Homework 7 – Algebraic Structures

Ch 11: 1.1, 1.2, 1.3, 1.8, 2.1, 3.1, 3.2, 3.3(a, d), 3.5, 3.6, 3.8, 3.12, 3.13

Blake Griffith

Pre-lect:

Exercise (11.1.1)**.** *Prove that* $7+2^{1/3}$ *and* $\sqrt{3}+\sqrt{-5}$ *are algebraic numbers.*

Proof. Recall that a number x is *algebraic* if it is the solution to the equation $0 = a_n x^n + \cdots + a_1 x + a_0$ for any set of a's in $\mathbb{Z}$.

So we must construct a polynomial for which the given numbers are roots.

For if we consider $7 + 2^{1/3}$ as the expression $x + y^{1/3}$ we would want to construct a polynomial which has no terms with the non-integer powers of y eliminated which yields an integer we can then choose a_0 to be minus this integer.

Consider

$$(x + y^{1/3})^3 = x^3 + 3x^2y^{1/3} + 3xy^{2/3} + y$$

So we can choose the a_2 term to be $-3x = -21$ giving

$$(x + y^{1/3})^3 - 3x(x + y^{1/3})^2 = -2x^3 - 3x^2y^{1/3} + y$$

So no we can choose the a_1 term to be $3x^2 = 147$ giving

$$(x + y^{1/3})^3 - 3x(x + y^{1/3})^2 + 3x^2(x + y^{1/3}) = x^3 + y$$

We then choose a_0 to be $x^3 + y = 345$. So $7 + 2^{1/3}$ is algebraic because it is the root of the polynomial $y = x^3 - 21x^2 + 147x + 345$.

For the next part let $x = \sqrt{3} + \sqrt{-5}$ then:

$$x = \sqrt{3}+\sqrt{-5} \implies x^2 = -2+2\sqrt{-15} \implies (x^2+2)^2 = (2\sqrt{15})^2 \implies x^4+4x^2+64 = 0$$

So $\sqrt{3} + \sqrt{-5}$ is algebraic because it is the root of the equation $y = x^4 + 4x^2 + 64$.

$\square$

Exercise (11.1.2)**.** *Prove that, for* $n \neq 0$, $\cos 2\pi/n$ *is an algebraic number.*

Proof. Notice recall by Euler's theorem

$$1 = \left(e^{2\pi i/n}\right)^n = (\cos 2\pi/n + i \sin 2\pi/n)^n)$$

Then applying the binomial theorem we have

$$1 = \sum_{j=0}^{n} \binom{n}{j} \cos{(2\pi/n)}^{n-j} \sin{(2\pi/n)}^j i^j$$

But the LHS is real, so the imaginary terms, which are where j is odd, sum to zero. So we can rewrite the sum with just the even j letting $j \to 2k$ as

$$1 = \sum_{k=0}^{m} \binom{n}{2k} \cos{(2\pi/n)}^{n-2k} \sin{(2\pi/n)}^{2k}$$

where $m = \text{floor } (n/2)$. Now we can rewrite the sine term using trig identity $\sin{(x)}^2 = 1 - \cos{(x)}^2$.

$$1 = \sum_{k=0}^{m} \binom{n}{2k} \cos{(2\pi/n)}^{n-2k} (1 - \cos{(2\pi/n)}^2)^k$$

Now letting $\cos 2\pi/n = x$ we see the polynomial

$$y = -1 + \sum_{k=0}^{m} \binom{n}{2k} x^{n-2k} (1 - x^2)^k$$

has the desired root, so $\cos 2\pi/n$ is algebraic.

$\square$

Exercise (11.1.3)**.** *Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing the rational numbers $\mathbb{Q}$ and the elements $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. Let $\gamma = \alpha + \beta$. Is $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$? Is $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\gamma]$?*

Proof. Note that $\mathbb{Q}[\alpha + \beta]$ contains

$$(1/3)(\alpha + \beta)^3 - 3(\alpha + \beta) = \sqrt{2}$$
$$(-1/3)(\alpha + \beta)^3 + 11/3(\alpha + \beta) = \sqrt{3}$$

So α and β are in $\mathbb{Q}[\alpha + \beta]$. So $\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{Q}[\alpha + \beta]$.

The other containment follows since $\alpha + \beta \in \mathbb{Q}[\alpha, \beta]$ and $\mathbb{Q}[\alpha + \beta]$.

So $\mathbb{Q}[\alpha + \beta] = \mathbb{Q}[\alpha, \beta]$.

But through trial and error I could not construct a polynomial in $\mathbb{Z}[\alpha + \beta]$ that equals α or β. So no, $\mathbb{Z}[\alpha, \beta]$ does not equal $\mathbb{Z}[\gamma]$.

$\square$

Exercise (11.1.8). *Determine the units in*

1. $\mathbb{Z}/12\mathbb{Z}$
2. $\mathbb{Z}/8\mathbb{Z}$
3. $\mathbb{Z}/n\mathbb{Z}$

Proof. Recall a *unit* is a element of a ring that has a multiplicative inverse.

1. The set of units in $\mathbb{Z}/12\mathbb{Z}$ is $\{1, 2, 3, 4, 6, 8, 9, 10\}$.
2. The set of units in $\mathbb{Z}/8\mathbb{Z}$ is $\{1, 2, 4, 6\}$.
3. The pattern in the previous two problems indicates that elements which are coprime to the order of the quotient group are *not* units. This is reasonable, if we consider a number q that does not divide n. Then the smallest number multiplied with p that is congruent to 1 is $\text{LCM}(q, n)$. But since q does not divide n this is qn. However there are only elements in the ring less than n, so q cannot be a unit.

   So the units are $\mathbb{Z}/n\mathbb{Z} - \phi(n)$. Where ϕ is Euler's totient function.

$\square$

Exercise (11.2.1). *For which positive integers n does $x^2 + x + 1$ divide $x^4 + 3x^3 + x^2 + 7x + 5$ in $[\mathbb{Z}/(n)][x]$?*

Proof. Carrying out the division algorithm we find a result in the form $p = qk + r$ is

$$x^4 + 3x^3 + x^2 + 7x + 5 = (x^2 + x + 1)(x^2 + 2x - 2) + (7x + 7)$$

The remainder here is $7x + 7$ which is zero if we choose $n = 7$.

$\square$

Exercise (11.3.1)**.** *Prove that an ideal of a ring R is a subgroup of the additive group R^+.*

Proof. Suppose we have some ideal $I = (a_1, \ldots, a_n)$ of R.

First, I is contained in R since $I = (a_1, \ldots, a_n) = \{a_1 r_1 + \cdots + a_n r_n | r_i \in R\}$, and all $a_i \in R$. Since I is in R we can consider it as part of R^+.

By definition I contains all linear combinations of $a_i r_i$, since elements of the form $a_i r_i$ are elements of R^+, linear combinations of such elements are also in R^+. So I is closed under addition.

I contains inverses. Consider an arbitrary element of the ideal $r_1 a_1 + \cdots + r_n a_n$. Since R contains inverse elements under addition, we can also construct the element $-r_1 a_1 - \cdots - r_n a_n$. Which is the inverse of $r_1 a_1 + \cdots + r_n a_n$.

I contains the additive identity 0. Since zero can be written as a linear combination. i.e. $a_1 r_1 - a_1 r_1 = 0$ where $a_1 \in I$ and $r_1, -r_1 \in R$.

$\square$

Exercise (11.3.2)**.** *Prove that every nonzero ideal in the ring of Gauss integers contains a nonzero integer.*

Proof. Consider the ideal generated by some integer a in the Gauss integers. If a is positive and real we are done since the ideal must contain a.

If a is negative and real. Then recall that the ideal is a subgroup of the elements of the ring under addition. So it contains additive inverses of each element. The additive inverse of a negative element is positive. So the ideal contains $-a$, a positive element.

If a is complex then it's conjugate $\bar{a}$ is in the Gauss integers so $\bar{a}a$ is in the ideal and it is real. By the above arguments a real integer element in the ideal always implies a real positive integer element in the ideal.

$\square$

Exercise (11.3.3 a and d)**.** *Find the generators for the kernels of the following maps:*

1. *$\mathbb{R}[x, y] \to \mathbb{R}$ defined by $f(x, y) \rightsquigarrow f(0, 0)$*
2. *$\mathbb{Z}[x] \to \mathbb{C}$ defined by $x \rightsquigarrow \sqrt{2} + \sqrt{3}$*

Proof. Recall that the kernel of the map is the ideal generated by the elements that are sent to zero.

1. The kernel is the ideal (x, y).
2. The kernel is the ideal $(x - \sqrt{2} - \sqrt{3})$.

$\square$

Exercise (11.3.5)**.** *The derivative of a polynomial f with coefficients in a field F is defined by the calculus formula $(a_n x^n + \cdots + a_1 x + a_0)' = n a_n x^{n-1} + \cdots + 1a_1$. The integer coefficients are interpreted in F using the unique homomorphism $\mathbb{Z} \to F$.*

1. *Prove the product rule $(fg)' = f'g + fg'$ and the chain rule $(f \circ g)' = (f' \circ g)g'$.*
2. *Let α be an element of F. Prove that α is a multiple root of a polynomial f if and only if it is a common root of f and of its derivative f'.*

Proof. 1. To prove the product rule let $f = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ and $g = b_m x^m + \ldots b_2 x^2 + b_1 x + b_0$. Then we have

$$\begin{aligned}
&f' = n a_n x^{n-1} + \ldots 2a_2 x + a_1 \\
&g' = m b_m x^{m-1} + \ldots 2b_2 x + b_1 \\
&f'g = n a_n b_m x^{m+n-1} + \cdots + (2a_2 b_0 + a_1 b_1)x + a_1 b_0 \\
&fg' = m a_n b_m x^{m+n-1} + \ldots (2a_0 b_2 + a_1 b_1)x + a_0 b_1
\end{aligned}$$

combining these

$$f'g + fg' = (n+m) a_n b_m x^{m+n-1} + \cdots + 2(a_0 b_2 + a_1 b_1 + a_2 b_0)x + a_0 b_1 + a_1 b_0$$

Now consider $(fg)'$

$$\begin{aligned}
[fg]' &= [(a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0)(b_m x^m + \cdots + b_2 x^2 + b_1 x + b_0)]' \\
&= [a_n b_m x^{m+n} + \cdots + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + (a_0 b_1 + a_1 b_0)x + a_0 b_0]' \\
&= (n+m) a_n b_m x^{m+n-1} + \cdots + 2(a_0 b_2 + a_1 b_1 + a_2 b_0)x + a_0 b_1 + a_1 b_0
\end{aligned}$$

Clearly $(fg)' = f'g + fg'$

2. ...

□

Exercise (11.3.6)**.** *An automorphism of a ring R is an isomorphism from R to itself. Let R be a ring. And let $f(y)$ be a polynomial in one variable with coefficients in R. Prove that the map $R[x,y] \to R[x,y]$ defined by $x \rightsquigarrow x + f(y)$, $y \rightsquigarrow y$ is an automorphism of $R[x,y]$.*

Proof. Recall for a map to be an automorphism it must be a bijection from the ring to itself. By definition we see that the map ϕ is from R to itself, so we must show that it is a bijection.

To see the map is surjective, consider an element $r(x,y)$ in the codomain $R[x,y]$, then the element $r(x - f(y), y)$ maps to this with the given map.

Recall that the map ϕ is injective if and only if $\ker \phi = \{0\}$. I cannot construct a non-zero kernel for this map. So I claim $\ker \phi = \{0\}$. So the map is injective.

□

Exercise (11.3.8)**.** *Let R be a ring of prime characteristic p. Prove that the map $R \to R$ defined by $x \rightsquigarrow x^p$ is a ring homomorphism. (It is called the Frobenius map.)*

Proof. Recall for a map $\phi : R \to R'$ to be a ring homomorphism it must satisfy for $a, b \in R$.

$$\phi(a+b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b), \quad \text{and} \quad \phi(1) = 1$$

For the Frobenius map we obviously have th last condition $\phi(1) = 1$.

We see the first condition is valid if we consider

$$\phi(a_n x^n + \cdots + a_1 x + a_0) = a_n x^{np} + \cdots + a_1 x^p + a_0 = \phi(a_n x^n) + \cdots + \phi(a_1 x) + \phi(a_0)$$

We see the multiplicative condition is valid if we consider

$$\begin{aligned}
&\phi\left((a_n x^n + \cdots + a_1 x + a_0)(b_m x^m + \ldots b_1 x + b_0)\right) = \\
&\quad = \phi(a_n b_m x^{n+m} + \cdots + a_0 b_0) \\
&\quad = a_n b_m x^{(n+m)p} + \cdots + a_0 b_0 \\
&\quad = (a_n x^{np} + \cdots + a_0)(b_m x^{mp} + \cdots + b_0) \\
&\quad = \phi(a_n x^n + \ldots a_0)\phi(b_m x^m + \cdots + b_0)
\end{aligned}$$

So the Frobenius map is a ring homomorphism.

□

Exercise (11.3.12). *Let I and J be ideals of a ring R. Prove that the set $I+J$ of elements of the form $x+y$, with x in I and y in J, is an ideal. This ideal is called the sum of the ideals I and J.*

Proof. Recall for $I+J$ to be an ideal it must be closed under addition, and if s is in $I+J$ and r is in R, then rs is in $I+J$.

First consider the closure condition, if we have two arbitrary elements a, b in $I+J$. They must be of the form $a = cx_1 + dy_1$ and $b = ex_2 + fy_2$, where c, d, b, e are in R, $x_i \in I$ and $y_i \in J$. Then we have the sum $a+b = (cx_1 + ex_2) + (dy_1 + fy_2)$, the first term is in I by definition of an ideal, the second term is in J by definition of an ideal, and the sum is in $I+J$ by definition of $I+J$ given in the problem.

For the second condition consider some element $s \in I+J$ and $r \in R$. By definition of $I+J$ there is some $x \in I$ and $y \in J$ such that $s = x+y$. And since I and J are ideals they contain rx and ry respectively, so by our definition of $I+J$ it must contain an element $rx + ry = r(x+y) = rs$. So $I+J$ meets the both conditions, it is therefore an ideal.

□

Exercise (11.3.13). *Let I and J be ideals of a ring R. Prove that the intersection $I \cap J$ is an ideal. Show by example that the set of products $\{xy | x \in I, y \in J\}$ need not be an ideal, but that the set of finite sums $\Sigma x_\nu y_\nu$ of products of elements of I and J is an ideal. This ideal is called the product ideal, and is denoted by IJ. Is there a relation between IJ and $I \cap J$?*

Proof. To show $I \cap J$ is an ideal we first prove the closure condition. If a and b are elements of $I \cap J$ then $a \in I$, $a \in J$, $b \in I$, $b \in J$. So since a and b are in both I and J, $a+b$ is in both I and J. So $a+b \in I \cap J$ and $I \cap J$ is therefore closed under addition.

For the ring-product condition consider some element $s \in I \cap J$. Then s is in both I and J, which are ideals so both I and J contain rs where r is any element of the ring R. Since rs is in both I and J it is in $I \cap J$.

So $I \cap J$ is an ideal.

For the next part consider $I = R[x]$ and $J = R[y]$, which are the rings of polynomials in x and y respectively. So IJ contains the two elements x^2 and y^2 are both in IJ but their sum $x^2 + y^2$ is not in IJ. So IJ, by this definition, is not an ideal.

For this definition of an ideal products, consider two elements $x = a_1 b_1 + \cdots + a_n b_n$ and $x = a'_1 b'_1 + \cdots + a'_m b'_m$ in IJ. Then $x + y = a_1 b_1 + a'_1 b'_1 + \cdots + a_n b_m + a'_m b'_m$ is in IJ because it is also a finite some of products of elements in I and J. Next for the ring-product condition of an ideal, if $s = a_1 b_1 + \ldots a_n b_n$ is in IJ and $r \in R$ then the elements $ra_1, \ldots ra_n$ are in I since it is an ideal. And since these are elements of I we can form rs with them as $rs = ra_1 b_1 + \ldots ra_n b_n$. So rs is in IJ so IJ is an ideal.

By inspection $I \cap J \supseteq IJ$.

$\square$