MATH 1530 ABSTRACT ALGEBRA
Selected solutions to problems

Problem Set 2

2. Define a relation $\sim$ on $\mathbb{R}$ given by $a \sim b$ if $a - b \in \mathbb{Z}$.

   (a) Prove that $\sim$ is an equivalence relation.

   (b) Let $\mathbb{R}/\mathbb{Z}$ denote the set of equivalence classes of $\sim$. Prove that the binary operation $+$ on $\mathbb{R}/\mathbb{Z}$ given by
   $$\overline{a} + \overline{b} = \overline{a+b}$$
   is well-defined.

   (c) Is $(\mathbb{R}/\mathbb{Z}, +)$ a group?

Solution. (I will omit the proof that $\mathbb{R}/\mathbb{Z}$ is a group.) Given $a, b, c \in \mathbb{R}$, note:

(a) $a - a = 0 \in \mathbb{Z}$;

(b) $a - b \in \mathbb{Z}$ implies $b - a = -(a - b) \in \mathbb{Z}$; and

(c) if $a - b \in \mathbb{Z}$ and $b - c \in \mathbb{Z}$ then $a - c = (a - b) - (b - c) \in \mathbb{Z}$;

so $\sim$ is an equivalence relation.

Next, we show that the binary operation $+$ on $\mathbb{R}/\mathbb{Z}$ given by $\overline{a} + \overline{b} = \overline{a+b}$ is well defined. Suppose $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$ for some $a, b, a', b' \in \mathbb{R}$. We wish to show $\overline{a+b} = \overline{a'+b'}$.

The assumptions imply $a - a' \in \mathbb{Z}$ and $b - b' \in \mathbb{Z}$, so

$$(a+b) - (a'+b') = (a-a') + (b-b') \in \mathbb{Z}.$$

So
$$\overline{a+b} = \overline{a'+b'},$$
as desired.

Problem Set 3

2. Write out the full multiplication table for the group S_3.

   It should be a 6×6 table whose entries are elements of S_3, and whose rows and columns are indexed by the elements of S_3. Please write all elements using cycle notation.

   Solution.

$\cdot$	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(132)	(231)	(23)	(13)
(13)	(13)	(123)	id	(231)	(12)	(23)
(23)	(23)	(132)	(123)	id	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)

3. Is it true that for all $n \geq 1$, every element of S_n has order at most n? Either prove it, or give a counterexample.

   Solution. **No.** We saw in the Youtube lecture that the order of an element $\sigma \in S_n$ is the least common multiple of all of the numbers appearing as lengths of some cycle in σ, when σ is expressed in cycle notation.

   Thus the order of $(12)(345) \in S_5$ is 6.

5. Let $(G, *)$ and $(H, \circ)$ be groups, and let $\phi\colon G \to H$ be an isomorphism. Let $\phi^{-1}\colon H \to G$ denote the *inverse* of ϕ. In other words, $\phi^{-1}(h) = g$ whenever $\phi(g) = h$.

   Prove that ϕ^{-1} is also an isomorphism.

   Solution. Let us use the fact from class:

   Fact. A map $f\colon A \to B$ is bijective if and only if there exists an inverse, i.e. a map $g\colon B \to A$ with $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$, where $\mathrm{id}_A\colon A \to A$ and $\mathrm{id}_B\colon B \to B$ denote the respective identity maps. This fact implies that the inverse of a bijective map is again a bijection. So ϕ^{-1} is a bijection, and it remains to show ϕ^{-1} is a homomorphism of groups.

   Indeed, given $h, h' \in H$, let $g, g' \in G$ be the unique elements of G such that $\phi(g) = h$ and $\phi(g') = h'$; such g, g' exist and are unique since ϕ is bijective. Then note $\phi(gg') = hh'$ since ϕ is a homomorphism.

   Then

$$\phi^{-1}(hh') = gg' = \phi^{-1}(h)\phi^{-1}(h'),$$

as desired.

6. Prove that isomorphism is an equivalence relation on groups.

Solution. It's reflexive since $\mathrm{id}_G \colon G \to G$ is an isomorphism from G to itself. The previous problem shows that it is symmetric. For transitivity, it suffices to show that a composition of isomorphisms is again an isomorphism. In other words, we show that if $\phi \colon G \to H$ and $\psi \colon H \to K$ are isomorphisms, then so is $\psi \circ \phi \colon G \to K$.

The fact that $\psi \circ \phi$ is a bijection follows from the fact that compositions of bijections are bijections. I omit the proof. To check that $\psi \circ \phi$ is a homomorphism: given $g, g' \in G$, note

$$(\psi \circ \phi)(gg') = \psi(\phi(g)\phi(g')) = (\psi \circ \phi)(g)(\psi \circ \phi)(g'),$$

where we used in turn the facts that ψ and ϕ are homomorphisms.

Problem Set 4

2. How many homomorphisms $\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ are there? How many homomorphisms $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}$ are there? Justify your answers briefly.

Solution. There are **three** homomorphisms $\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, since we showed in class that for any group G and any $g \in G$, there is a unique homomorphism $\phi\colon \mathbb{Z} \to G$ such that $\phi(1) = g$.

There is **one** homomorphism $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}$. We mentioned in class that for any pair of groups G and H, the map sending everything in G to 1_H is always a homomorphism (check this), so there is at least one such homomorphism.

On the other hand, suppose $\phi\colon \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}$ is any homomorphism; we'll show that $\phi(\overline{n}) = 0$ for all $\overline{n} \in \mathbb{Z}/3\mathbb{Z}$, so ϕ was in fact the one homomorphism we already identified.

It suffices to show that $\phi(\overline{1}) = 0$, since then $\phi(\overline{n}) = n\phi(1) = 0$. We note

$$0 = \phi(\overline{0}) = \phi(\overline{1} + \overline{1} + \overline{1}) = \phi(\overline{1}) + \phi(\overline{1}) + \phi(\overline{1}).$$

So $\phi(\overline{1}) = 0$.

5. Does $\mathbb{R}$ have any subgroups isomorphic to $\mathbb{Z}^2$? Prove your answer.

Solution. Yes, let

$$H = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

We claim $H \leq \mathbb{R}$ is a subgroup isomorphic to $\mathbb{Z}^2$. I will omit the proof that H is a subgroup.[1]

Let us now consider the map

$$\phi\colon \mathbb{Z}^2 \to H$$

given by $(a, b) \mapsto a + b\sqrt{2}$. This map is a homomorphism: indeed

$$\phi((a, b) + (c, d)) = \phi((a + c, b + d)) = (a + c) + (b + d)\sqrt{2} = \phi((a, b)) + \phi((c, d)).$$

It is surjective by construction. As for injectivity, suppose $\phi((a, b)) = \phi((c, d))$; we wish to show $(a, b) = (c, d)$. We have

$$a + b\sqrt{2} = c + d\sqrt{2} \text{ implies } a - c = (d - b)\sqrt{2}.$$

The left hand side is an integer and the right hand side is irrational unless $d - b = 0$. We conclude $d - b = 0$, and therefore $a - c = 0$, as desired. Therefore ϕ is an isomorphism.

[1] In fact, it follows from the fact that $H = \text{im}(\phi)$ where ϕ is defined below; but we had not isolated and proved the fact that $\text{im}(\phi)$ is always a subgroup when this problem was assigned.)

6. Does $\mathbb{Q}$ have any subgroups isomorphic to $\mathbb{Z}^2$? Prove your answer.

Solution. We claim the answer is no. Suppose on the contrary that $\phi\colon \mathbb{Z}^2 \to H$ was an isomorphism from $\mathbb{Z}^2$ to some subgroup H. Let us write the rational numbers $\phi(1,0)$ and $\phi(0,1)$ with a common denominator, say

$$\phi(1,0) = a/n, \qquad \phi(0,1) = b/n$$

for some $a, b, n \in \mathbb{Z}$ with $n \neq 0$. Then

$$\phi(b,0) = \phi(0,a) = ab/n.$$

Since ϕ is injective, we conclude $(b,0) = (0,a)$, so $a = b = 0$. But this contradicts that $\phi(1,0) \neq 0$ and $\phi(0,1) \neq 0$ by injectivity of ϕ.

Problem Set 5

2. (a) Let G be a group acting on a set A. The *stabilizer* of an element $a \in A$, denoted G_a, is defined to be the set
$$G_a = \{g \in G : g \cdot a = a\}.$$
Prove that the stabilizer is a subgroup of G.

In class on Thursday February 23, you considered the action of the group G of rotations on the power set $\mathcal{P}(\mathbb{R}^2)$ of $\mathbb{R}^2$.

(b) Which elements of $\mathcal{P}(\mathbb{R}^2)$ have stabilizer equal to G? Justify your answer briefly.

(c) (optional, extra) Does there exist any $S \in \mathcal{P}(\mathbb{R}^2)$ with infinite cyclic stabilizer?

Solution. Note $1 \in G_a$. Next, if $g, h \in G_a$, then we have
$$(gh^{-1}) \cdot a = g(h^{-1} \cdot a) = g \cdot a = a,$$
so $gh^{-1} \in G_a$. (In general, if $h \in G$ and $h \cdot b = c$ for some $b, c \in A$, then applying h^{-1} on both sides yields that $b = h^{-1} \cdot c$. Then in particular $h \cdot a = a$ implies $h^{-1} \cdot a = a$.) Thus G_a is a subgroup by the subgroup criterion.

For part (b), suppose $S \subseteq \mathbb{R}^2$ has $G_S = G$. If $p \in S$ then every point obtained by rotating p about the origin must also be in S; in other words, the entire locus of points
$$\{x \in \mathbb{R}^2 \colon ||x|| = ||p||\}$$
lies in S. Thus S is a union of such loci, i.e. it is a union of circles centered at the origin, possibly together with the origin itself.

4. Let p be any prime number. Prove that every group of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Solution. Let G be a group of order p. Since $p \geq 2$, G has some nonidentity element, say x. Then $\langle x \rangle$ is a subgroup of G whose cardinality is greater than 1 and divides p (by Lagrange). Therefore $\langle x \rangle = G$, so G is cyclic, and every cyclic group of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, as shown in class.

5. We showed in an earlier lecture that
$$Z(G) = \{x \in G \ : \ gx = xg \text{ for all } g \in G\}$$
is a subgroup of G, called the *center* of G. Prove that $Z(G)$ is normal, and that it consists precisely of the elements of G whose conjugacy classes have size 1.

Solution. The first claim follows from the second, since we showed that if a subgroup is a union of conjugacy classes then it is normal. For the second claim, note that an element $x \in G$ has conjugacy class $\{x\}$ if and only if

$$gxg^{-1} = x \quad \text{for all } g \in G,$$

equivalently, if $gx = xg$ for all $g \in G$, equivalently if $x \in Z(G)$, as desired.

6. List the conjugacy classes of the dihedral group D_{12}. Draw the lattice of subgroups of D_{12} and indicate in your lattice which subgroups are normal. (No proofs necessary.)

Solution. I will leave the full drawing of the lattice to you. The conjugacy classes are

$$\{1\}, \{r, r^5\}, \{r^2, r^4\}, \{r^3\}, \{s, sr^2, sr^4\}, \{sr, sr^3, sr^5\}.$$

(Having listed these conjugacy classes, you may wish to use this list to check which subgroups are normal. Namely, you simply check whether your subgroup is made up of conjugacy classes.)

Problem Set 6

1. An element g of a group G is called *torsion* if it has finite order, and G is called *torsion-free* if its only torsion element is the identity.

   Let A be an abelian group and let N be the set of its torsion elements. Prove that N is a subgroup and that A/N is torsion-free.

   Solution. 1 has order 1, so $1 \in N$. Now given $a, b \in N$, let us show $ab^{-1} \in N$. Since a, b are torsion, there exist integers $m, n \geq 1$ with $a^m = b^n = 1$. Then note

   $$(ab^{-1})^{mn} = a^{mn}b^{-mn} = (a^m)^n(b^n)^{-m} = 1,$$

   where the first equality follows from the fact that A is abelian. Thus the subgroup criterion implies that N is a subgroup.

   Next, we show A/N is torsion-free. Given $aN \in A/N$, suppose aN is torsion; we wish to show $aN = N$ is the identity. Let $m \geq 1$ be such that $(aN)^m = N$. Then $a^m N = N$, implying $a^m \in N$.

   In other words, a^m itself is torsion in A, so there exists an integer $n \geq 1$ with $(a^m)^n = 1$. Therefore $a^{mn} = 1$ and so a is torsion itself. So $a \in N$, and $aN = N$ as desired.

2. (No proofs necessary) Let $N = Z(D_{12}) \trianglelefteq D_{12}$.

   (a) List the elements of N. You may use Dummit and Foote Problem 4 on p.28, on Homework 3, or combine your answers from Problems 5 and 6 from Homework 5.
   Now list the elements of D_{12}/N; there should be six of them.

   Solution. $N = \{1, r^3\}$, and

   $$D_{12}/N = \{N, rN, r^2N, sN, srN, sr^2N\}.$$

   (b) Write out the multiplication table for the group D_{12}/N. This should be a 6×6 table, all of whose entries are taken from your list of elements of D_{12}/N from part (a).

   Solution.

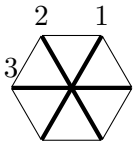
$\cdot$	N	rN	r^2N	sN	srN	sr^2N
N	N	rN	r^2N	sN	srN	sr^2N
rN	rN	r^2N	N	sr^2N	sN	srN
r^2N	r^2N	N	rN	srN	sr^2N	sN
sN	sN	srN	sr^2N	N	rN	r^2N
srN	srN	sr^2N	sN	r^2N	N	rN
sr^2N	sr^2N	sN	srN	rN	r^2N	N

3. Number the three diagonals of a regular hexagon as shown. Let D_{12} act on the set $\{1, 2, 3\}$ via $g \cdot i = j$ if $g \in D_{12}$ takes the diagonal i to diagonal j.

   Let $\phi\colon D_{12} \to S_3$ be the permutation representation of this action. Use ϕ to prove that

   $$D_{12}/N \cong S_3.$$

   Feel free to appeal to your geometric intuition. (In light of this fact, you may wish to compare your multiplication table for D_{12}/N with your multiplication table for S_3 from Homework 3.)



Solution. We know that ϕ is indeed a homomorphism, as stated in the guest lecture. It suffices to check that ϕ is surjective, and that $\ker \phi = N$, for then the desired isomorphism follows from the First Isomorphism Theorem.

Let us show that ϕ is surjective. Let us write r for rotation 60 degrees clockwise, and s for reflection across the diagonal 1. (Please note: *we shall follow the conventions of the textbook that products like sr are interpreted as "first do r, then do s."*) Then $\phi(r) = (132)$ and $\phi(s) = (23)$.

Now $\mathrm{im}(\phi)$, being a subgroup of S_3, necessarily contains $\langle(132)\rangle = \{1, (132), (123)\}$. But it also contains $\phi(s) = (23)$. Therefore $|\,\mathrm{im}(\phi)| \geq 4$, but $|\,\mathrm{im}(\phi)|$ divides 6 by Lagrange's theorem; therefore $\mathrm{im}(\phi) = S_3$.

Finally we claim $\ker(\phi) = N$. For the inclusion $\supseteq$, note that 1 and r^3 do indeed send each diagonal to itself (r^3 does so by flipping each diagonal). On the other hand, since rigid motions send adjacent vertices to adjacent vertices, any rigid motion in $\ker(\phi)$ that flips one diagonal flips them all, and any rigid motion in $\ker(\phi)$ that fixes one diagonal fixes them all. This shows the claim.

Problem Set 8

1. In class today (March 21), you formed groups of five students each with four students remaining, and then groups of seven students each with three students remaining. In your opinion, how many students came to class today?

   Solution. Since the natural map $\mathbb{Z}/35\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ discussed in class sends $\overline{24}$ to $(\overline{4}, \overline{3})$, we conclude from the Chinese Remainder Theorem that the number of students present must have been 24 (mod 35). I think there were $24 + 35 = 59$ students present.

2. Let $m, n \geq 1$ be integers. Prove that the set of numbers appearing as the order of some element of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is

$$\{d \in \mathbb{Z}_{>0} : d \text{ divides } \operatorname{lcm}(m, n)\}.$$

   Solution. Let us first establish a lemma: for any group G, if $g \in G$ has order n, and $n = cd$ for integers $c, d \geq 1$, then g^d has order c. Indeed, $(g^d)^c = 1$ but for any positive number $c' < c$, note $dc' < dc = |g|$, so $(g^d)^{c'} = g^{dc'} \neq 1$.

   Let's write $\ell = \operatorname{lcm}(m, n)$ for short. We claim that $|(\overline{1}, \overline{1})| = \ell$. Indeed, note that $(\overline{\ell}, \overline{\ell}) = (\overline{0}, \overline{0})$ since $m|\ell$ and $n|\ell$. On the other hand, if $(\overline{d}, \overline{d}) = (\overline{0}, \overline{0})$ for $d \in \mathbb{Z}$, then $m|d$ and $n|d$, hence $\ell|d$ (as established in class). Hence $|(\overline{1}, \overline{1})| = \ell$, and by the lemma, every positive divisor of ℓ occurs as the order of some element of the form $(\overline{d}, \overline{d})$.

   Conversely, if $(\overline{a}, \overline{b})$ has order d, then d necessarily divides ℓ since $(\overline{a\ell}, \overline{b\ell}) = (\overline{0}, \overline{0})$.

3. Let G be a group and let

$$\Delta = \{(g, g) : g \in G\} \subseteq G \times G.$$

   Prove that $\Delta \leq G \times G$ and that Δ is normal if and only if G is abelian.

   Solution. Δ is often called the *diagonal*. I leave it to you to check Δ is a subgroup. I also leave it to you to check that $G \times G$ is abelian if and only if G is abelian. Thus the "if" direction follows since every subgroup of an abelian group is normal. Conversely, suppose Δ is normal, and given $g, h \in G$, let us prove $gh = hg$, or equivalently $g = hgh^{-1}$. We have

$$\Delta \ni (h, 1)(g, g)(h, 1)^{-1} = (hgh^{-1}, g),$$

   implying that $hgh^{-1} = g$ as desired.

4. Let H, K be groups and let $\phi\colon K \to \mathrm{Aut}(H)$ be a homomorphism. Recall that $G = H \rtimes_\phi K$ contains subgroups

$$\widetilde{H} = \{(h,1) : h \in H\} \trianglelefteq G \qquad \widetilde{K} = \{(1,k) : k \in K\} \leq G$$

isomorphic to H and K respectively. Prove that $\widetilde{K} \trianglelefteq G$ if and only if ϕ is trivial.

(The map ϕ being *trivial* means that $\phi(k) = \mathrm{id}_H$ for all $k \in K$.)

Solution. If ϕ is trivial, then $k \cdot h = h$ for all $h \in H, k \in K$ (here $\cdot$ denotes the action of k on h via the map ϕ. Then for all $h \in H, k, k' \in K$, we have

$$(h,k)(1,k')(h,k)^{-1} = (h,kk')(h^{-1},k^{-1}) = (hh^{-1}, kk'k^{-1}) = (1, kk'k^{-1}) \in \widetilde{K},$$

so $\widetilde{K} \trianglelefteq G$.

Conversely, assume $\widetilde{K} \trianglelefteq G$. Given $h \in H$, $k \in K$, we wish to show $k \cdot h = h$. Note

$$(h^{-1},1)(1,k)(h^{-1},1)^{-1} = (h^{-1},k)(h,1) = (h^{-1}(k \cdot h), k).$$

This last element is in $\widetilde{K}$ by assumption, so $h^{-1}(k \cdot h) = 1$, so $k \cdot h = h$ as desired.

5. Consider the group of rigid motions of $\mathbb{R}^2$, i.e. rotations, reflections, translations, and compositions of these. (Optional, ungraded: express this group as a nontrivial semidirect product.)

For each of the following subsets S of $\mathbb{R}^2$, let G be the group of rigid motions of $\mathbb{R}^2$ that preserves S. Exhibit G as a nontrivial semidirect product in each case. Brief explanations may be helpful, but full proofs are not necessary.

(a) $S = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$, the unit circle

Solution.
$\mathbb{R}/2\pi\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acts on the group of rotations $\mathbb{R}/2\pi\mathbb{Z}$ by negation. (Same as the cylinder example in class.)

(b) $S = \mathbb{Z}^2$, the integer lattice points

Solution.
One possible solution: $\mathbb{Z}^2 \rtimes D_8$, where D_8 is identified with the group of rotations and reflections preserving the square $\{(x,y) \in \mathbb{R}^2 : -1 \leq x, y \leq 1\}$ (these are precisely the rigid motions of the plane that fix the origin and preserve $\mathbb{Z}^2$), and acts on $\mathbb{Z}^2$ according to the natural action of this group on the plane $\mathbb{R}^2$.

(c) $S = \{(x, y) \in \mathbb{R}^2 : -1 \leq y \leq 1\}$, an infinite horizontal strip.

Solution. $\mathbb{Z}/2\mathbb{Z} \rtimes (\mathbb{R} \times \mathbb{Z}/2\mathbb{Z})$, where the second factor records translations and reflection across the x-axis, and the first factor records reflection across the y-axis. Here, the action $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{R} \times \mathbb{Z}/2\mathbb{Z})$ sends the nonidentity element of $\mathbb{Z}/2\mathbb{Z}$ to the automorphism of $\mathbb{R} \times \mathbb{Z}/2\mathbb{Z}$ acting by negation on $\mathbb{R}$ and trivially on $\mathbb{Z}/2\mathbb{Z}$.

(There are other equally good ways to describe the same group, such as $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\phi \mathbb{R}$, with ϕ defined appropriately.)

6. Let p and q be distinct primes. Prove that any group of order pq is a semidirect product of two of its proper subgroups.

Solution. By Sylow's theorem such a group G has subgroups K and H of order p and q respectively. Assume without loss of generality that $p < q$; then $n_q \equiv 1 \bmod q$ and $n_q | p$ implies $n_q = 1$, hence H is normal.

Moreover $H \cap K = 1$, since $(|H|, |K|) = 1$, and the fact that $HK/H \cong K/(K \cap H)$ (Second Isomorphism Theorem) implies $|HK| = |H||K|$ so $HK = G$.

As shown in class, these hypotheses imply that $G \cong H \rtimes K$.

Problem Set 9

4. Let I be the ideal of $\mathbb{Z}[x]$ consisting of polynomials whose constant term, coefficient of x, and coefficient of x^2 are zero. Identify, with proof, the nilradical of $\mathbb{Z}[x]/I$.

   Solution. Write $\overline{f} = f + I$ for short. We claim the nilradical is $(\overline{x})$, that is, the nilradical is comprised of the classes of polynomials with zero constant term. If f has zero constant term, then $f^3 \in I$, so $\overline{f}^3 = 0$ in $\mathbb{Z}[x]/I$. Conversely, if f has constant term $a_0 \neq 0$, then f^n has constant term $a_0^n \neq 0$, so $\overline{f}^n \neq 0 \in \mathbb{Z}[x]/I$ for any $n \geq 0$.

5. Let I be an ideal in a ring R, and let $\pi\colon R \to R/I$ be the natural projection. Prove the following *universal property of quotients:* If $\varphi\colon R \to S$ is any ring homomorphism such that $I \subseteq \ker(\phi)$, then there exists a unique homomorphism $\overline{\varphi}\colon R/I \to S$ such that

$$\varphi = \overline{\varphi} \circ \pi.$$

   Solution. If such a $\overline{\varphi}$ exists, then given any $a \in R$, the equation above implies

$$\overline{\varphi}(\pi(a)) = \overline{\varphi}(a + I) = \varphi(a).$$

   Thus $\overline{\varphi}$ is uniquely determined, if it exists.

   Now we check that $\overline{\varphi}(a + I) = \varphi(a)$ is a well-defined homomorphism. Given $a, a' \in R$, if $a + I = a' + I$ then $a - a' \in I \subseteq \ker(\varphi)$, hence $\varphi(a) = \varphi(a')$. This shows well-definedness. I leave it to you to check that φ is a homomorphism of rings.

Problem Set 10

1. Let R be an integral domain, and let $f, g \in R$. Prove that $(f) = (g)$ if and only if $f = ga$ for some unit a.

   Solution. Let us prove the $\Rightarrow$ direction; I leave the other direction to you. If $(f) = (g)$ then $f = ga$ and $g = fb$ for some $a, b \in R$. Thus $f = abf$ and $f(1 - ab) = 0$. Now if $f = 0$ then necessarily $g = 0$ and we are done; if $f \neq 0$ then $1 - ab = 0$ since R has no zero divisors. So a and b are units.

2. Let K be a field, and consider the ring $K[[x]]$ of formal power series.

   (a) Prove that $K[[x]]$ is an integral domain.

   Solution. Suppose $f, g \in K[[x]]$ are nonzero; we wish to show fg is nonzero. Define the *order* of a nonzero power series f to be the smallest exponent appearing in f.
   Let d and e denote the orders of f and g respectively, and let a_d and b_e be the coefficient of x^d in f and the coefficient of x^e in g, respectively. Note $a_d, b_e \neq 0$.
   Then the coefficient of x^{d+e} in fg is $a_d b_e$, which is nonzero since K is a field and hence has no zerodivisors.
   Thus $fg \neq 0$, since we have exhibited a nonzero coefficient in it.

   (b) Prove that the ideals of $K[[x]]$ are 0 or are of the form (x^n) for some integer $n \geq 0$.

   Solution. Let $I \subseteq K[[x]]$ be an ideal. If $I = 0$ we are done. Otherwise, let $f \in I$ be a nonzero element of smallest order d.
   We claim $I = (x^d)$. The inclusion $I \subseteq (x^d)$ follows from the fact that every element of I has order at least d and hence is divisible by x^d.
   The inclusion $I \supseteq (x^d)$ follows from the fact that we may factor $f = x^d \cdot g$ for $g \in K[[x]]$ a power series with nonzero constant term. Such power series are units, by a previous homework problem. Therefore $x^d \in I$, as desired.

   (c) Which of the ideals of $K[[x]]$ are principal? maximal? prime? Prove your answers.

   Solution. Each ideal is generated by 1 element (including the 0 ideal which is generated by 0), so they are are all principal.
   Note $(x) \supset (x^2) \supset \cdots \supset 0$ and (x) is thus the unique maximal ideal.

Note that (x) is therefore prime, being maximal; and 0 is prime since $K[[x]]$ is an integral domain. On the other hand, we claim that for $d \geq 2$ the ideal $I = (x^d)$ is not prime, since $x \cdot x^{d-1} \in I$ but $x \notin I$ and $x^{d-1} \notin I$, which I leave to you to verify.

5. This is a problem in beginning algebraic geometry. Given an ideal $I \subseteq \mathbb{R}[x, y]$, we let the **v***anishing locus* or **v***ariety* of I be the subset of $\mathbb{R}^2$

$$V(I) = \{(a, b) \in \mathbb{R}^2 : f(a, b) = 0 \text{ for all } f \in I\}.$$

   (a) Prove that if $I = (f_1, \ldots, f_n)$ then $V(I) = \{(a, b) \in \mathbb{R}^2 : f_i(a, b) = 0 \text{ for all } i = 1, \ldots, n\}$.

   (b) Draw pictures of $V(I)$ for $I = (y(y - x^2))$ and for $I = (x - y, y - x^3)$.

   (c) Prove that if $I_1 \subseteq I_2$ are ideals of $\mathbb{R}[x, y]$ then $V(I_1) \supseteq V(I_2)$.

   (d) Using part (c) to help, prove the identities

$$V(I + J) = V(I) \cap V(J) \quad \text{and} \quad V(IJ) = V(I \cap J) = V(I) \cup V(J).$$

   Check your results in part (b) accordingly.

Solution. I will prove the second statement of (d) only and leave the rest to you. This is the statement that

$$V(IJ) = V(I \cap J) = V(I) \cup V(J).$$

To prove it, let us begin by noting

$$IJ \subseteq I \cap J \subseteq I \quad \text{and} \quad IJ \subseteq I \cap J \subseteq J.$$

So by part (c), we have

$$V(IJ) \supseteq V(I \cap J) \supseteq V(I) \cup V(J).$$

It remains only to prove

$$V(IJ) \subseteq V(I) \cup V(J).$$

Suppose there is a point $(a, b) \in \mathbb{R}^2$ in neither $V(I)$ nor $V(J)$. This means there exists $f \in I$ and $g \in J$ with $f(a, b) \neq 0$ and $g(a, b) \neq 0$. Therefore $(fg)(a, b) \neq 0$. Since $fg \in IJ$, we conclude $(a, b) \notin V(IJ)$, as desired.

Problem Set 11

2. Let K be a field. Prove that $K[[x]]$ is a Euclidean domain with respect to the following norm: $N(0) = 0$, and for all nonzero $p \in K[[x]]$, $N(p)$ is the *order* of p, i.e. the smallest exponent appearing in p.

   Solution. First, we claim the following, using what you know about $K[[x]]$ from last week's homework: if $f, g \in K[[x]]$ are nonzero power series, then $g|f$ if and only if $\text{ord}(f) \geq \text{ord}(g)$.

   I leave the proof of the above claim to you.

   Now, suppose $f, g \in K[[x]]$ and $g \neq 0$. If $f = 0$ then

   $$f = 0 \cdot g + 0.$$

   If $f \neq 0$ and $\text{ord}(f) < \text{ord}(g)$, then

   $$f = 0 \cdot g + f.$$

   Finally, if $f \neq 0$ and $\text{ord}(f) \geq \text{ord}(g)$, then

   $$f = h \cdot g + 0$$

   for some h, by the claim above. In each case, the Euclidean property is satisfied.

   (By the way, this problem is an instance of the more general statement that *discrete valuation rings* are Euclidean domains).

4. Compute a gcd of $4 + 2i$ and $5i$ in $\mathbb{Z}[i]$. Identifying $\mathbb{Z}[i]$ with the integer lattice points in the complex plane, draw a picture of the elements of the ideal $(4 + 2i, 5i)$.

   Solution. We have

   $$\begin{aligned} 5i &= i(4 + 2i) + (2 + i) \\ 4 + 2i &= 2(2 + i) + 0 \end{aligned}$$

   So $2 + i$ is a gcd, and the ideal $(4 + 2i, 5i) = (2 + i)$ looks like a square lattice, generated additively by $2 + i$ and $-1 + 2i$.

5. Let R be an integral domain. We defined the *field of fractions* K, whose elements are equivalence classes of $\{(a, b) \colon a, b \in R, b \neq 0\}$ where $(a, b) \sim (c, d)$ if $ad = bc$. We write a/b for the class of (a, b). We defined

   $$a/b + c/d = (ad + bc)/bd, \qquad a/b \cdot c/d = (ac)/(bd).$$

   Convince yourself that $+$ and $\cdot$ are well-defined and make K into a field with $0 = 0/1$ and $1 = 1/1$ (ungraded).

(a) Prove that the map $i\colon R \to K$ given by $i(r) = r/1$ is a ring homomorphism sending all nonzero elements to units.

Solution. Given $r, r' \in R$, we check

$$i(r + r') = (r + r')/1 = r/1 + r'/1 = i(r) + i(r')$$

and

$$i(rr') = (rr')/1 = i(r)i(r').$$

Moreover if $r \neq 0$ then $r/1$ is a unit since $r/1 \cdot 1/r = 1$.

(b) Prove the following *universal property of localization*: Let S be a commutative ring with 1. If $f\colon R \to S$ is any ring homomorphism sending all nonzero elements of R to units of S, then there is a unique ring homomorphism $\widetilde{f}\colon K \to S$ such that

$$f = \widetilde{f} \circ i.$$

Solution. First we establish that $f(1) = 1$. We have

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1).$$

But $f(1)$ is a unit in S by assumption, so we conclude $1 = f(1)$.

Next, if $\widetilde{f}\colon K \to S$ is a ring homomorphism satisfying the conditions above, then $\widetilde{f}(r/1) = f(r)$ for all $r \neq 0$. This implies

$$\widetilde{f}(r/1) \cdot \widetilde{f}(1/r) = \widetilde{f}(1) = f(1) = 1,$$

and since $\widetilde{f}(r/1) = f(r)$ is assumed to be a unit, the equation above implies $\widetilde{f}(1/r) = f(r)^{-1}$. Therefore, for all $r, s \in R$ with $r \neq 0$,

$$\widetilde{f}(s/r) = \widetilde{f}(s/1 \cdot 1/r) = f(s)f(r)^{-1}.$$

This shows uniqueness of $\widetilde{f}$, if it exists.

Finally, we check existence, i.e. that $\widetilde{f}(s/r) := f(s)f(r)^{-1}$ really is a well-defined ring homomorphism with $f = \widetilde{f} \circ i$. Suppose $s'/r' = s/r$, so $s'r = sr'$. Then $f(s')f(r) = f(s)f(r')$, and

$$f(s')f(r')^{-1} = f(s)f(r)^{-1},$$

which shows that $\widetilde{f}$ is well-defined. I leave it to you to check that $\widetilde{f}$ is a ring homomorphism with $f = \widetilde{f} \circ i$.

Problem Set 12

1. Let $R = \{(a_1, a_2, a_3, \ldots) : a_i \in \mathbb{Z}\}$, i.e., R is the ring of infinite tuples of $\mathbb{Z}$, indexed by the positive integers, with coordinatewise addition and multiplication. For each $j = 1, 2, \ldots$ let

$$I_j = \{(a_1, a_2, a_3 \ldots) \in R : a_i = 0 \text{ for all } i \geq j.\}$$

   (a) Show that the I_j are principal ideals forming an ascending chain $I_1 \subsetneq I_2 \subsetneq \cdots$ that doesn't stabilize. Conclude that $I = \bigcup_{j \geq 1} I_j$ an ideal that is not finitely generated.

   Solution. Write e_j for the element which is j ones followed by all zeroes. Note that $I_j = \{(a_1, a_2, \ldots) \cdot e_j : a_i \in \mathbb{Z}\} = (e_j)$, so in particular I_j is a principal ideal.
   For each j, we have $I_j \subsetneq I_{j+1}$ directly from the definitions; in particular $e_{j+1} \in I_{j+1} \setminus I_j$ shows that I_j is properly contained in I_{j+1}.
   Therefore I is not finitely generated, since if instead $I = (f_1, \ldots, f_n)$, then there are indices $j_1, \ldots, j_n$ such that $f_i \in I_{j_i}$. Let $j = \max(j_1, \ldots, j_n)$. Then $f_1, \ldots, f_n \in I_j$. But this would imply that $I_j = I$, contradicting that the ideals $I_{j+1}, I_{j+2}, \ldots$ are strictly bigger than I_j.

   (b) Is I prime?

   Solution. No. Note that I consists of those sequences of integers which are eventually zero. Then writing $a = (1, 0, 1, 0, \ldots)$ and $b = (0, 1, 0, 1, \ldots)$, we have $ab = 0 \in I$ but $a, b \notin I$.

3. Convince yourself that the polynomial $x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. Write out the multiplication table for the 8-element field $K = \mathbb{F}_2[x]/(x^3 + x + 1)$, and check that the multiplicative group of nonzero elements in K is isomorphic to $\mathbb{Z}/7\mathbb{Z}$.

   Solution. If $x^3 + x + 1$ were reducible, then one of its factors would have to have degree 1, since it has degree 3, i.e. it would have a solution over $\mathbb{F}_2$. But it doesn't (as seen by plugging in 0 and 1.)

   The elements of K are (the classes of)

$$0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1.$$

   I leave the full multiplication table to you, but here is one example. Let us compute $x^2 \cdot (x^2+1)$ in K. We use the division algorithm, dividing $x^4 + x^2$ by $x^3 + x + 1$ to get

$$x^4 + x^2 = x(x^3 + x + 1) + x$$

So in K, we have $x^2 \cdot (x^2+1) = x$.

4. For K a field of characteristic $p > 0$, we define the *Frobenius map* $e\colon K \to K$ by $e(a) = a^p$. Show that e is a homomorphism. (To show that $e(a+b) = e(a)+e(b)$ you may wish to appeal to the Binomial Theorem.)

   Also, compute what e does to each element of the field K from Problem 3.

   Solution. We have $e(ab) = (ab)^p = a^p b^p = e(a)e(b)$ by commutativity of multiplication. Next, we have

   $$(a+b)^p = a^p + (\text{stuff}) + b^p,$$

   where the stuff in the middle consists of terms of the form $\binom{p}{i} \cdot a^i b^{p-i}$ where

   $$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

   (To be clear, by $\binom{p}{i}$ we officially mean $1 + \cdots + 1 \in K$ where there are $\binom{p}{i}$ summands. The integer $\binom{p}{i}$ is a multiple of p, since the numerator has a factor of p but not the denominator. Since k has characteristic p, we conclude that $(a+b)^p = a^p + b^p$.

   As for the specific field K from problem 3, I computed that e sends the elements

   $$0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1$$

   to

   $$0,\ 1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1,\ x,\ x+1$$

   respectively.

   (In particular, you may check that e is actually an *automorphism* of K whenever K is a finite field.)