ALGEBRA I HOMEWORK VII

HOJIN LEE 2021–11045

Problem 1.

Problem 2.

Problem 3.

Problem 4. *Let A be a domain. Let $S \subset A - \{0\}$ be a multiplicative subset. Show*

(1) *A PID $\Rightarrow A_S$ PID*
(2) *A UFD $\Rightarrow A_S$ UFD*

Proof. (1) Suppose $I \subset A_S$ is an ideal. Then I is generated by elements of the form $a/1$ where $a/s \in I$ for some $s \in S$. This is because $a/s \in I$ iff $a/1 \in I$. Denote this generating set T. Then $T = \ell_S(T')$ where ℓ_S is the canonical localization map and $T' \subset A$. Clearly $0 \in T'$ since $0/1 \in T$. If $a, b \in T'$, then $a + b \in T'$ since $a/1 + b/1 = (a + b)/1 \in T$. Also, if $a \in A$ and $t \in T'$, then $t/1 \in T \subset I$, and $a/1 \cdot t/1 = at/1 \in I$ so $at/1 \in T$. Hence $at \in T'$, so T' is an ideal of A. Since A is a PID, we may write $T' = (t)$, hence $T = \{at/1 \mid a \in A\}$ so $I = (t/1)$. Therefore every ideal of A_S is principal. A_S is a domain since it is a subring of $K(A)$. □

Proof. (2) We use Kaplansky's theorem. Suppose $\mathfrak{p} \subset A_S$ is a nonzero prime ideal. This corresponds to a nonzero prime ideal $\mathfrak{p}'$ of A that does not touch S. Since A is a UFD, $\mathfrak{p}'$ contains a nonzero prime, say p. Then $\mathfrak{p}$ contains $p/1$. Suppose $\frac{p}{1} | \frac{a}{s}\frac{b}{s'}$. Then we have $\frac{p}{1} \times \frac{c}{d} = \frac{ab}{ss'}$ for some $\frac{c}{d}$, i.e. $(pcss' - abd)s'' = 0$ for some $s'' \in S$. Since S does not contain zero and A is a domain, we have $pcss' = abd$, i.e. $p|abd$. Note that $p|d$ cannot happen since if so, then $pd' = d$ where $d \in S$ and $pd' \in \mathfrak{p}$. So either $p|a$ or $p|b$. WLOG $p|a$, so $a = pa'$, then $\frac{a}{s} = \frac{p}{1}\frac{a'}{s}$, so $\frac{p}{1}|\frac{a}{s}$. Hence $p/1$ is a prime element. It follows that A_S is a UFD. □

Problem 5.

Problem 6. *Let $x \in A$.*

(1) *Let $S \subset A$ be multiplicatively closed. Show $\ell_S(x) = 0$ iff $\mathrm{Ann}(x) \cap S \neq \varnothing$.*
(2) *Show TFAE:*
    (a) $x = 0$
    (b) $\ell_{\mathfrak{p}}(x) = 0$ *for all primes.*
    (c) $\ell_{\mathfrak{m}}(x) = 0$ *for all maximal ideals.*

Proof. (1) Suppose $sx = 0$ for some $s \in S$. Then $s \in \mathrm{Ann}(x) \cap S$. Conversely this also implies $x/1 = 0$ since $xs = 0$. □

Proof. (2) (a) $\Rightarrow$ (b) $\Rightarrow$ (c) is obvious. To show (c) $\Rightarrow$ (a), we show the contrapositive. If $x \neq 0$, then $\mathrm{Ann}(x)$ is proper. Hence there exists some maximal ideal $\mathfrak{m}$ containing $\mathrm{Ann}(x)$. Then $\mathrm{Ann}(x) \cap (A - \mathfrak{m}) = \varnothing$, so $\ell_{\mathfrak{m}}(x) \neq 0$. □

Date: May 8, 2024.

Problem 7. *Let $k = \overline{k}$. Show $(x, y) \subset k[x, y]$ is not principal.*

Proof. Suppose $(x, y) = (f)$. Then $x \in (f)$, so $x = fg$ for some $g \in k[x, y]$. Since x is irreducible, either $f = c$ or $f = cx$ for $c \in k$. The first case implies $(x, y) = k[x, y]$, which is not the case since $k[x, y]/(x, y) \cong k \neq 0$. The second case implies $(x, y) = (x)$ which is nonsense. □

Problem 8.

(1) *Show that a Euclidean domain is a PID.*
(2) *Show that $\mathbb{Z}[i]$ is a Euclidean domain.*

Proof. (1) Let A be a Euclidean domain, and $I \subset A$ an ideal. Consider the set $f(I) \subset \mathbb{N}$. This has a minimal element, and denote by b an element of $I - \{0\}$ in $f^{-1}(\min(f(I)))$. If $a \in I - \{0\}$, then $a = bq + r$ for either $r = 0$ or $f(r) < f(b)$. In this case, $r = a - bq \in I$, so by minimality of $f(b)$, the latter cannot happen. Hence $a = bq$ for all $a \in I$, so $I = (b)$. □

Proof. (2) Obviously a domain since it is a subring of $\mathbb{C}$. Define $f : \mathbb{Z}[i] - \{0\} \to \mathbb{N}$ by $f(a + bi) = a^2 + b^2$. WTS if $z, w \in \mathbb{Z}[i]$ with $w \neq 0$, then there exists $q, r \in \mathbb{Z}[i]$ such that $z = wq + r$ where either $r = 0$ or $f(r) < f(b)$. WMA $r \neq 0$. Then $z/w = (z_1 + z_2 i)/(w_1 + w_2 i) = \frac{z_1 w_1 + z_2 w_2 + (z_2 w_1 - z_1 w_2)i}{f(w)}$. By the Euclidean algorithm on $\mathbb{Z}$ (plus some obvious observations), we may write $z_1 w_1 + z_2 w_2 = f(w)q_1 + r_1$ and $z_2 w_1 - z_1 w_2 = f(w)q_2 + r_2$ for $|r_i| \leq \frac{1}{2} f(w)$. Thus, $\frac{z}{w} = \frac{f(w)(q_1 + q_2 i) + r_1 + r_2 i}{f(w)} = q_1 + q_2 i + \frac{r_1 + r_2 i}{f(w)}$. Hence $z = (q_1 + q_2 i)w + \frac{r_1 + r_2 i}{w_1 - w_2 i}$, where $f(\frac{r_1 + r_2 i}{w_1 - w_2 i}) = \frac{r_1^2 + r_2^2}{w_1^2 + w_2^2}$, omitting tedious calculations. (Trust me, I have done all the calculations.) This is just $f(r_1 + r_2 i)/f(w)$, and we want to show this is $< f(w)$, i.e. $f(r_1 + r_2 i) < f(w)^2$. Since $r_1^2 + r_2^2 \leq 2 \times \frac{f(w)^2}{4} = \frac{f(w)^2}{2}$, we have $f(r_1 + r_2 i) \leq \frac{f(w)^2}{2} < f(w)^2$. Take $q = q_1 + q_2 i$ and $r = z - (q_1 + q_2 i)w = \frac{r_1 + r_2 i}{w_1 - w_2 i} \in \mathbb{Z}[i]$. □

Problem 9.

Problem 10.

Problem 11. *Is it irreducible?*

Proof. (1) $x^4 + 1$ does not have a linear factor since it does not have a root in $\mathbb{Q}$ (let alone $\mathbb{R}$). Hence if it did factorize, then each factor would have to be at least of degree 2. Thus the only possible case is $x^4 + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$ for $a, b \in \mathbb{Q}$. By expanding, the conditions become $a + b = 0$ and $ab + 2 = 0$, i.e. $a = -b$ and $a^2 = 2$. This does not have any solution in $\mathbb{Q}$. Hence it is irreducible over $\mathbb{Q}$. □

Proof. (2) Substitute $x \mapsto x + 1$. We get $(x + 1)^6 + (x + 1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$. Eisenstein's criterion for $p = 3$ is applicable. Hence $x^6 + x^3 + 1$ is irreducible over $\mathbb{Q}$. □

Proof. (3) The polynomial $x^3 - 5x^2 + 1$ has no roots in $\mathbb{F}_2$, hence is irreducible over $\mathbb{F}_2$ since it is of degree 3. Thus it is irreducible over $\mathbb{Q}$. □

Proof. (4) The polynomial $5x^5 - 5x + 1 = 2x^5 + x + 1$ has no roots in $\mathbb{F}_3[x]$. Thus if it did factor in $\mathbb{F}_3[x]$, then it would contain an irreducible factor of degree 2. The degree 2 irreducible polynomials of $\mathbb{F}_3[x]$ are precisely the following:

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

Note that the last 3 polynomials are just -1 times the first three, so it suffices to show that $2x^5 + x + 1$ does not have as factors the first three polynomials.

First, suppose $2x^5 + x + 1 = (x^2 + 1)(2x^3 + ax^2 + bx + 1)$. This cannot happen since the degree 4 coefficient is $a = 0$, but the degree 2 coefficient is $a + 1 \neq 0$.

Next suppose $2x^5 + x + 1 = (x^2 + x + 2)(2x^3 + ax^2 + bx + 1) = 2x^5 + (2 + a)x^4 + (1 + a + b)x^3 + (2a + b + 2)x^2 + (2b + 2)x + 1$. Then $a = b = 1$, but then $2a + b + 2 = 2 \neq 0$.

Suppose $2x^5 + x + 1 = (x^2 + 2x + 2)(2x^3 + ax^2 + bx + 1) = 2x^5 + (1 + a)x^4 + (1 + 2a + b)x^3 + (2a + 2b + 2)x^2 + (2b + 1)x + 1$. Then $a = 2, b = 1$ but $2a + 2b + 2 = 2 \neq 0$.

Therefore it is irreducible over $\mathbb{F}_3$, hence irreducible over $\mathbb{Q}$. $\square$