Math 123 HW 3 Solutions

Eric Shen

February 2023

1 Problem 1

Author's Solution:

$p(x) = (x+2)(x^3+x+1)$ while $q(x) = (2x+1)(x^3+x+1)$ (we may find this through the Euclidean Algorithm), so thus $\gcd(p,q) = x^3+x+1$.

2 Problem 2

Author's Solution:

$\mathbb{Q}[x]$ is a PID, so $(p,q) = (r)$ for some $r \in \mathbb{Q}[x]$. By Bezout we may write $r = ap+bq$ for some $a, b \in \mathbb{Q}[x]$. Now $r(z) = ap(z)+bq(z) = 0$, so r is nonconstant. However r also divides p and q, so since p, q are irreducible we must have $p = r = q$ as desired.

2.1 Warning

A common mistake on this problem was confusing the irreducibles of $\mathbb{C}[x]$, $\mathbb{R}[x]$, and $\mathbb{Q}[x]$. As a reminder:

1. The nonzero constants of $\mathbb{K}[x]$ (K field) are *never* irreducibles, and *always* units.
2. The irreducibles of $\mathbb{C}[x]$ are the linear polynomials $(x-a)$. These polynomials are evidently irreducible as the nonzero degree 0 polynomials are all units, and moreover every other polynomial is not an irreducible by the Fundamental Theorem of Algebra.
3. The irreducibles of $\mathbb{R}[x]$ are the the linear polynomials $(x-a)$ where $a \in \mathbb{R}$, and the quadratic polynomials (x^2+ax+b) with negative discriminant. These polynomials are evidently irreducible (over $\mathbb{C}[x]$ you can only factor the latter into two non-real polynomials), and they're the only irreducibles as we can always factor out either a real root or a pair of complex conjugate complex roots out of a real polynomial.
4. The irreducibles of $\mathbb{Q}[x]$ are dramatically more interesting. In particular, as we've discovered with Eisenstein's criterion, $x^n - 2$ is always an irreducible polynomial. This will become much of the content of our discussion in our coming weeks.

On this front, we should also distinguish the notion of factoring in these rings. We can always factor out a root z of a polynomial $p(x)$ in $\mathbb{C}[x]$, by writing $p(x) = q(x)(x-z)$. But if $z \in \mathbb{C}$ and $p \in \mathbb{Q}[x]$, it does not need to be true that $q \in \mathbb{Q}[x]$ (and indeed this is often not true; i.e. $z = \sqrt{2}$, $p = x^2 - 2$.) This is also part of why we define the minimal polynomial, as this represents the polynomial which we can "factor" out when we know an algebraic number is a root. But for the purposes of this problem this means we cannot just talk about factoring in $\mathbb{Q}[x]$ so nicely.

3 Problem 3

Author's Solution:

Assume FTSOC $(2, x) = (p)$ for some $p \in \mathbb{Z}[x]$. The leading coefficient of any nonzero polynomial in (p) is divisible by the leading coefficient of p, so thus p has leading coefficient ± 1. Also, any nonzero multiple of p must have degree at least the degree of p, so thus p has degree 0. Thus $p = \pm 1$, but note that $r(0)$ is even for all polynomials in I while this is false for p, hence contradiction. Thus $(2, x)$ is not a principal ideal as desired.

3.1 Remark

For any $a_1, \ldots a_n \in A$, $(a_1, \ldots a_n)$ is always just the ideal $a_1A + \ldots + a_nA = \{a_1b_1 + \ldots + a_nb_n : b_1, \ldots b_n \in A\}$ (do you see why this is true?) But you need not prove this, and can assume this on future PSets.

4 Problem 4

Author's Solution:

(i) If $J = \langle I, f \rangle = A$, then there exists $i \in I$, $a \in A$ such that $i + af = 1$. But then $ig + afg = g$, but the LHS is in I while the RHS is not, a contradiction. Therefore $J \neq A$ as desired.

(ii) If a maximal ideal J is not prime then there exists $f, g \notin J$ such that $fg \in J$. But then by part (i) we have that $J \subsetneq \langle J, f \rangle \subsetneq A$, contradicting the maximality of J. Hence J is prime as desired.

5 Problem 5

Author's Solution:

Let $\overline{q}$ denote the image of q in $\mathbb{Z}[x]/(p)$. Then note that $\overline{x}(\overline{-x^2 - 5}) = \overline{-x^3 - 5x} = \overline{1}$ in $\mathbb{Z}[x]/(p)$, so thus $\overline{x}$ is a unit in $\mathbb{Z}[x]/(p)$.

6 Problem 6

Author's Solution:

We first prove that p has infinitely many zeroes. Note that p is nonconstant. If p has no monomial terms in (y) then evidently it has some root α in x, and now $p(\alpha, y) = 0$ for all y. Otherwise we may write $p(x,y) = \sum_{i=0}^{k} p_i(x)y^i$, where $k > 0$ and $p_k(x)$ is nonzero. Now $p_k(\alpha) = 0$ for all but finitely many α, and for any such α, $p(\alpha, y)$ has at least one root in y. Thus p has infinitely many roots, as desired.

Now, by **Artin Theorem 11.9.10**, since both p and f share infinitely many roots, we have that they have a common factor in $\mathbb{C}[x,y]$. But p is irreducible so this implies $p|f$ as desired.

6.1 Remark

In class we discussed the Nullstellensatz, which we claimed was the statement that the maximal ideals of $A = \mathbb{C}[x_1, \dots x_n]$ are precisely the ideals $(x_1 - a_1, \dots x_n - a_n)$, where $a_i \in \mathbb{C}$. But this is not the canonical statement of the Nullstellensatz. To understand the usual statement, we first define

- For any ideal $I \subset A$, $V(I) \subset \mathbb{C}^n$ is the "vanishing locus" of I; i.e. the set of points at which every polynomial in I vanishes.
- For any subset $V \subset \mathbb{C}^n$, $I(V)$ is the ideal of polynomials which vanish at all points in V.

It is a natural question to ask what $I(V(J))$ is for any ideal J; that is, what is the ideal of polynomials which vanish at the places where J vanishes? This is not always equal to J; indeed, if $J = (x)^2$ then evidently (x) also vanishes in the same place. But this reduction is all you need: if we define $\sqrt{J} = \{f : f^k \in J \text{ for some } k \in \mathbb{Z}^+\}$, then the usual (full) Hilbert's Nullstellensatz states that

$$I(V(J)) = \sqrt{J}$$

There is also a weak form of Hilbert's Nullstellensatz, which states that if $V(J) = \emptyset$ then $J = A$. Evidently this follows from the full Nullstellensatz (as everything vanishes on nothing, so $\sqrt{J} = I(V(J)) = A \implies J = A$), and in fact this also follows from *our version* of the Nullstellensatz (as every other ideal is contained in some maximal ideal, and hence contains the vanishing locus of the maximal ideal, which is a point.) But in fact this Weak Nullstellensatz is also equivalent to the full Nullstellensatz, by what is known as the *Rabinowitsch trick.* You can learn a lot more about this in i.e. Wikipedia, but if you really like this stuff you should take Math 137.