

MATH113 PROBLEMS: HOMEWORK 6 (DUE MON. JULY 31)

(1) Some facts about ideals. Let I and J be ideals in a commutative ring R with unit.

(a) If $1 \in I$, what can you say about I ?

Solution: Claim: $1 \in I \iff I = R$. Proof: If $I = R$, then clearly $1 \in I$. If $1 \in I$, then by “super-extra closure”, for any $r \in R$, we have $r \cdot 1 \in I$, so $R \subset I$, and so $I = R$.

(b) §4.3 #6 Show that $I \cap J$ is an ideal of R .

Solution: I and J are subgroups, and the intersection of two subgroups is also a subgroup, so $I \cap J$ is a subgroup. So all we need to check is the “super-extra closure” property. Let $x \in I \cap J$, and let $r \in R$. Then $x \in I$, so by super-extra closure of I , $rx \in I$. Likewise, $x \in J$, and so by super-extra closure of J , $rx \in J$. Thus $rx \in I \cap J$, and hence $I \cap J$ is super-extra closed under multiplication.

(c) §4.3 #4 Define $I + J = \{i + j \mid i \in I, j \in J\}$. Show that $I + J$ is an ideal of R .

Solution: It may not look like it, but we have actually shown that this thing is a subgroup a long time ago: Recall if $K \triangleleft G$ and H is any subgroup of G , then HK is a subgroup of G . But now we’re dealing with rings, so the group operation is addition, and since the group is abelian, every subgroup is normal. I and J are (normal) subgroups of the group $R, +$, and so $I + J$ is a subgroup. So we only need to check the super-extra closure under multiplication: Let $x \in I + J$, and let $r \in R$. Then we can write $x = a + b$ for $a \in I$ and $b \in J$. Thus $rx = r(a + b) = ra + rb$, and by super-extra closure of I and J , $ra \in I$ and $rb \in J$, so $rx \in I + J$. Thus $I + J$ is an ideal. Note $I + J$ is the smallest ideal that contains all the elements from I and all the elements from J (can you prove this?). A good name for it might be “the ideal generated by the ideals I and J .”

(d) §4.3 #15 Define $IJ = \{i_1j_1 + \dots + i_nj_n \mid n \in \mathbb{Z}^+, i_k \in I, j_k \in J\}$. I.e. IJ is the set of all the elements of R which can be written as a finite sum of elements of the form ij for $i \in I$ and $j \in J$. Show that IJ is an ideal of R . Why don’t we define IJ as $\{ij \mid i \in I, j \in J\}$?

Solution: Nuts! This example is not going to be a subgroup for free - you can tell this immediately, since it’s defined using the multiplication from our ring, which didn’t even exist when we were treating R as a group (when it only had addition!). Claim: IJ is a subgroup. Proof: Let $x, y \in IJ$. Then $x = i_{1_x}j_{1_x} + \dots + i_{n_x}j_{n_x}$, and $y = i_{1_y}j_{1_y} + \dots + i_{m_y}j_{m_y}$, for i ’s in I and j ’s in J . Then (A) we have closure under addition since

$$x + y = i_{1_x}j_{1_x} + \dots + i_{n_x}j_{n_x} + i_{1_y}j_{1_y} + \dots + i_{m_y}j_{m_y} \in IJ$$

(B) Associativity is for free. (C) $0 = 0 \cdot 0 \in IJ$, so the zero is in IJ . Finally, (D) $-x = -(i_{1_x}j_{1_x} + \dots + i_{n_x}j_{n_x}) = (-i_{1_x})j_{1_x} + \dots + (-i_{n_x})j_{n_x}$, which is in IJ , since I is a subgroup, and hence closed under taking (additive) inverses. Therefore, IJ is a subgroup of R . Claim: IJ is super-extra closed under multiplication. Proof: Let $x \in IJ$ be as above, and let $r \in R$, then

$$rx = r(i_{1_x}j_{1_x} + \dots + i_{n_x}j_{n_x}) = (ri_{1_x})j_{1_x} + \dots + (ri_{n_x})j_{n_x} \in IJ$$

since I is an ideal, and super-extra closed under multiplication.

It would be a bad idea to forget that IJ contains all SUMS of products ij , because if you try to define $IJ = \{ij \mid i \in I, j \in J\}$, then it’s not guaranteed to be closed under addition. (We don’t have any reason to believe that $i_1j_1 + i_2j_2$ is a product of something from I with something from J .)

- (2) What are all the ring homomorphisms from $\mathbb{Z} \times \mathbb{Z}$ to itself?

Solution: Let $\phi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ be a homomorphism of rings. Suppose $\phi((1, 0)) = (a, b)$ and $\phi((0, 1)) = (c, d)$. Then, for any element (x, y) in the domain, we see that

$$\phi((x, y)) = \phi(x \cdot (1, 0) + y \cdot (0, 1)) = x \cdot (a, b) + y \cdot (c, d) = (xa + yc, xb + yd)$$

So any such homomorphism is completely determined by its values at $(1, 0)$ and $(0, 1)$. Moreover, we are restricted in our choices for a, b, c and d . Since ϕ is a homomorphism:

$$(a^2, b^2) = (a, b)(a, b) = \phi((1, 0))\phi((1, 0)) = \phi((1, 0)(1, 0)) = \phi((1, 0)) = (a, b)$$

Similarly for (c, d) , so a, b, c and d are all integers with the property that $x^2 = x$. The only such integers are 1 and 0. And we are even further restricted,

$$(ac, bd) = (a, b)(c, d) = \phi((1, 0))\phi((0, 1)) = \phi((1, 0)(0, 1)) = \phi((0, 0)) = (0, 0)$$

So at least one of a and c is zero, and at least one of b and d is zero. Here is a table of the possible values of a, b, c and d , and the corresponding image of (x, y) as determined by the images of $(1, 0)$ and $(0, 1)$:

	ϕ_0	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6	ϕ_7	ϕ_8
$\phi((1, 0)) = (a, b)$	(0, 0)	(1, 0)	(1, 0)	(0, 1)	(0, 1)	(1, 1)	(0, 0)	(0, 0)	(0, 0)
$\phi((0, 1)) = (c, d)$	(0, 0)	(0, 0)	(0, 1)	(0, 0)	(1, 0)	(0, 0)	(1, 0)	(1, 1)	(0, 1)
i.e. $\phi((x, y)) = (xa + yc, xb + yd)$	(0, 0)	(x, 0)	(x, y)	(0, x)	(y, x)	(x, x)	(y, 0)	(y, y)	(0, y)

It is straightforward to check that all these maps are homomorphisms. In fact, this is an example of a general idea, namely that if a ring R has a certain set of generators r_1, \dots, r_k , which satisfy certain relations $p_i(r_1, \dots, r_k) = 0$, then we can define a homomorphism $R \rightarrow S$ by specifying s_1, \dots, s_k with $p_i(s_1, \dots, s_k) = 0$. I.e. we get a homomorphism by specifying the images $\phi(r_j) = s_j$, as long as the s_j 's satisfy the same relations as the r_j 's. we can say more about the p_i 's: they are polynomials in their arguments, since the only operations in a ring are multiplication and addition, so the sorts of relations that the r_j 's can satisfy involve just products and sums of the r_j 's.

- (3) Define the map $\phi : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ by $\phi([k]_N) = ([k]_{n_1}, [k]_{n_2})$.

- (a) Show that ϕ is well-defined if and only if $n_1 | N$ and $n_2 | N$.

Solution: Suppose the map is well-defined. I.e. the image of an equivalence class $[k]_N$ doesn't depend on the representative k that we choose. Then in particular, since $0 \equiv N \pmod{N}$, we have

$$([0]_{n_1}, [0]_{n_2}) = \phi([0]_N) = \phi([N]_N) = ([N]_{n_1}, [N]_{n_2})$$

And therefore, $[0]_{n_1} = [N]_{n_1}$ so $n_1 | N$. Similarly, $n_2 | N$. As for the converse, assume that $n_1 | N$ (so $N = xn_1$) and $n_2 | N$ (so $N = yn_2$). If we have two different names for the same equivalence class in the domain, $[k]_N = [k']_N$, i.e. $k' = k + tN$ for some $t \in \mathbb{Z}$, then

$$\phi([k']_N) = \phi([k + tN]_N) = ([k + txn_1]_{n_1}, [k + tyn_2]_{n_2}) = ([k]_{n_1}, [k]_{n_2}) = \phi([k]_N)$$

Therefore the map is well-defined.

- (b) Show that ϕ is an isomorphism of rings if and only if $(n_1, n_2) = 1$ and $N = n_1n_2$.

Solution: First we check that the map is a homomorphism of groups: let $[k]_N$ and $[k']_N$ be elements of the domain, $\mathbb{Z}/N\mathbb{Z}$

$$\phi([k]_N) + \phi([k']_N) = ([k]_{n_1}, [k]_{n_2}) + ([k']_{n_1}, [k']_{n_2}) = ([k + k']_{n_1}, [k + k']_{n_2}) = \phi([k + k']_N)$$

And similarly, ϕ is a homomorphism of rings since in addition we have:

$$\phi([k]_N) \cdot \phi([k']_N) = ([k]_{n_1}, [k]_{n_2}) \cdot ([k']_{n_1}, [k']_{n_2}) = ([kk']_{n_1}, [kk']_{n_2}) = \phi([kk']_N)$$

Now we claim that ϕ is one-to-one. It was a very good idea to do the ‘homomorphism’ part of the proof first, since now we can apply our favorite characterization of 1-1 homomorphisms, namely: ϕ is 1-1 if and only if the kernel is trivial. Suppose $0 = \phi([k]_N) = ([k]_{n_1}, [k]_{n_2})$, then we must have $n_1|k$ and $n_2|k$. Since (n_1, n_2) are relatively prime, we must have $N = n_1n_2|k$, and therefore $[k]_N = [0]_N$. So the kernel of the homomorphism is trivial, and thus ϕ is one-to-one. Since $\mathbb{Z}/N\mathbb{Z}$ has the same (finite) number of elements as $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$, and ϕ is a one-to-one map, ϕ is also onto. (This is an example of the pigeon-hole principle at work, and I gave you this fact on the hints page.) Therefore, ϕ is an isomorphism. This is a quite important theorem that you have just proved! You have just shown that given some $(a, b) \in \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ there is a unique $[k]_N$ with $([k]_{n_1}, [k]_{n_2}) = (a, b)$. In other words if you want to solve the system of equations:

$$\begin{aligned} x &\equiv a \pmod{n_1} \\ x &\equiv b \pmod{n_2} \end{aligned} \quad \text{with } (n_1, n_2) = 1$$

Then there is exactly one solution x between 0 and $n_1n_2 - 1$, i.e. a unique solution $(\text{mod } n_1n_2)$. This theorem is usually called the Chinese Remainder Theorem.

- (4) Let R be a commutative ring with unit. Let I be an ideal of R . Show that I is a maximal ideal if and only if for any $r \in R - I$ there are $x \in R$ and $y \in I$ with $rx + y = 1$.

Solution: A very good way to do this problem is to remember that one of our characterizations of maximal ideals (in commutative rings with unitS) is that their quotients are fields. If I am very clever, (and careful to make sure that all my arguments are ‘ifs and only ifs’) then I’ll be able to argue both directions at once. Since I is an ideal of R , consider the quotient ring R/I . Then because R is commutative with unit, I is maximal if and only if R/I is a field. R/I is a field if and only if each non-zero coset $r + I$ (i.e. $r \notin I$) is invertible, i.e. there is a coset $x + I$ with $(r + I)(x + I) = rx + I = 1 + I$. Since rx and 1 represent the same coset, they differ by an element in I , i.e. $rx - 1 = y \in I$. Therefore, I is maximal if and only if for each $x \in R - I$ there is an $r \in R$ and a $y \in I$ with $rx + y = 1$.

- (5) Let $R = \mathbb{Z}/3\mathbb{Z}$.

- (a) Show that the polynomial $x^3 + x^2 + 2x + 1$ is irreducible in $R[x]$.

Solution: Let $f = x^3 + x^2 + 2x + 1$. Since f has degree ≤ 3 , it is irreducible if and only if it has no roots. So all we need to do to check irreducibility is to make sure that f has no roots in R , namely, that when we evaluate f at each of the (three) values in $\mathbb{Z}/3\mathbb{Z}$ we don’t get zero. It’s straightforward to calculate $f(0) = 1$, $f(1) = 2$, $f(2) = f(-1) = -1 = 2$. Therefore f has no roots in R , and is thus irreducible over R .

- (b) Prove that $F = R[x]/(x^3 + x^2 + 2x + 1)$ is a field.

Solution: We showed in class that in a principal ideal domain, an ideal is maximal if and only if it is generated by an irreducible element. R is a field, so $R[x]$ is a PID, and f is irreducible, so the principal ideal (f) is maximal, so $R[x]/(f)$ is a field.

- (c) How many elements are in F ?

Solution: The idea of the solution is important since it involves counting cosets: The elements of F are the cosets of (f) in $R[x]$. A coset of (f) looks like $g + (f)$ for some polynomial $g \in R[x]$. But, as usual, we will have some repetition (quite a lot, actually) in the names of the cosets. $g + (f) = g' + (f)$ if and only if $g - g' \in (f)$, if and only if $f | g - g'$. If g and g' are different polynomials, and have degrees less than 3, then their difference has degree less than three, and hence f cannot possibly divide their difference. There are 27 distinct polynomials of degree < 3 in $\mathbb{Z}/3\mathbb{Z}[x]$ (such a polynomial looks like $r_2x^2 + r_1x + r_0$, where there are three possible values ($[0]_3, [1]_3, [2]_3$) for each of the r 's.) Now I claim that these are enough representatives for ALL the cosets of (f) . Suppose we have some other coset $g + (f)$ (with degree $g \geq 3$). Then by the division algorithm for (polynomials over a field) we get $g = qf + r$ with $\deg(r) < \deg(f) = 3$, hence $g - r = qf \in (f)$, and therefore $g + (f) = r + (f)$. So all the polynomials of degree ≥ 3 represent cosets we already saw by considering representatives of degree less than 3. Therefore there are 27 elements in this field! I was talking with some students the other day, who noticed that 'we haven't seen very many rings - just $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, M_{n \times n}$, and some fields like \mathbb{R}, \mathbb{Q} . But actually, we have seen many more rings than that, because we can get new (and very interesting) rings by looking at subrings, direct products, and (most importantly?) quotients by ideals. The rings $\mathbb{F}[x]/I$ for an ideal I in $\mathbb{F}[x]$ are especially near and dear to my heart, and the hearts of all algebraic geometers, and I'd love to tell you a little more about this if you're interested: Please come ask me (sometime when you're not studying furiously for a midterm)!

- (d) Find the multiplicative inverse of the element $[x^2 - 2x + 1]$ in F

Solution: $-2 = 1$ in $\mathbb{Z}/3\mathbb{Z}$, so we might as well write $[x^2 + x + 1]$ instead of the notation we're given. I'm about to use the Euclidean algorithm to find the gcd of $x^2 + x + 1$ and $x^3 + x^2 + 2x + 1$. Then I'll reverse the steps to write the gcd as a sum $(x^2 + x + 1, x^3 + x^2 + 2x + 1) = p(x^2 + x + 1) + q(x^3 + x^2 + 2x + 1)$. Even if I weren't long-division-challenged, I wouldn't be able to typeset my long-division - and anyway, I just guessed and checked these divisions... but you should make sure that you can do long-division (even in $\mathbb{Z}/3\mathbb{Z}[x]$, and come to ask me in office hours if you can't figure it out! Using the Euclidean algorithm, we get:

$$\begin{aligned} x^3 + x^2 + 2x + 1 &= (x) \cdot [x^2 + x + 1] + (x + 1) \\ x^2 + x + 1 &= (x) \cdot [x + 1] + 1 \end{aligned}$$

So the gcd is 1, and reversing the steps, we get

$$\begin{aligned} 1 &= (x^2 + x + 1) - (x)(x + 1) \\ &= (x^2 + x + 1) - x[(x^3 + x^2 + 2x + 1) - (x)(x^2 + x + 1)] \\ &= (x^2 + 1)[x^2 + x + 1] + x[(x^3 + x^2 + 2x + 1)] \end{aligned}$$

Therefore, $(x^2 + 1)(x^2 - 2x + 1) \equiv 1 \pmod{x^3 + x^2 + 2x + 1}$
I.e. $[x^2 - 2x + 1]^{-1} = [x^2 + 1]$ in $\mathbb{Z}/3\mathbb{Z}[x]/\langle x^3 + x^2 + 2x + 1 \rangle$.

(6) Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$:

(a) $x^5 + 75x^4 + 30x + 60$

Solution: Consider the prime 5. We have $5 \nmid 1, 5|75, 5|30, 5|60$ and $5^2 \nmid 60$, so this polynomial is irreducible in $\mathbb{Z}[x]$ by Eisenstein's Criterion. Because it's monic, it is also irreducible in $\mathbb{Q}[x]$ by Gauss's Lemma.

(b) $x^3 + 15x^2 + 28x + 7$

Solution: Consider $x^3 + 15x^2 + 28x + 7$ as a polynomial in $\mathbb{Z}[x]$. We need to do this to use the reduction of coefficients method, since there's no map from \mathbb{Q} to $\mathbb{Z}/n\mathbb{Z}$! Consider the reduction of coefficients mod 3, then we get the polynomial $g = x^3 + 2x + 1$ in $\mathbb{Z}/3\mathbb{Z}$, which has the same degree as the one we started with. So if we show that this new polynomial is irreducible, we will know that the original one is too. Luckily, the polynomials we are looking at have degree less than four, so we can check for irreducibility just by making sure that the new polynomial has no roots: $g(0) = 1, g(1) = 1, g(2) = 1$. So g has no roots, and is therefore irreducible. Therefore $x^3 + 15x^2 + 28x + 7$ is irreducible in $\mathbb{Z}[x]$, and hence in $\mathbb{Q}[x]$ by Gauss's Lemma.

(c) $x^4 + 2x^3 + 10x^2 + x + 1$

Solution: Consider the polynomial $h = x^4 + 2x^3 + 10x^2 + x + 1$ as a polynomial in $\mathbb{Z}[x]$. Now reduce the coefficients mod 2 to get the new polynomial $h_2 = x^4 + x + 1 \in \mathbb{Z}/2\mathbb{Z}$. By checking $h_2(0) = 1, h_2(1) = 1$, we see that h_2 has no roots in $\mathbb{Z}/2\mathbb{Z}$ BUT THIS IS NOT enough to show that h_2 is irreducible, since it has degree greater than 3. It does tell us, however, that h_2 doesn't have any linear factors, so if it does factor, the factorization looks like

$$h_2 = (ax^2 + bx + c)(a'x^2 + b'x + c') \quad \text{for } a, b, c, a', b', c' \in \mathbb{Z}/2\mathbb{Z}$$

h_2 is monic, so we must have $aa' = 1$, and thus $a = a' = 1$ (the only invertible element in $\mathbb{Z}/2\mathbb{Z}$). Similarly, $cc' = 1$ so $c = c' = 1$. So the only possible factorization of h_2 looks like

$$x^4 + x + 1 = (x^2 + bx + 1)(x^2 + b'x + 1) = x^4 + (b + b')x^3 + (bb')x^2 + (b + b')x + 1$$

But this can't possibly be the factorization of h , since it's coefficients of x and x^3 are equal, whereas h_s 's are certainly not! So h_2 is irreducible, and by the reduction of coefficients method, h is irreducible in $\mathbb{Z}[x]$, hence it's irreducible in $\mathbb{Q}[x]$ by Gauss's Lemma.