Homework 1

MATH 322 **Solutions** Due: Wednesday, January 23

(5pts) 1. Find a single generator for the smallest ideal in $\mathbb{Q}[x]$ which contains the polynomials x^3+3x^2+3x+2 and $2x^3-3x^2-11x+6$. Explain how you know that this generator is in the ideal.

> **Solution:** Both polynomials are multiples of $x+2$, which we can find using the Euclidean Algorithm. In fact, doing this gives $91/81x+182/81$, but this is a multiple of the simpler $x+2$. We know that $x+2$ is in the ideal generated by the two polynomials because we can write it as a combination of them using Bezout's lemma. Really, this is because in each stop of the Euclidean Algorithm, we have $a(x) = q(x)b(x) + r(x)$. We have that $a(x)$ and $b(x)$ are in the ideal, so therefore $r(x) = a(x) - q(x)b(x)$ is as well.

(9pts) 2. Consider the polynomial $p(x) = x^3 - 5$ in $\mathbb{Q}[x]$.

(a) Explain how we know that the quotient ring $\mathbb{Q}[x]/\langle x^3-5\rangle$ is actually a field. That is, show that every non-zero element of the quotient ring has a multiplicative inverse. Hint: you will want to use Bezout's lemma.

> **Solution:** Let $a(x)$ be a polynomial in $\mathbb{Q}[x]$ which is not in $\langle x^3-5\rangle$, so that $\langle x^3-5\rangle + a(x) \neq \langle x^3-5\rangle$ (the zero element). We will show that $\langle x^3-5\rangle + a(x)$ has a multiplicative inverse.
>
> Since $a(x) \notin \langle x^3-5\rangle$ we know that $a(x)$ is not a multiple of x^3-5. Since x^3-5 is irreducible, this tells us that $a(x)$ and x^3-5 have gcd 1. Thus by Bezout's lemma there are polynomials $s(x)$ and $t(x)$ such that
>
> $$(x^3-5)s(x) + a(x)t(x) = 1$$
>
> But this says that
>
> $$1 \in \langle x^3-5\rangle + a(x)t(x) = (\langle x^3-5\rangle + a(x))(\langle x^3-5\rangle + t(x))$$
>
> so $(\langle x^3-5\rangle + a(x))(\langle x^3-5\rangle + t(x)) = \langle x^3-5\rangle + 1$. But $\langle x^3-5\rangle + 1$ is the multiplicative identity, so we have found an inverse for $\langle x^3-5\rangle + a(x)$.

(b) Let $E = \{a + b\sqrt[3]{5} + c\sqrt[3]{5}^2 \ : \ a,b,c \in \mathbb{Q}\}$. How does this set relate to the field $\mathbb{Q}[x]/\langle x^3-5\rangle$? Be explicit (for example, if you say they are isomorphic, give the isomorphism).

> **Solution:** Using our notation, we have the $E = \mathbb{Q}(\sqrt[3]{5})$ which we know is isomorphic to $\mathbb{Q}[x]/\langle x^3-5\rangle$ by the Fundamental Homomorphism Theorem. The homomorphism from $\mathbb{Q}[x]$ onto E is given by the evaluation map which sends a polynomial $a(x)$ to $a(\sqrt[3]{5})$. The kernel of this homomorphism is the set of polynomials which have $\sqrt[3]{5}$ as a root. In other words, all multiples of the minimum polynomial x^3-5.
>
> So what is the isomorphism from $E \to \mathbb{Q}[x]/\langle x^3-5\rangle$? Well we need to send elements of E to cosets. Define:
>
> $$a + b\sqrt[3]{5} + c\sqrt[3]{5}^2 \quad \rightsquigarrow \quad \langle x^3-5\rangle + a + bx + cx^2$$

Notice that going backwards is exactly the evaluation map of "plugging in $\sqrt[3]{5}$ into $a(x)$" - the exact same map we defined for the homomorphism, only this time we are grouping all elements that are equivalent modulo $\langle x^3 - 5\rangle$.

(c) Find the element of E (in $a + b\sqrt[3]{5} + c\sqrt[3]{5}^2$ form) equal to $1/(3 - 2\sqrt[3]{5} + \sqrt[3]{5}^2)$ using polynomials. That is, use the relationship you described in part (b) so you can work in $\mathbb{Q}[x]/\langle x^3 - 5\rangle$ instead of in E.

Solution: We want to find the inverse of $\sqrt[3]{5}^2 - 2\sqrt[3]{5} + 3$, which under the isomorphism corresponds to $a(x) = x^2 - 2x + 3$. Apply the Euclidean Algorithm to $a(x)$ and $x^3 - x$:

$$(x^3 - 5) = (x + 2)(x^2 - 2x + 3) + (x - 11)$$

$$x^2 - 2x + 3 = (x + 9)(x - 11) + 102.$$

Solving backwards we get that

$$\begin{aligned} 102 = (x^2 - 2x + 3) - (x + 9)(x - 11) &= (x^2 - 2x + 3) - (x + 9)((x^3 - 5) - (x + 2)(x^2 - 2x + 3)) \\ &= (1 + (x + 9)(x + 2))(x^2 - 2x + 3) - (x + 9)(x^3 - 5) \\ &= (x^2 + 11x + 19)(x^2 - 2x + 3) - (x + 9)(x^3 - 5) \end{aligned}$$

Now if we move back to E (by plugging in $\sqrt[3]{5}$ in for x) we see that

$$102 = (\sqrt[3]{5}^2 + 11\sqrt[3]{5} + 19)(\sqrt[3]{5}^2 - 2\sqrt[3]{5} + 3)$$

so the inverse of $\sqrt[3]{5}^2 - 2\sqrt[3]{5} + 3$ is

$$\frac{1}{102}\sqrt[3]{5}^2 + \frac{11}{102}\sqrt[3]{5} + \frac{19}{102}$$

(6pts) 3. Let A be a commutative ring with unity. Let J be an ideal of A. We say that J is prime provided for any $a, b \in A$, if $ab \in J$ then $a \in J$ or $b \in J$.

(a) Prove that if J is prime, then A/J is an integral domain.

Solution: Suppose J is prime. Consider elements $J+a$ and $J+b$ in A/J, and suppose $(J + a)(J + b) = J$. This says that $ab \in J$, and since J is prime, we can conclude that either $a \in J$ or $b \in J$. But this means either $J + a = J$ or $J + b = J$. This proves that A/J is an integral domain: given that two elements multiply to the zero element, either one or the other is zero, so there are no zero divisors.

(b) Prove that if A/J is an integral domain, then J is prime.

Solution: Suppose A/J is an integral domain. Let $ab \in J$ be given. We have $(J + a)(J + b) = J + ab = J$. But this means that $J + a = J$ or $J + b = J$ (since there are no zero divisors) so either $a \in J$ or $b \in J$.

(8pts) 4. Let A be a commutative ring with unity. An ideal J is *proper* if $A \neq J$. We say that a proper ideal J is *maximal* if no proper ideal of A strictly contains J (that is, if K is a proper ideal of A and $J \subseteq K$ then $J = K$).

(a) Prove that if J is maximal, then A/J is a field (you may assume that A/J is a commutative ring with unity). Here are some hints: first, explain why you want to show that for any $a \notin J$, that there is some element x such that $(J + a)(J + x) = J + 1$. Then let $K = \{xa + j \ : \ x \in A, j \in J\}$, and prove that K is an ideal strictly larger than J. In particular, $1 \in K$. Finally, explain why this is enough to finish the proof.

Solution: We want to show that every non-zero element of A/J has an inverse. So consider such an element $J + a$ (so $a \notin J$, since this should be non-zero). Let $K = \{xa + j \ : \ x \in A, j \in J\}$. First, we claim K is an ideal. It is closed under subtraction: $x_1a + j_1 - (x_2a + j_2) = (x_1 - x_2)a + (j_1 - j_2)$. It also absorbs products: $(xa + j) \cdot b = xab + jb$. This is in K since $xb \in A$ and $jb \in J$ (as J absorbs products).

Further, the ideal K contains J, since for any $j \in J$, $j = 0a + j \in K$. But $K \neq J$ since $1a + 0 = a \notin J$. So K is a strictly larger ideal than J, which implies that $K = A$, since J is maximal. In particular, $1 \in K$, so $1 = xa + j$ for some $x \in A$ and $j \in J$. This means that $1 \in J + ax$ and thus $J + 1 = J + ax = (J + a)(J + x)$. We have found the inverse of $J + a$, it is $J + x$.

(b) Prove that if A/J is a field, then J is maximal.

Solution: Assume A/J is a field. Suppose there is an ideal K containing J but strictly larger (we will show that $K = A$, which shows that J is maximal). So there is some element $a \in K$ not in J. In particular, $J + a \neq J$, so this coset has a multiplicative inverse, call it $J + a'$. We have $(J + a)(J + a') = J + aa' = J + 1$. This tells us that $1 \in J + aa'$ and as such $1 = j + aa'$. But $j \in K$ and $a \in K$ so $1 = j + aa' \in K$. The only ideal that contains 1 is the trivial ideal A, so we are done.

(2pts) 5. Assuming the results from the previous two questions, prove that every maximal ideal is prime. This should be a 3-sentence proof.

Solution: Let J be a maximal ideal. Then A/J is a field, and since every field is an integral domain, A/J is also an integral domain. But then we have that J must be prime.

(3 bns) 6. Bonus: it is not true that every prime ideal is maximal (although this does hold for $\mathbb{Z}$ and for $F[x]$). Find an example of a ring A with an ideal J that is prime but not maximal. Justify your answer. Hint: look at a polymoial ring that for which the coefficients do not belong to a field.

Solution: Consider $\mathbb{Z}[x]/\langle x\rangle$. We can argue that this quotient ring is isomorphic to $\mathbb{Z}$, so we have that $\langle x\rangle$ is not maximal ($\mathbb{Z}$ is not a field). But $\langle x\rangle$ is prime (do you see why?).