Math 120 HW 9 Solutions

June 8, 2018

Question 1

Write down a ring homomorphism (no proof required) f from $R = \mathbb{Z}[\sqrt{11}] = \{a + b\sqrt{11} | a, b \in \mathbb{Z}\}$ to $S = \mathbb{Z}/35\mathbb{Z}$.

The main difficulty is to find an element $x \in \mathbb{Z}/35\mathbb{Z}$ which satisfies $x^2 \equiv 11 \pmod{35}$. One way to solve for such an element systematically is to work separately modulo 5 and 7. The solutions to $x^2 \equiv 11 \pmod 5$ are $x \equiv \pm 1$, and the solutions to $x^2 \equiv 11 \pmod 7$ are $x \equiv \pm 2$. Putting these possibilities together using the Chinese Remainder Theorem, the four solutions to $x^2 \equiv 11 \pmod{35}$ are $x \equiv 9, 16, 19, 26 \pmod{35}$.

Picking any of these, say $x = 9$, we get a ring homomorphism $f : R \to S$ given by $f(a + b\sqrt{11}) = a + 9b$ by sending $\sqrt{11}$ to 9.

Question 2

Let $R \subset \mathbb{R}[x]$ be the subring of $\mathbb{R}[x]$ consisting of polynomials whose coefficient of x is 0:

$$R = \{f(x) = a_0 + a_2x^2 + \cdots + a_nx^n | a_i \in \mathbb{R}\}.$$

You proved in HW8 Q1 that R is not a PID. Is R a UFD? Prove or disprove.

No, R is not a UFD. For example, $x^6 = x^2 \cdot x^2 \cdot x^2 = x^3 \cdot x^3$, and neither x^2 nor x^3 can be factored further (by degree considerations) in R. Thus x^6 has two different factorizations into irreducibles in R.

Question 3

Given a polynomial $p(x) \in R[x]$ and an element $a \in R$, we say that a is a *root* of $p(x)$ if $p(a) = 0 \in R$.

Prove that if R is a domain and $p(x)$ has degree n, then $p(x)$ has at most n roots in R.

We start with a "zero theorem" for polynomials over a general commutative ring.

Lemma 1. *If R is a commutative ring, $p(x) \in R[x]$, and $a \in R$ is a root of $p(x)$, then $p(x) = (x - a)q(x)$ for some $q \in R[x]$.*

Proof. Induct on the degree of $p(x)$. If $\deg p = 0$, then $p(x)$ is a nonzero constant function, so it can't have roots.

Suppose the lemma is true for all polynomials of degree at most $n - 1$, and let $\deg p = n$. If the leading term of p is a_nx^n, then

$$p(x) = a_nx^{n-1}(x - a) + r(x)$$

for some $r(x)$ of strictly smaller degree. By induction, $r(x)$ is a multiple of $(x - a)$, so $p(x)$ is as well. □

Now, suppose for the sake of contradiction that R is a domain and $p(x)$ has degree n but $n + 1$ roots $a_1, \ldots, a_{n+1}$. Then, by the lemma, $p(x) = (x - a_1)p_1(x)$ for some $p_1(x) \in R[x]$ of degree $n - 1$. Since $p(a_i) = 0$ for all i,

$$p(a_i) = (a_i - a_1)p_1(a_i) = 0$$

for all i. But R is a domain and has no zero divisors, so since $(a_i - a_1) \neq 0$, we conclude that $p_1(a_i) = 0$ for all $i = 2, \ldots, n+1$. Applying the lemma to p_1 next, we find $p(x) = (x - a_1)(x - a_2)p_2(x)$, where p_2 has all the roots $a_3, \ldots, a_{n+1}$. Continuing in this manner, we find that $p(x) = (x - a_1)\cdots(x - a_{n+1})p_{n+1}(x)$ for some polynomial $p_{n+1}(x) \in R[x]$. But such a product has degree at least $n+1$, which is a contradiction. Thus $p(x)$ had at most n roots to begin with.

Question 4

Let $p(x) \in \mathbb{C}[x]$ be a nonzero polynomial. Consider the following two properties of $p(x)$:

(A) The quotient ring $\mathbb{C}[x]/(p(x))$ is isomorphic to a product ring $\mathbb{C} \times \cdots \times \mathbb{C}$.

(B) The polynomial $p(x)$ has no repeated roots.

Prove that these two properties are equivalent: $(A) \iff (B)$.

Write $\mathbb{C}^n$ for the n-fold product ring $\mathbb{C} \times \cdots \times \mathbb{C}$.

Suppose first that $p(x)$ has no repeated roots. By the fundamental theorem of algebra, $p(x)$ factors as $p(x) = u(x - \alpha_1)\cdots(x - \alpha_n)$ where $u \neq 0$ and $\alpha_i \in \mathbb{C}$ are all distinct. Then, consider the map $\phi : \mathbb{C}[x]/(p(x)) \to \mathbb{C}^n$, given by evaluating at each of the roots of p:

$$\phi(\overline{f}) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)).$$

Then, $\phi(\overline{f}) = (0, \ldots, 0)$ if and only if $f(\alpha_i) = 0$ for all i. This happens if and only if $f \in (p(x))$, so indeed $\ker\phi = (p(x))$ and ϕ is well-defined. Note that ϕ is just the product of n different evaluation maps, which we have shown (e.g. HW7 Q3) are individually ring homomorphisms. Thus ϕ is a ring homomorphism. It remains to show that ϕ is an isomorphism. By the argument before, $\ker\phi = (p(x))$ exactly so ϕ is injective.

To prove surjectivity, pick any $(z_1, \ldots, z_n) \in \mathbb{C}^n$. There exists by Lagrange interpolation a polynomial $q(x) \in \mathbb{C}[x]$ for which $q(\alpha_i) = z_i$. Explicitly,

$$q(x) = \sum_{i=1}^{n} z_i \frac{\prod_{j \neq i}(x - \alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)}.$$

For this polynomial q, $\phi(\bar{q}) = (z_1, \ldots, z_n)$. Thus ϕ is bijective and therefore an isomorphism of rings, as desired.

Conversely, suppose the quotient ring $\mathbb{C}[x]/(p(x))$ is isomorphic to some product $\mathbb{C}^n$.

Define a *nilpotent* element of a ring R to be an element $r \in R$ for which some power vanishes: $r^m = 0$ for some $m \in \mathbb{N}$. We claim that $\mathbb{C}^n$ has no nonzero nilpotents. Indeed, if $(z_1, \ldots, z_n) \in \mathbb{C}^n$, then multiplication is coordinatewise, so $(z_1, \ldots, z_n)^m = 0$ iff all of the z_i are zero.

Thus, $\mathbb{C}[x]/(p(x))$, being isomorphic to $\mathbb{C}^n$, must also have no nonzero nilpotents. Write by the fundamental theorem of algebra

$$p(x) = u(x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2}\cdots(x - \alpha_r)^{m_r}$$

where now the α_i are the distinct roots of p but the multiplicities m_i are not necessarily 1. In fact, if $p(x)$ has repeated roots, then some $m_i \neq 1$, and so the function $q(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_r)$ is not a multiple of p, so $q \neq 0$ in $\mathbb{C}[x]/(p(x))$. But $q(x)^M$ is a multiple of p, where $M = \max(m_1, \ldots, m_r)$, so $q(x)^M = 0$ in $\mathbb{C}[x]/(p(x))$, and therefore q would be a nonzero nilpotent in $\mathbb{C}[x]/(p(x))$. Since $\mathbb{C}[x]/(p(x))$ has no nonzero nilpotents, it follows that all the $m_i = 1$ and $p(x)$ has no repeated roots, as desired.

Question 5

Let $R = \mathbb{Z}/5^\infty\mathbb{Z}$ (just like the ring $\mathbb{Z}/10^\infty\mathbb{Z}$ from HW6, but in base 5 instead).

(a) Prove that $R = \mathbb{Z}/5^\infty\mathbb{Z}$ is a domain.

One way of explicitly describing the elements $r \in R$ is to identify them with infinite sequences $(r_1, r_2, \ldots)$ where $r_i \in \mathbb{Z}/5^i\mathbb{Z}$ and $r_i \equiv r_{i-1} \pmod{5}^{i-1}$, where addition and multiplication is coordinatewise. Suppose $r, s \in R$ are identified with sequences $(r_1, r_2, \ldots)$ and $(s_1, s_2, \ldots)$, and $r, s \neq 0$. We want to show that $rs \neq 0$.

But if $rs = 0$, then $r_i s_i \equiv 0 \pmod{5}^i$ for all i. In particular, for each i, one of r_i or s_i is divisible by $5^{\lfloor i/2 \rfloor}$. Since $r_i \equiv r_{\lfloor i/2 \rfloor} \pmod{5}^{\lfloor i/2 \rfloor}$ and $s_i \equiv s_{\lfloor i/2 \rfloor} \pmod{5}^{\lfloor i/2 \rfloor}$, it follows that for all i, either $r_{\lfloor i/2 \rfloor} \equiv 0 \pmod{5}^{\lfloor i/2 \rfloor}$or $s_{\lfloor i/2 \rfloor} \equiv 0 \pmod{5}^{\lfloor i/2 \rfloor}$.

In particular, one of $(r_1, r_2, \ldots)$ and $(s_1, s_2, \ldots)$ has infinitely many terms equal to zero (in the appropriate ring $\mathbb{Z}/5^i\mathbb{Z}$). But then every term before each zero must also be zero. Thus, one of r, s is zero, and there are no nontrivial zero divisors in R, as desired.

(b) Describe which elements of $R = \mathbb{Z}/5^\infty\mathbb{Z}$ are units.

The answer is all elements for which $r_1 \not\equiv 0 \pmod 5$. Concretely, in base 5 this includes all "infinite base-5 integers" which do not end in zero. To prove this rigorously, one must construct an s for each such r for which $rs = 1$ - in other words, to give a sequence $(s_1, s_2, \ldots)$ for which $r_i s_i \equiv \pmod 5$ for all i. This turns out to be a special case of an important result known as Hensel's Lifting Lemma.

(c) Let K be the fraction field of domain $R = \mathbb{Z}/5^\infty\mathbb{Z}$. Give a *concrete* description of K. What are its elements? What are the operations of addition/multiplication on these elements? Can one easily see from your description that every nonzero element is invertible, or is that difficult to see? Sketch a proof that your description is correct.

One way of defining K is as the set of fractions $5^n u$ where $n \in \mathbb{Z}$ and $u \in R$ is a unit, together with 0. By part (b), every element $r \in R$ can be written as $5^n u$ for some $n \geq 0$ and some unit u by dividing r by the highest power of 5 dividing r.

Addition and multiplication work in the obvious ways. If $5^m u$ and $5^n v$ are two elements for which $m \leq n$ (without loss of generality), $5^m u + 5^n v = 5^m(u + 5^{n-m}v)$, where the latter addition is addition in R. It is possible for powers of 5 to appear in the sum $u + 5^{n-m}v$ if $n = m$; in this case, factor out the largest power of 5 dividing $u + v$ and combine it with 5^m. Multiplication is just

$$(5^m u)(5^n v) = 5^{m+n}(uv).$$

Every nonzero element $5^n u$ has an inverse $5^{-n}u^{-1}$ since u is a unit in R.

The point is that the only elements not invertible already in R are multiples of 5, and so "inverting 5" is all that's necessary to obtain the fraction field.

Question 6

Suppose that R is a commutative ring which contains $\mathbb{Z}$.

(a) Prove that if $P \subset R$ is a prime ideal of R, then $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

Certainly, $P \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$, since P itself must be closed under multiplication by $\mathbb{Z} \subseteq R$. Suppose for the sake of contradiction that P is prime but $P \cap \mathbb{Z}$ is not prime in $\mathbb{Z}$. Then, since the ideals of $\mathbb{Z}$ are just $n\mathbb{Z}$ and are prime iff n is prime, this implies that $P \cap \mathbb{Z} = n\mathbb{Z}$ for a composite n. Pick any nontrivial factorization $n = ab$ of z. Since $a, b \in \mathbb{Z} \subseteq R$ as well, it follows that $ab \in P$ but $a, b \notin P$,so P is not a prime ideal. This is the contradiction we were looking for.

(b) Part (a) defines a function $\beta : \{$prime ideals of $R\} \to \{$prime ideals of $\mathbb{Z}\}$. Construct an explicit commutative ring R containing $\mathbb{Z}$ such that the image of β is

$$\mathbf{im}\beta = \{(0), (5), (7), (11), (13), \ldots\}$$

i.e. all prime ideals except (2) and (3). Prove (or at least sketch a proof) R has this property.

One such ring is $R = \mathbb{Z}[\frac{1}{6}] = \{\frac{a}{2^m 3^n}, a \in \mathbb{Z}, m, n \in \mathbb{N}\}$. This ring certainly contains $\mathbb{Z}$. Also, note that $(p) \subset R$ is still a prime ideal for every $p \in \mathbb{Z}$ prime which is not 2 and 3, and $(0) \subset R$ is as well since R is a domain. For these, it is easy to check that $\beta(pR) = p\mathbb{Z}$ and $\beta(0R) = 0\mathbb{Z}$.

Thus, $\text{im}\beta \supseteq \{(0), (5), (7), (11), (13), \ldots\}$. It remains to show that (2) and (3) are not in this image.

If $(2) \in \text{im}\beta$, there is some prime $P \subset R$ for which $P \cap \mathbb{Z} = 2\mathbb{Z}$. But then $P \ni 2$, and $\frac{1}{2}$ lies in R, so $P \ni \frac{1}{2} \cdot 2 = 1$. Thus P must be the entire ring, contradicting the fact that $P \cap \mathbb{Z} = 2\mathbb{Z}$. Similarly, $P \cap \mathbb{Z} \neq 3\mathbb{Z}$ for any $P \subset R$.

Question 7

(a) Let F be a field, and let $R \subset F$ be a subring with the property that for every $x \in F$, either $x \in R$ or $\frac{1}{x} \in R$ (or both).

Prove that if I and J are two ideals of R, then either $I \subseteq J$ or $J \subseteq I$.

Suppose for the sake of contradiction that there exist two ideals I, J neither of which contains the other. Then, there are elements $x \in I \backslash J$ and $y \in J \backslash I$. Since all ideals contain 0, we have $x, y \neq 0$. Thus, $x/y \in F$, and the property given tells us that either x/y or its inverse y/x lies in R. Without loss of generality, $x/y \in R$. Then, since J is an ideal of R, $x = (x/y) \cdot y \in J$, contradicting the assumption $x \notin J$. Thus one of I, J contains the other.

(b) Construct a proper subring $R \subsetneq \mathbb{Q}$ such that for every $x \in \mathbb{Q}$, either $x \in R$ or $\frac{1}{x} \in R$ (or both).

Let

$$R = \{\frac{a}{b} \in \mathbb{Q}, 2 \nmid b\},$$

i.e. the ring of all fractions with odd denominator. Sums and products of such fractions also have odd denominator, so R is a subring of $\mathbb{Q}$, and it is proper because $\frac{1}{2} \notin R$.

For any $x \in \mathbb{Q}$, x can be written as a/b, where a, b are coprime. Thus, at least one of a and b is odd, so at least one of a/b and its inverse b/a lies in R, as desired.

Question 8

Given an abelian group A, we say the 10-*dual* $A^\vee$ is the abelian group of homomorphisms $f : A \to \mathbb{Z}/10\mathbb{Z}$ under pointwise addition.

We call an abelian group 10-*invisible* if $A^\vee = 0$, i.e. if there are no nonzero group homomorphisms $f : A \to \mathbb{Z}/10\mathbb{Z}$.

(a*) Compute $A^\vee$ for $A = \mathbb{Z}, A = \mathbb{Z}/6\mathbb{Z}$, and $A = \mathbb{Z}/10\mathbb{Z}$.

As abelian groups, the answers are $\mathbb{Z}^\vee \simeq \mathbb{Z}/10\mathbb{Z}$, $(\mathbb{Z}/6\mathbb{Z})^\vee \simeq \mathbb{Z}/2\mathbb{Z}$, and $(\mathbb{Z}/10\mathbb{Z})^\vee \simeq \mathbb{Z}/10\mathbb{Z}$. These can be computed using the fact that a homomorphism between cyclic groups is determined by the image of a generator.

(b) We know from class (or will soon) that every finitely-generated abelian group A is isomorphic to

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

for a unique $r \geq 0$ and a unique sequence of positive integers $n_1|n_2|\cdots|n_k$.

In terms of this description, which finitely-generated abelian groups are 10-invisible?

If there is a nonzero homomorphism $f : G_i \to \mathbb{Z}/10\mathbb{Z}$ from any single factor in a direct sum $\bigoplus G_i$ of abelian groups to $\mathbb{Z}/10\mathbb{Z}$, then there is a nonzero homomorphism from the whole sum to $\mathbb{Z}/10\mathbb{Z}$, given by first projecting an element $(a_1, \ldots, a_n) \in \bigoplus G_i$ onto the i-th coordinate a_i and then applying f.

Thus it suffices to check which cyclic groups $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ are 10-invisible. The answer is exactly the groups $\mathbb{Z}/n\mathbb{Z}$ for which $(n, 10) = 1$, which we show now.

First, if $(n, 10) = 1$, then any homomorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ must send $\bar{1}$ to an element with order dividing n. But no nonzero element of the range has order dividing n, so $f = 0$.

Conversely, if $2|n$, there exists a nonzero homomorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ given by sending $\bar{1}$ to $\bar{5}$. Similarly, if $5|n$, one can simply send $\bar{1}$ to $\bar{2}$.

As a result, the finitely-generated 10-invisible abelian groups are exactly those finite abelian groups of the form

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

where $n_1|n_2|\cdots|n_k$, and $(n_k, 10) = 1$.

(c) Choose two of the following abelian groups A, and for each, describe as best you can the abelian group $A^\vee$:

(i) $A = \mathbb{Q}$,

We show $\mathbb{Q}^\vee = 0$. If not, some $f : \mathbb{Q} \to \mathbb{Z}/10\mathbb{Z}$ is nonzero, and sends $a/b \mapsto \bar{n}$ for $10 \nmid n$ and $a/b \in \mathbb{Q}$. But then it must send $a/10b$ to an element $\bar{m} \in \mathbb{Z}/10\mathbb{Z}$ for which $10\bar{m} = \bar{n}$, which is absurd.

(ii) $A = \mathbb{Z}[\frac{1}{6}]$,

We show $(\mathbb{Z}[\frac{1}{6}])^\vee \simeq \mathbb{Z}/5\mathbb{Z}$. In fact, the five homomorphisms are $f_i, 0 \leq i \leq 4$, where $f_i(a/6^k) = \overline{2ai}$ (mod 10). It is easy to check that these maps are homomorphisms - note that $\bar{6}\bar{m} \equiv \bar{m}$ (mod 10) for any even m. Conversely, to show that these are the only homomorphisms can be reduced to checking that if $f(1) = \bar{0}$ then $f = 0$.

Suppose there is a nonzero group homomorphism f for which $f(1) = \bar{0}$. Then, $6^k f(1/6^k) = \bar{0}$, so $f(1/6^k)$ is an element divisible by 5 in $\mathbb{Z}/10\mathbb{Z}$, i.e. $f(1/6^k) \in \{\bar{0}, \bar{5}\}$. But if $f(1/6^k) = \bar{5}$, then $6f(1/6^{k+1}) \equiv 5 \pmod{10}$, which is absurd since 5 is odd. Thus, $f(1/6^k) = 0$ for all k. It now follows that $f(a/6^k) = 0$ for all a, k, as desired.

(iii) $A = \mathbb{Q}/\mathbb{Z}$**,**

Any group homomorphism $\mathbb{Q}/\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ can be precomposed with the quotient map $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ to give a homomorphism $\mathbb{Q} \to \mathbb{Z}/10\mathbb{Z}$. By (i) there are no such nonzero maps, so $(\mathbb{Q}/\mathbb{Z})^\vee = 0$ as well.

(iv) $A = \mathbb{Z}/10^\infty\mathbb{Z}$**.**

We claim that $(\mathbb{Z}/10^\infty\mathbb{Z})^\vee \simeq \mathbb{Z}/10\mathbb{Z}$, and the ten maps are given by $f_i(r) = ir \pmod{10}$ for each of $i = 0, \ldots, 9$. These are certainly homomorphisms; it remains to check that they are all possible ones.

Note that $f(10r) = 10f(r) \equiv 0 \pmod{10}$, so every multiple of 10 is sent to zero in $\mathbb{Z}/10\mathbb{Z}$. Also, every $r \in \mathbb{Z}/10^\infty\mathbb{Z}$ can be written as $r_0 + 10r_1$ where $r_0 \in \{0, \ldots, 9\}$ is the ones digit and $r_1 \in \mathbb{Z}/10^\infty\mathbb{Z}$. Thus, for f to be a group homomorphism,

$$f(r) = f(r_0 + 10r_1) = r_0 f(1) + 10f(r_1) = r_0 f(1).$$

Thus, f is uniquely determined by $f(1)$, and we're done.