = 0\), check that every term of the binomial expansion of \((x + y)^{m+n-1}\) contains either a factor of \(x^m\) or \(y^n\), so \((x + y)^{m+n-1} = 0\) as well, and \(x + y\) is nilpotent.

Second, if \(x \in R\) is nilpotent and \(a \in R\) is any element, we need to check \(ax\) is nilpotent. But if \(x^n = 0\) then \((ax)^n = a^nx^n = 0\) since \(R\) is commutative, so we’re done. \(\square\)

Exercise 7.4.14(a,b,c,d)*. Assume \(R\) is commutative. Let \(x\) be an indeterminate, let \(f(x)\) be a monic polynomial in \(R[x]\) of degree \(n \geq 1\) and use the bar notation to denote passage to the quotient ring \(R[x]/(f(x))\).

(a) Show that every element of \((R[x]/(f(x)))\) is of the form \(p(x)\) for some polynomial \(p(x) \in R[x]\) of degree less than \(n\).

(b) Prove that if \(p(x)\) and \(q(x)\) are distinct polynomials of \(R[x]\) which are both of degree less than \(n\), then \(\overline{p(x)} \neq \overline{q(x)}\).

(c) If \(f(x) = a(x)b(x)\) where both \(a(x)\) and \(b(x)\) have degree less than \(n\), prove that \(\overline{a(x)}\) is a zero divisor in \(R[x]/(f(x))\).

(d) If \(f(x) = x^n - a\) for some nilpotent element \(a \in R\), prove that \(\overline{a}\) is nilpotent in \(R[x]/(f(x))\).

Proof. (a) Every element is certainly \(\overline{p(x)}\) for some polynomial \(p\). By the division algorithm for polynomials over a commutative ring, it is possible to write every \(p(x)\) as

\[
p(x) = q(x)f(x) + r(x)
\]

where \(r(x)\) has degree less than \(n\). Then \(\overline{p(x)} = \overline{r(x)}\), and every element of the quotient can be expressed this way.

(b) If \(\overline{p(x)} = \overline{q(x)}\), then \(p(x) - q(x) \in (f(x))\), which would imply that \(p(x) - q(x)\) is a multiple of \(f(x)\). But \(p(x) - q(x)\) has lower degree than \(f(x)\), so this is impossible.

(c) Simply note \(\overline{a(x)b(x)} = 0\), but \(a(x), b(x)\) are both nonzero by part (b).

(d) Since \(a\) is nilpotent in \(R\), there is \(m \in \mathbb{Z}^+\) for which \(a^m = 0\). Thus \(\overline{(a)m}n = \overline{(ax)m} = \overline{am} = 0\). \(\square\)

Question 0. Prove that the ideal \(I = (x^2 + 1)\) in \(\mathbb{R}[x]\) is maximal. (For maximum understanding, try to prove this with the same approach we used in class for the ideal \((x - 2, y - 3)\) in \(\mathbb{R}[x,y]\).)

Proof. Recall that an ideal is maximal iff quotienting by it results in a field. Consider the ring homomorphism \(\alpha : \mathbb{R}[x] \rightarrow \mathbb{C}\) which sends \(x \mapsto i\). Any element of \(\mathbb{C}\) is of the form \(a + bi\) where \(a, b \in \mathbb{R}\), so \(\alpha\) is surjective. It follows that \(\mathbb{R}[x]/\ker(\alpha) \simeq \mathbb{C}\), which is a field.

It remains to notice that \(\ker(\alpha) = I\). On the one hand, \(x^2 + 1 \mapsto i^2 + 1 = 0\), so \(I \subseteq \ker(\alpha)\). On the other hand, consider any polynomial \(p(x) \in \ker(\alpha)\). The map \(\alpha\) just evaluates \(p(x)\) at \(i\), so \(p(i) = 0\). But \(p\) is a real polynomial, so its roots come in conjugate pairs; therefore \(p(-i) = 0\) as well. Therefore, \(p(x)\) is divisible by the product \((x - i)(x + i) = x^2 + 1\), and \(p(x) \in I\), as desired.

Thus, \(I = \ker(\alpha)\) and \(\mathbb{R}[x]/I \simeq \mathbb{C}\) is a field, implying that \(I\) is maximal in \(\mathbb{R}[x]\). \(\square\)

Question 1. Let \(R \subset \mathbb{R}[x]\) be the subring of \(\mathbb{R}[x]\) consisting of polynomials whose coefficient of \(x\) is 0:

\[
R = \left\{ f(x) = a_0 + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{R} \right\}
\]

\[
\mathbb{R}[x] = \left\{ f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{R} \right\}
\]

You may use without proof that if \(g(x)\) and \(h(x)\) are polynomials in \(\mathbb{R}[x]\), then \(\deg(gh) = \deg(g) + \deg(h)\).

Exhibit an ideal \(I \subset R\) in \(R\) that is not principal, and justify your answer by proving that \(I\) is not a principal ideal of \(R\).

Proof. One such example is the ideal \(I = (x^2, x^3)\) = \{polynomials with no constant term\}. Suppose \(I\) were principal, i.e. \(I = (f)\). Then, since \(x^2 \in I\), \(x^2\) must be a multiple of \(f\), so \(\deg(f) \leq 2\).

If \(\deg(f) = 0\), then \(f\) is a nonzero constant and \((f) = R\), so \((f) \neq I\).

Also, no polynomials in \(R\) have degree 1. Thus, \(\deg(f) = 2\). But then since \(x^3 \in I\), we can write \(x^3 = f \cdot g\), for some other \(g \in R\). This implies that \(\deg(g) = \deg(x^3) - \deg(f) = 3 - 2 = 1\), which contradicts the fact that no polynomials in \(R\) have degree 1. Therefore, \(I\) cannot be principal. \(\square\)
**Question 2.** Let \( R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \).

(a) Find a prime ideal \( P_2 \subset R \) such that \( P_2 \cap \mathbb{Z} = 2\mathbb{Z} \).

(b) Find a prime ideal \( P_3 \subset R \) such that \( P_3 \cap \mathbb{Z} = 3\mathbb{Z} \).

(c) Find a prime ideal \( P_5 \subset R \) such that \( P_5 \cap \mathbb{Z} = 5\mathbb{Z} \).

Justify your answers. For each one, describe (as best you can) the domain \( R/P \).

**Proof.** Recall that to prove \( P \) is a prime ideal, it suffices to check that \( R/P \) is a domain.

(a) Take \( P_2 = (1 + i) \). It is easy to check that \( a + bi \in R \) lies in \( P_2 \) if \( a \equiv b \pmod{2} \). Thus \( R/P_2 \) contains exactly two elements \( 0 \) and \( 1 \). The unique such ring is \( \mathbb{Z}/2\mathbb{Z} \), which is a domain. This implies \( P_2 \) is prime.

The set \( P_5 \cap \mathbb{Z} \) will contain exactly those \( a + bi \) where \( a \equiv b \pmod{2} \) and \( b = 0 \), i.e. the even integers \( 2\mathbb{Z} \). We have shown that \( R/P \) consists of exactly these \( 9 \) distinct elements, and furthermore that all the nonzero ones are units. Thus \( R/P \) is a field, and \( P_3 \) must be prime. (Note, this field is not \( \mathbb{Z}/9\mathbb{Z} \), which is not even a domain).

It is easy to check that \( P_3 \cap \mathbb{Z} = 3\mathbb{Z} \).

(b) Take \( P_3 = (2 + i) \). The elements of \( R/P_3 \) can certainly be reduced mod 3 in both real and imaginary parts, so every element is of the form \( a + bi \) where \( a, b \in \{0, 1, 2\} \). Also, all of these elements are distinct. To see this, note that if two were the same in \( R/P_3 \), then their difference is also of the same form \( a + bi \) with not both of \( a, b \) zero, and their difference would be zero.

But if \( a, b \in \{1, 2\} \), then \( (a + bi)(-a + bi) = -a^2 - b^2 = -1 \), since \( 1^2 \equiv 2^2 \equiv 1 \pmod{3} \). Thus \( a + bi \) is a unit and therefore nonzero if \( a, b \in \{1, 2\} \).

The other case is if \( a = 0 \) or \( b = 0 \). If \( a = 0 \), then \( -b^2 = b^2 = 1 \) so \( bi \) is a unit. If \( b = 0 \), then \( \bar{a}^2 = 1 \) so \( a \) is a unit.

We have shown that \( R/P_3 \) consists of exactly these \( 9 \) distinct elements, and furthermore that all the nonzero ones are units. Thus \( R/P_3 \) is a field, and \( P_3 \) must be prime. (Note, this field is not \( \mathbb{Z}/9\mathbb{Z} \), which is not even a domain).

(c) Take \( P_5 = (2 + i) \). The elements of \( P_5 \) will be exactly those elements \( a + bi \) for which \( a \equiv 2b \pmod{5} \). We can therefore check that \( R/P_5 \) contains five distinct elements corresponding to the possible residue classes mod 5. The only ring on 5 elements is the field \( \mathbb{Z}/5\mathbb{Z} \), which shows that \( P_5 \) is prime, as desired.

It is easy to check that \( P_5 \cap \mathbb{Z} = 5\mathbb{Z} \). \( \square \)

**Question 3.** Construct a commutative ring \( L \) with the property that for every commutative ring \( R \),

\[
\text{the \# of ring homomorphisms } \varphi : L \rightarrow R \\
\text{is equal to } \text{the number of elements } r \in R \text{ satisfying } r^2 = 2.
\]

Note that “2” here means the element \( 1 + 1 \in R \). (You do not have to prove your answer is correct.)

**Proof.** The ring \( L \) is \( \mathbb{Z}[x]/(x^2 - 2) \). An alternative description of this ring is \( L = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \).

It suffices to construct a bijection between the sets

\[ \{ \text{ring homomorphisms } L \rightarrow R \} \]

and

\[ \{ \text{elements } r \in R \text{ satisfying } r^2 = 2 \} \].

Given an element of \( R \) satisfying \( r^2 = 2 \), let \( \varphi_r \) be the map which sends \( \pi \in L \) to \( r \). To check that this is a well-defined map, note that by Question 3 from Homework 7, there exists a ring homomorphism \( \psi_r : \mathbb{Z}[x] \rightarrow R \) which sends \( x \) to \( r \). The kernel of \( \psi_r \) contains \( x^2 - 2 \), since

\[ \psi_r(x^2 - 2) = r^2 - 2 = 0 \]

and so it contains the whole ideal \( (x^2 - 2) \). Thus, \( \psi_r \) induces a well-defined ring homomorphism \( \varphi_r : \mathbb{Z}[x]/(x^2 - 2) \rightarrow R \), which is the map we wanted.

Using Question 3 from Homework 7, we see that \( \varphi_r \) is also unique. Otherwise, given two maps \( \varphi_r, \varphi'_r : \mathbb{Z}[x]/(x^2 - 2) \rightarrow R \), they lift to ring homomorphisms \( \mathbb{Z}[x] \rightarrow R \) which both send \( x \) to the same element \( r \). Such a map is unique, so \( \varphi_r = \varphi'_r \).
It remains to check that every ring homomorphism $L \to R$ is one of the $\varphi_r$. In fact, if $\varphi : L \to R$ is a ring homomorphism, then $\varphi(\overline{r})$ must satisfy
\[
\varphi(\overline{r})^2 - 2 = \varphi(\overline{r}^2 - 2) = 0,
\]
so $\varphi$ always sends $\overline{r}$ to some $r$ for which $r^2 = 2$. For this $r$, $\varphi = \varphi_r$ by the uniqueness mentioned previously. \hfill \qed

**Question 4.** Construct a commutative ring $M$ with the property that for every commutative ring $R$,

\[
\text{the } \# \text{ of ring homomorphisms } \varphi : M \to R
\]

is equal to the number $|R^\times|$ of invertible elements in $R$.

Prove your answer is correct.

**Proof.** Take $M = \{ \sum_{k=-m}^n a_k x^k \mid m \geq 0, n \geq 0, a_k \in \mathbb{Z} \}$, the so-called ring of Laurent polynomials over $\mathbb{Z}$. In other words, every element of $M$ is $x^{-m} \cdot p(x)$ for some (regular) polynomial $p(x) \in \mathbb{Z}[x]$.

It suffices to construct a bijection between the sets
\[
\{ \text{ring homomorphisms } M \to R \}
\]
and
\[
\{ \text{invertible elements } r \in R \}.
\]

Given an invertible element $r \in R$, let $\varphi_r$ be the map which sends $x \in M$ to $r$ (and thus $x^{-1}$ to $r^{-1}$). A general element $x^{-n}p(x)$ will be sent to $r^{-n}p(r)$. This $\varphi_r$ is a ring homomorphism, preserving addition, negation, products, and the identity.

To see that given the image of $r$, $\varphi_r$ is uniquely determined, notice that for $\varphi_r$ to be a ring homomorphism,
\[
\varphi_r(\sum_{k=-m}^n a_k x^k) = \sum_{k=-m}^n a_k \varphi_r(x)^k = \sum_{k=-m}^n a_k r^k,
\]
so the images of all elements of $M$ are fixed once the image of $x$ is chosen.

It remains to check that every ring homomorphism $M \to R$ is one of the $\varphi_r$. In fact, if $\varphi : M \to R$ is a ring homomorphism, then $\varphi(x^{-1})\varphi(x) = \varphi(1) = 1$, so $\varphi(x)$ must be some invertible element $r \in R$. For this $r$, $\varphi = \varphi_r$ by the uniqueness mentioned previously. \hfill \qed

**Question 5.** Can there exist a commutative ring $N$ with the property that for every commutative ring $R$,

\[
\text{the } \# \text{ of ring homomorphisms } \varphi : N \to R
\]

is equal to the number of elements $r \in R$ such that both $r$ and $1-r$ are units.

Either construct such a ring and prove that your answer is correct (at least outline a proof), or prove that no such ring can exist.

**Proof.** Take
\[
N = \{ f(x) = x^k (1-x)^\ell p(x) \mid k \in \mathbb{Z}, \ell \in \mathbb{Z}, p(x) \in \mathbb{Z}[x] \text{ satisfies } p(0) \neq 0, p(1) \neq 0 \}.
\]

This is similar to the ring $M$ in Question 4 except that we additionally allow for negative powers of $(1-x)$. The tricky part about proving $N$ is a ring is showing that it is closed under addition. If $f(x) = x^k (1-x)^\ell p(x)$ and $g(x) = x^{k'} (1-x)^{\ell'} q(x)$, then define $k_0 = \min(k, k')$, $\ell_0 = \min(\ell, \ell')$, and check that
\[
f(x) + g(x) = x^{k_0}(1-x)^{\ell_0}(x^{k-k_0}(1-x)^{\ell-\ell_0}p(x) + x^{k'-k_0}(1-x)^{\ell'-\ell_0}q(x)),
\]
where the polynomial in the parentheses is an honest polynomial. However, it may vanish at $x$ and/or $1-x$; in this case, factor out a finite number of factors of $x$ and $1-x$, until this is no longer the case.
It suffices to construct a bijection between the sets
\[ \{ \text{ring homomorphisms } N \to R \} \]
and
\[ \{ \text{elements } r \in R \text{ for which } r, 1-r \text{ are both units} \}. \]

Given \( r \in R \) such that \( r, 1-r \) are both units, let \( \varphi_r \) be the map which sends \( x \in N \) to \( r \). Again, for \( \varphi_r \) to be a ring homomorphism and \( \varphi_r(x) = r \), it must be the unique "evaluation at \( r \)" map which sends
\[ \varphi_r(x^k(1-x)^fp(x)) = r^k(1-r)^fp(r). \]

It remains to check that every ring homomorphism \( N \to R \) is one of the \( \varphi_r \). In fact, if \( \varphi : N \to R \) is a ring homomorphism, then \( \varphi(x^{-1})\varphi(x) = \varphi(1) = 1 \), so \( \varphi(x) \) must be some invertible element \( r \in R \). Also \( \varphi((1-x)^{-1})\varphi(1-x) = \varphi(1) = 1 \), so \( \varphi(1-x) = 1-r \) is also invertible. For this \( r, \varphi = \varphi_r \) by the uniqueness mentioned previously. \( \square \)

In Question 6, you can use the following fact, which we will prove later in the course:

If \( G \) is a finitely generated abelian group, then every subgroup of \( G \) is finitely generated.

(This is false if \( G \) is a finitely generated nonabelian group, as you proved for \( G = F_2 \) in Q5B on HW3.)

**Question 6.** Given a complex number \( z \in \mathbb{C} \), let \( A(z) \) denote the additive subgroup of \( \mathbb{C} \) generated by the positive powers \( 1, z, z^2, z^3, \ldots \) under addition.

For example, \( A(2) = \{ 1, 2, 4, 8, \ldots \} = \mathbb{Z} \), whereas \( A(\frac{2}{3}) = \{ 1, \frac{2}{3}, \frac{4}{3}, \frac{8}{3}, \ldots \} = \{ \frac{2^k}{3^k} \in \mathbb{Q} \} \).

A complex number \( z \in \mathbb{C} \) is called integral if \( A(z) \) is finitely generated as a group under addition.

**Question 6(a)**. Prove that a rational number \( x \in \mathbb{Q} \) is integral if and only if \( x \in \mathbb{Z} \).

**Proof.** If \( x \in \mathbb{Z} \), then \( A(x) \) is just \( \mathbb{Z} \), so it is finitely generated.

If \( x \in \mathbb{Q} \) is integral, then \( A(x) \) is a finitely generated subgroup of \( \mathbb{Q} \). We showed as a corollary of an earlier homework that the finitely generated subgroups of \( \mathbb{Q} \) are exactly the singly generated subgroups of \( \frac{\mathbb{Z}}{n\mathbb{Z}} \). Thus, for \( x \) to be integral, all of its powers must be integer multiples of a single rational number \( \frac{m}{n} \). This is impossible if \( x \notin \mathbb{Z} \). \( \square \)

**Question 6(b).** Describe exactly which elements of \( \mathbb{Q}(i) \) are integral. (Recall that \( \mathbb{Q}(i) = \{ a + bi \mid a, b \in \mathbb{Q} \} \).

**Proof.** The elements are those in \( \mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \} \).

For any \( z = a + bi \in \mathbb{Z}[i] \), note that \( A(z) \) will be a subgroup of \( \mathbb{Z}[i] \) under addition, which is isomorphic as an abelian group to \( \mathbb{Z} \times \mathbb{Z} \). But any subgroup of \( \mathbb{Z} \times \mathbb{Z} \) is finitely generated (using e.g. the fact in the beginning). Thus \( z \) is integral.

For the other direction, we will use the following version of Gauss’ Lemma. Define the content \( C(p) \) of a polynomial \( p \in \mathbb{Z}[x] \) to be the greatest common divisor of its coefficients.

**Lemma 1.** For any two polynomials \( p(x), q(x) \in \mathbb{Z}[x] \),
\[ C(p)C(q) = C(pq). \]

**Proof.** Because \( C(p) \) divides all the coefficients of \( p \) and \( C(q) \) divides all the coefficients of \( q \), \( C(p)C(q) \) divides all the coefficients of \( pq \), so \( C(p)C(q))C(pq) \).

Dividing \( p \) by \( C(p) \) and \( q \) by \( C(q) \) we may assume \( C(p) = C(q) = 1 \). It remains to show that in this case, \( C(pq) = 1 \). Write \( p(x) = \sum_i a_ix^i \) and \( q(x) = \sum_j b_jx^j \).

Otherwise, there is a prime \( r \) which divides all of the coefficients of \( pq \), but not all the coefficients of \( p \) or \( q \). Let \( a_i x^i \) and \( b_j x^j \) be the smallest degree monomials in \( p, q \) respectively for which \( r \not| \ a_i \) and \( r \not| \ b_j \). Then, the coefficient of \( x^{i+j} \) in \( pq \) is
\[ \sum_{k=0}^{i+j} a_kb_{i+j-k}x^{i+j-k}, \]
and every term except \( a_i x^i b_j x^j \) has a coefficient which is divisible by \( r \). But \( a_i b_j \) is not divisible by \( r \), so this implies that the whole coefficient of \( x^{i+j} \) in \( pq \) is not divisible by \( r \), a contradiction. Thus \( C(pq) = 1 \). \( \square \)
Now suppose $z \in \mathbb{Q}[i]$ is not in $\mathbb{Z}[i]$, but $A(z)$ is finitely generated. Since every element of $A(z)$ can be written as a finite integer linear combination of its generators $1, z, z^2, \ldots$, the finite set of generators can all be written this way too. Thus, $A(z)$ has a finite set of generators which are integer polynomials of $z$.

It follows that there is some smallest $n \geq 1$ for which $A(z)$ is generated by $1, z, z^2, \ldots, z^{n-1}$.

In particular, $z^n$ can be written as an integer linear combination $z^n = a_{n-1}z^{n-1} + \cdots + a_0$ of the previous generators. Define $p(x) = x^n - a_{n-1}z^{n-1} - \cdots - a_0$, so that $z$ is a root of this polynomial. Since $p$ has real coefficients, $z$ is also a root of $p$, so $p$ is divisible by the polynomial $q(x) = (x-z)(x-\bar{z})$. We can write $z = (a+bi)/c$ in simplest terms, where $c \geq 2$ shares no factors with both $a$ and $b$, then

$$q(x) = x^2 - \frac{2a}{c}x + \frac{a^2 + b^2}{c^2}$$

is a polynomial with rational coefficients. The quotient $r(x) = p(x)/q(x)$ will also be a polynomial with rational coefficients. In addition, $p(x)$ and $q(x)$ both have leading coefficient 1, so $r(x)$ does as well.

There exist integers $A, B$ for which $Aq(x) \in \mathbb{Z}[x]$ and $Br(x) \in \mathbb{Z}[x]$, clearing the denominators of $r$ and $q$. Then, $ABp = (Aq)(Br)$, so by Lemma 1,

$$C(ABp) = C(Aq)C(Br).$$

The left hand side is exactly $AB$, since $p \in \mathbb{Z}[x]$ to begin with and had leading coefficient 1. But the leading coefficient of $Aq$ is $A$ and the leading coefficient of $Br$ is $B$, so the right hand side is at most $AB$. For it to be exactly $AB$, both $C(Aq) = A$ and $C(Br) = B$ must be the case.

Therefore, $C(Aq) = A$ and $q \in \mathbb{Z}[x]$ to begin with. In particular, $c|2a$ and $c^2|a^2 + b^2$. If $\gcd(a,c) \neq 1$, then $\gcd(a,c)^2|a^2 + b^2$, and $\gcd(a,c)^2|a^2$, so $\gcd(a,c)^2|b^2$, and $a, b, c$ have a common factor, contradicting our assumption that $z$ was written in simplest terms.

Thus, $\gcd(a,c) = 1$, which together with $c|2a$ implies that $c = 2$ and $a$ is odd. Otherwise, $c = 2$ and $4 = c^2|a^2 + b^2$. But $a^2 \equiv 1 \pmod{4}$ and $b^2$ is either 0 or 1 (mod 4), so this is impossible. We have thus proved that $z \in \mathbb{Z}[i]$.

**Question 6(c).** Describe exactly which elements of $\mathbb{Q}(\sqrt{3})$ are integral. (Recall that $\mathbb{Q}(\sqrt{3}) = \{a+b\sqrt{3} \mid a, b \in \mathbb{Q}\}$.)

**Proof.** The answer is $\{a+b\sqrt{3} \mid a, b \in \mathbb{Z}\}$.

The situation is similar to 6(b), replacing $i$ by $\sqrt{3}$. For showing that elements of this set are integral, check that $\mathbb{Z}[\sqrt{3}] \simeq \mathbb{Z} \times \mathbb{Z}$ as an abelian group.

In the other direction, we may again assume that $z \in \mathbb{Q}(\sqrt{3})$ and $z$ is integral, so $z$ is the zero of some polynomial of the form $p(x) = x^n - a_{n-1}z^{n-1} - \cdots - a_0$.

Any such element $z$ not in $\mathbb{Z}[\sqrt{3}] = \{a+b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ can be written in simplest terms as $(a+b\sqrt{3})/c$ where $\gcd(a,b,c) = 1$ and $c \geq 2$. Then, $z$ is also the zero of a quadratic

$$q(x) = x^2 - \frac{2a}{c}x + \frac{a^2 - 3b^2}{c^2}$$

with rational coefficients. Repeating the argument in 6(b), $q(x)|p(x)$, so $q(x)$ has integer coefficients. Therefore, $c|2a$ and $c^2|a^2 - 3b^2$. The first condition again implies that $c = 2$ and $a$ is odd. The second is then impossible by the same argument as before, because $a^2 - 3b^2 \equiv a^2 + b^2 \pmod{4}$ can never be divisible by $c^2 = 4$.

**Question 6(d).** Describe exactly which elements of $\mathbb{Q}(\sqrt{5})$ are integral. (Recall that $\mathbb{Q}(\sqrt{5}) = \{a+b\sqrt{5} \mid a, b \in \mathbb{Q}\}$.)

**Proof.** The answer is $\{a+b\frac{\sqrt{5}}{2} \mid a, b \in \mathbb{Z}, a + b \equiv 0 \pmod{2}\}$.

The situation is similar 6(b) and (c), replacing $i$ by $\frac{1+\sqrt{5}}{2}$. For showing that the elements above are indeed integral, check that $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] \simeq \mathbb{Z} \times \mathbb{Z}$ as an abelian group.

In the other direction, we may again assume that $z \in \mathbb{Q}(\sqrt{5})$ and $z$ is integral, so $z$ is the zero of some polynomial of the form $p(x) = x^n - a_{n-1}z^{n-1} - \cdots - a_0$. 

6
Any such element $z$ can be written in simplest terms as $(a + b\sqrt{5})/c$ where $\gcd(a, b, c) = 1$ and $c \geq 2$. Then, $z$ is also the zero of a quadratic

$$q(x) = x^2 - \frac{2a}{c}x + \frac{a^2 - 5b^2}{c^2}$$

with rational coefficients. Repeating the argument in 6(b), $q(x)|p(x)$, so $q(x)$ has integer coefficients. Therefore, $c|2a$ and $c^2|a^2 - 5b^2$. The first condition implies $c = 2$ and $a$ is odd. The second implies that $b$ is also odd. This shows that the integral elements of $\mathbb{Q}(\sqrt{5})$ are either elements of $\mathbb{Z}[\sqrt{5}]$, or can be written as $(a + b\sqrt{5})/2$, where $a, b$ are both odd. This is exactly the set described.

\[\Box\]

**Question 6(e).** Let $x \in \mathbb{C}$ be an integer element, and let $y \in \mathbb{C}$ be an $n$th root of $x$ (meaning $y^n = x$). Prove that $y$ is integral.

**Proof.** Notice that $A(y)$ is contained in the union of the $n$ sets $A(x), yA(x), \ldots, y^{n-1}A(x)$. This is because every generator $y^m$ of $A(y)$ can be written as $y^{rn} = x^r$ where $r \leq n - 1$. If $g_1, \ldots, g_m$ are a finite set of generators for $A(x)$, then the set of $mn$ elements $y^i g_j$, $0 \leq i \leq n - 1$, $1 \leq j \leq m$, generate $A(y)$.

\[\Box\]

**Question 6(f).** Prove that if $x \in \mathbb{C}$ and $y \in \mathbb{C}$ are both integral, then $x + y$ and $xy$ are integral. Conclude that the set $A \subset \mathbb{C}$ of all integral elements of $\mathbb{C}$ forms a subring of $\mathbb{C}$.

**Proof.** Let $A(x, y)$ be the additive subgroup of $\mathbb{C}$ spanned by $x^iy^j$ for $i, j \geq 0$.

If $A(x)$ is finitely generated by $g_1, \ldots, g_m$ and $A(y)$ is finitely generated by $h_1, \ldots, h_n$, then $A(x, y)$ is finitely generated by the $mn$ products $g_i h_j$ for $1 \leq i \leq n$, $1 \leq j \leq m$. To see this, any product $x^iy^j$ can be written as an integer linear combination of $g_i h_j$ by writing $x^i$ as an integer linear combination of the $g_i$ and $y^j$ as an integer linear combination of the $h_j$.

Now simply observe that $A(x + y)$ and $A(xy)$ are both contained in $A(x, y)$, so using the remark, each is finitely generated. Note that $A(-x) = A(x)$ so $A$ is closed under negation as well. Thus the ring of integral elements of $\mathbb{C}$ forms a subring of $\mathbb{C}$.

\[\Box\]

**Question 6(g).** Describe exactly which elements of $\mathbb{Q}(\sqrt{2})$ are integral. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} + c\sqrt{2}^2 : a, b, c \in \mathbb{Z}\}$.

**Proof.** The answer is $\{a + b\sqrt{2} + c\sqrt{2}^2 : a, b, c \in \mathbb{Z}\}$.

\[\Box\]

**Question 6(h).** Describe which elements of $\mathbb{Q}(\sqrt{10})$ are integral. $\mathbb{Q}(\sqrt{10}) = \{a + b\sqrt{10} + c\sqrt{10}^2 : a, b, c \in \mathbb{Z}\}$.

**Proof.** The answer is $\{a + b\sqrt{10} + c\sqrt{10}^2 : a, b, c \in \mathbb{Z}, a + b + c \equiv 0 \mod 3\}$, but proving this is quite difficult.

\[\Box\]

**Question 6(i).** Prove that $z = 2 \cos(\frac{2\pi}{n})$ is integral for any $n \in \mathbb{N}$.

**Proof.** This can be done directly using trigonometric identities. Alternately, let $w = \cos(\frac{2\pi}{n}) + \sin(\frac{2\pi}{n})i$. De Moivre’s formula says that

$$w^n = \cos(n \cdot \frac{2\pi}{n}) + \sin(n \cdot \frac{2\pi}{n})i = \cos(2\pi) + \sin(2\pi)i = 1.$$ 

Therefore Q6(e) tells us that $w$ is integral, since it is an $n$th root of 1 which is definitely integral, so $A(w)$ is a finitely generated abelian group. Since $z = 2 \cos(\frac{2\pi}{n}) = w + w^{n-1}$ we see that $z \in A(w)$ and thus $A(z) \subset A(w)$. Using the italicized remark above, we conclude that $A(z)$ is finitely generated.

\[\Box\]

**Question 6(j).** For $z = 2 \cos(\frac{2\pi}{n})$, the group $A(z)$ is isomorphic to $\mathbb{Z}_k$ for some $k = k(n)$ depending on $n$. Compute the rank $k(n)$ for $n = 3, 4, 5, 6, 7$. Can you express the rank $k(n)$ as a function of $n$?

**Proof.** The rank $k(n)$ for $n = 3, 4, 5, 6, 7$ is: $k(3) = 1, k(4) = 1, k(5) = 2, k(6) = 1, k(7) = 3$. For general $n$, the rank is given by $k(n) = \varphi(n)/2$.

\[\Box\]