Homework 8

Jaden Wang

Problem (1).

(a) First it's clear that $\langle a \rangle + \langle b \rangle = \langle a, b \rangle$. So $\langle 2, x^3+1 \rangle = \langle 2 \rangle + \langle x^3+1 \rangle$. Then by the third isomorphism theorem, FIX: Use Proposition 9.2.

$$\mathbb{Z}[x]/\langle 2, x^3+1 \rangle = \mathbb{Z}[x]/(\langle 2 \rangle + \langle x^3+1 \rangle) \cong \frac{\mathbb{Z}[x]/\langle 2 \rangle}{(\langle 2 \rangle + \langle x^3+1 \rangle)/\langle 2 \rangle} \cong \mathbb{Z}_2[x]/\langle x^3+1 \rangle.$$

By the correspondence theorem, there is a bijection between ideals of $\mathbb{Z}_2[x]/\langle x^3+1 \rangle$ and ideals of $\mathbb{Z}_2[x]$ containing $\langle x^3+1 \rangle$. Since $\mathbb{Z}_2$ is a field, $\mathbb{Z}_2[x]$ is a PID. Suppose $\langle x^3+1 \rangle \subseteq I$ in $\mathbb{Z}_2[x]$, then $I = \langle p(x) \rangle$ and $x^3+1 = a(x)p(x)$ for some $a(x) \in \mathbb{Z}_2[x]$. We see that $x^3+1 = (x+1)(x^2-x+1)$. Since $0, 1$ is not a root of x^2-x+1, x^2-x+1 is irreducible in $\mathbb{Z}_2[x]$. Since $\mathbb{Z}_2[x]$ is a UFD, this is the unique factorization into irreducibles and there is no more factors. Together with the factors 1 and x^3+1, we obtain that $p(x) = 1, x+1, x^2-x+1$, or x^3+1. Therefore, $\langle 1 \rangle = \mathbb{Z}_2[x], \langle x+1 \rangle, \langle x^2-x+1 \rangle$, and $\langle x^3+1 \rangle$ are the only ideals containing $\langle x^3+1 \rangle$ in $\mathbb{Z}_2[x]$, and the corresponding ideals modulo $\langle x^3+1 \rangle$ are the only ideals of $\mathbb{Z}_2[x]/\langle x^3+1 \rangle \cong \mathbb{Z}[x]/\langle 2, x^3+1 \rangle$.

(b) Let $f(x) = x^3+2x+2$. First let's consider the case when $n = 1$. It is easy to see that $\langle 1, f(x) \rangle = \langle 1 \rangle = \mathbb{Z}[x]$ so the quotient is zero which is not a field. Next, I claim that $n \neq 1$ must be a prime for I to be maximal. If n is not prime, then $\mathbb{Z}_n$ contains zero divisors. Let $a, b \in \mathbb{Z}_n$ be zero divisors s.t. $ab = 0$. Then $\overline{a}, \overline{b}$ are zero divisors of $\mathbb{Z}_n[x]/\langle f(x) \rangle$ so it cannot be a field (so I cannot be maximal). Thus by 2a, we only need to check whether $f(x)$ is irreducible for $n = 2, 3, 5, 7$. Note in $\mathbb{Z}[x]$, evaluation yields $f(0) = 2, f(1) = 5, f(2) = 14$. When $n = 2$, $x^3+2x+2 = x^3$ is clearly reducible. If $n = 3$, 0,1,2 are not roots of $f(x)$, so $f(x)$ is irreducible. If $n = 5$, 1 is a root so $f(x)$ is reducible. If $n = 7$, 2 is a root so $f(x)$ is reducible.

In summary, I is maximal iff the quotient is a field only when $n = 3$ for $1 \leq n \leq 7$.

Problem (2).

(a) $(\Rightarrow)$: If $K[x]/\langle f(x) \rangle$ is a field, then $\langle f(x) \rangle$ is a maximal ideal. It follows that if

$\langle f(x)\rangle \leq \langle p(x)\rangle \leq \langle 1\rangle = F[x]$, then $\langle p(x)\rangle = \langle f(x)\rangle$ or $\langle p(x)\rangle = \langle 1\rangle$. Either way, if $f(x) = a(x)p(x)$ then $a(x)$ or $p(x)$ is a unit, showing that $f(x)$ is irreducible.

$(\Leftarrow)$: if $f(x)$ is irreducible, for any $p(x)$ s.t. $\langle f(x)\rangle \leq \langle p(x)\rangle \leq \langle 1\rangle$, *i.e.* $f(x) = a(x)p(x)$, either $a(x) = u$ or $p(x) = u$ where u is a unit, then $\langle p(x)\rangle = \langle f(x)\rangle$ or $\langle p(x)\rangle = \langle 1\rangle$ respectively. Thus $\langle f(x)\rangle$ is maximal and $F[x]/\langle f(x)\rangle$ is a field.

(b) By 2a we know $K[x]/\langle f(x)\rangle$ is a field. Since K is a field, $K[x]$ is a Euclidean domain, thus by division algorithm the elements in the quotient all have degree less than n and has the form $a_{n-1}x^{n-1}+\cdots+a_0$ where $a_i \in K$. I claim that all values of a_i are achieved since we can just multiply the reduced polynomial with $f(x)$ to get a polynomial in $K[x]$ that reduces to this polynomial in the quotient. There are n number of coefficients, and each coefficient has $|K| = p$ possible values so there are p^n possible combinations of coefficients and thus p^n distinct elements in the quotient.

Problem (3)**.** Since $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is clearly an integral domain so $R \subseteq \mathbb{Q}[x]$ is also an integral domain. Since x is not a unit in $\mathbb{Q}[x]$, it is also not a unit in the subset. Suppose $x = p_1^{k_1}(x)\cdots p_n^{k_n}(x)$. By degree consideration, exactly one $p_i^{k_i}(x)$ has degree 1 and the other factors must all be constants. This forces $p_i^{k_i} = ax, a \in \mathbb{Q}\setminus\{0\}$. However, since we can always factor $ax = \frac{a}{b}x \cdot b$ for some $b \in \mathbb{Z}\setminus\{0\}$, ax is not an irreducible. This implies that x cannot be written as a product of irreducibles. Thus R is not a UFD.

Problem (4)**.** (collab with Daniel): Let $f(x) = \frac{a_n}{b_n}x^n + \cdots + \frac{a_0}{b_0}, g(x) = \frac{c_m}{d_m}x^m + \cdots + \frac{c_0}{d_0} \in \mathbb{Q}[x]$ s.t. $f(x)g(x) \in \mathbb{Z}[x]$. Recall that a content $\text{cont}(f)$ of $f(x)$ is a gcd of numerators of coefficients dividing a lcm of denominators of coefficients. Since $fg \in \mathbb{Z}[x]$, $\text{cont}(fg) \in \mathbb{Z}$ so we can WLOG assume fg is primitive, *i.e.* $\langle \text{cont}(fg)\rangle = \langle 1\rangle$ (if the statement is true for primitive fg, it is clearly true for general fg since we just multiply by integers). Since $\mathbb{Z}$ is a UFD, by Gauss's lemma,

$$\begin{aligned}\langle 1\rangle = \langle \text{cont}(fg)\rangle &= \langle \text{cont}(f)\rangle\langle \text{cont}(g)\rangle \\ &= \left\langle \frac{\gcd(a_0,\ldots,a_n)\cdot\gcd(c_0,\ldots,c_m)}{\text{lcm}\,(b_0,\ldots,b_n)\cdot\text{lcm}\,(d_0,\ldots,d_m)}\right\rangle =: \left\langle \frac{p}{q}\right\rangle\end{aligned}$$

This forces $\frac{p}{q}$ to be a unit in $\mathbb{Z}[x]$, *i.e.* $\frac{p}{q} = \pm 1$. This implies that $q|p$. Given any product $\frac{a_i c_j}{b_i d_j}$ of coefficients of f with that of g, by the definition of gcd and lcm, p divides the numerator whereas $b_i d_j$ divides q. Since $q|p$, we have $b_i d_j|q|p|a_i c_j$, and therefore $\frac{a_i c_j}{b_i d_j} \in \mathbb{Z}$.

Problem (5)**.** Since $\mathbb{Z}[i]$ is a Euclidean domain, it is also a UFD so the irreducibles are also primes. By Proposition 8.18,

Case (1). If $p = 3 \bmod 4$, then primes $p \in \mathbb{Z}$ are also primes in $\mathbb{Z}[i]$. Thus by Eisenstein, $p|p$ but $p^2 \not| p$ so $x^n - p$ is irreducible over $\mathbb{Z}[i]$.

Case (2). If $p = 1 \bmod 4 = a^2 + b^2 = (a + bi)(a - bi)$, then $(a + bi)$ is irreducible and thus prime in $\mathbb{Z}[i]$. By Eisenstein, $(a + bi)|p$ but $(a + bi)^2 \not| p$ so $x^n - p$ is irreducible over $\mathbb{Z}[i]$.

FIX: remove this case.

Case (3). If $p = 2 = (1 + i)(1 - i)$ (the only even prime), then we see that $(1 + i)|2$ but $(1 + i)^2 \not| 2$ so by Eisenstein $x^n - 2$ is irreducible over $\mathbb{Z}[i]$.

Problem (6)**.** Recall that $\mathbb{C}[x, y]$ is the same as $(\mathbb{C}[x])[y]$. Notice $x^m + 1 = 0$ has exactly m unique roots in the form ζ^k where $\zeta := e^{ipi/m}$ and $0 < k < 2m$ odd. The irreducibles in $\mathbb{C}[x]$ are degree 1 polynomials (as $\mathbb{C}$ is algebraically closed so we can always split higher degree polynomials into linear factors) so $x - \zeta$ is irreducible in $\mathbb{C}[x]$ and therefore prime. By Eisenstein, we see that $(x - \zeta)|x^m + 1$ and $(x - \zeta)^2 \not| x^m + 1$ by uniqueness, thus $x^m + y^m + 1$ is irreducible over $\mathbb{C}[x]$ and therefore irreducible in $\mathbb{C}[x, y]$.

Problem (7)**.**

(a) Consider the module homomorphism $\phi_n : R \to N, r \mapsto rn$. Then $\ker \phi_n = \{r \in R : rn = 0\}$ is a submodule of R. Notice that $\mathrm{Ann}_R(N) = \bigcap_{n \in N} \ker \phi_n$ and we know arbitrary intersection of submodules is a submodule as long as it is nonempty, which is true since $0 \in \mathrm{Ann}_R(N)$. Since submodules of R correspond to ideals of R, $\mathrm{Ann}_R(N)$ is an ideal of R.

(b) Consider the module homomorphism $\phi_a : M \to M, m \mapsto am$. Then $\ker \phi_a = \{m \in M : am = 0\}$. Again $\mathrm{Ann}_M(I) = \bigcap_{a \in I} \ker \phi_a$ is a submodule of M. It is nonempty since $0 \in \mathrm{Ann}_M(I)$.

(c) Given $n \in N$, let $I := \mathrm{Ann}_R(N) = \{r \in R : rn = 0 \ \forall\ n \in N\}$. Then $\mathrm{Ann}_M(I) = \{m \in M : am = 0 \ \forall\ a \in I\}$. Since $an = 0 \ \forall\ a \in I$, $n \in \mathrm{Ann}_M(I)$.

Let $N := \langle x \rangle \leq \mathbb{Z}_6[x] =: M$ and $R := \mathbb{Z}$, *i.e.* we treat $\mathbb{Z}_6[x]$ as an abelian group. Then it suffices to annilate the generator x, and it's easy to see that $\mathrm{Ann}_R(N) = \langle 6 \rangle =: I$. But $\mathrm{Ann}_M(I) = M \neq N$ since 6 annilates any element of M.

(d) Given $a \in I$, let $N := \mathrm{Ann}_M(I) = \{m \in M : am = 0 \ \forall \ a \in I\}$. Then $\mathrm{Ann}_R(N) = \{r \in R : rn = 0 \ \forall \ n \in N\}$. Since $an = 0 \ \forall \ n \in N$, $a \in \mathrm{Ann}_R(N)$.

Let $I := \langle x \rangle \leq \mathbb{Z}_6[x] =: R = M$. Then it is easy to see that $p(x) \cdot x = 0 \Leftrightarrow p(x) = 0$ so $\mathrm{Ann}_M(I) = 0 =: N$. But $\mathrm{Ann}_R(N) = \mathbb{Z}_6[x] \neq I$.

Problem (8)**.** $(\Rightarrow)$: Suppose M is simple. Given $m \in M \setminus \{0\}$, we must have $\langle m \rangle = M$, *i.e.* every element $m' \in M$ can be expressed as rm for some $r \in R$. Then let $I := \ker \phi_m = \{r \in R : rm = 0\}$. Define $\phi : M \to R/I, rm \mapsto r + I$. This is a module homomorphism:

$$\begin{aligned}
\phi(s(rm) + (r'm)) &= \phi((sr + r')m) \\
&= sr + r' + I \\
&= (sr + I) + (r' + I) \\
&= s(r + I) + (r' + I) \\
&= s\phi(rm) + \phi(r'm)
\end{aligned}$$

It is clearly surjective. Suppose $\phi(rm) = r + I = I$, then $r \in I$. Thus $rm = 0$ by definition of annilator. It follows that $\ker \phi = \{0\}$ and ϕ is injective. Therefore, $M \cong R/I$. Since M is simple, by the isomorphism R/I also has no proper nontrivial submodules and thus has no proper nontrivial ideals. Hence R/I is a field (every nonzero element generates $R/I = \langle 1 \rangle$ and therefore is a unit) so I is maximal.

$(\Leftarrow)$: Suppose I is maximal and $M \cong R/I$ as R modules. Since R/I is a field, it has no proper nontrivial ideals so it has no proper nontrivial submodules. By the isomorphism so is M. Thus M is simple.