SERGE LANG'S ALGEBRA CHAPTER 2 EXERCISE SOLUTIONS

KELLER VANDEBOGERT

1. Problem 1

Assume $1 \neq 0$ in A. Let S be a multiplicative subset of A not containing 0. Let $\mathfrak{p}$ be a maximal elements in the set of ideals whose intersection with S is empty. Show that $\mathfrak{p}$ is prime.

Consider

$$\Gamma := \{I \subset A \mid I \text{ ideal}, \ I \cap S \neq \varnothing\}$$

Then, $\mathfrak{p}$ is assumed to be maximal in the above set. Suppose fro sake of contradiction that $\mathfrak{p}$ is not prime, and choose x, $y \in \mathfrak{p}^c$ with $xy \in \mathfrak{p}$.

We see that $\mathfrak{p}+Ax$ strictly contains p, so, by maximality $\mathfrak{p}+Ax \notin \Gamma$, whence

$$(\mathfrak{p} + Ax) \cap S \neq \varnothing$$

implying there exists $p \in \mathfrak{p}$, $a \in A$ such that

$$p + ax \in S$$

Similarly, there exists $p' \in \mathfrak{p}$, $a' \in A$ such that

$$p' + a'y \in S$$

We then see that the product

$$(p + ax)(p' + a'y) \in S$$

Date: October 22, 2018.

Expanding this,

$$pp' + pa'y + ap'x + aa'xy \in S$$

However, all of the terms in the above are elements of $\mathfrak{p}$, implying that

$$\mathfrak{p} \cap S \neq \varnothing$$

which is a contradiction; whence the result follows.

2. Problem 2

Let $f : A \to A'$ be a surjective homomorphism of rings, and assume that A is local, $A' \neq 0$. Show that A' is local.

Note that in a local ring, every $x \notin \mathfrak{m}$ must be a unit, since $(x) = A$. By surjectivity, the image of $\mathfrak{m}$ is an ideal. We want to show that it is maximal.

Let $a' \notin f(\mathfrak{m})$. There exists $a \in A$ such that $f(a) = a'$. We see that $a \notin \mathfrak{m}$, so that a is a unit. Letting b denote the inverse,

$$f(ab) = f(a)f(b) = 1$$

Implying that $f(a) = a'$ is also a unit, so that $f(\mathfrak{m})$ is also maximal.

3. Problem 3

Let $\mathfrak{p}$ be a prime ideal of A. Show that $A_{\mathfrak{p}}$ has a unique maximal ideal.

Let $A_{\mathfrak{p}}$ denote our localization. Then,

$$\mathfrak{p}A_{\mathfrak{p}} = \left\{\frac{p}{s} \mid p \in \mathfrak{p},\ s \in \mathfrak{p}^c\right\}$$

is our maximal ideal, since if $r/s \notin \mathfrak{p}A_{\mathfrak{p}}$,

$$\frac{r}{s} \cdot \frac{s}{r} = 1$$

so that r/s is a unit, implying $\mathfrak{p}A_{\mathfrak{p}}$ is our unique maximal ideal.

4. Problem 4

Let A be a principal ideal domain and S a multiplicative subset with $0 \notin S$. Show that $S^{-1}A$ is principal.

Suppose that A is principal. Given any ideal $I \subset S^{-1}A$, the preimage under the natural inclusion $i : A \to S^{-1}A$ will remain an ideal. Hence, $i^{-1}(I) = (a)$ for some $a \in A$. Since $i : A \hookrightarrow S^{-1}A$ is injective,

$$f \circ f^{-1}(I) = I \implies I = \left(\frac{a}{1}\right)$$

whence I is also a principal ideal, implying $S^{-1}A$ is a PID.

5. Problem 5

Let A be a unique factorization domain and S a multiplicative subset with $0 \notin S$. Show that $S^{-1}A$ is also a UFD, and that the prime elements of $S^{-1}A$ are of the form up with primes p of A with that $(p) \cap S$ is empty, and units in $S^{-1}A$.

Suppose $\mathfrak{p} \in \operatorname{Spec}(A)$ is such that $\mathfrak{p} \cap S = \varnothing$. If $i : A \to S^{-1}A$ denotes the natural inclusion, we wish to show that $i^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$.

Certainly, $\mathfrak{p} \subset i^{-1}(S^{-1}\mathfrak{p})$ holds tautologically. For the reverse inclusion, let $a \in A$ be such that

$$\frac{a}{1} \in S^{-1}\mathfrak{p}$$

Then, there exists $t \in S$, $s \in S$, $a' \in \mathfrak{p}$ such that

$$t(sa - a') = 0$$

As $st \in S$ and $S \cap \mathfrak{p} = \varnothing$, we deduce that $a \in \mathfrak{p}$. Hence, $i^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$.

Now, if $\mathfrak{p}$ is prime and $\mathfrak{p} \cap S = \varnothing$, then suppose

$$\frac{a}{s} \cdot \frac{b}{s'} \in S^{-1}\mathfrak{p}$$

so that there exists $t,\ t' \in S$ and $p \in \mathfrak{p}$ such that

$$t'(tab - ss'p) = 0$$

As $\mathfrak{p} \cap S = \varnothing$ and $tt' \in S$, we see that this forces $ab \in \mathfrak{p}$. But $\mathfrak{p}$ is prime, so

$$\begin{aligned} ab \in \mathfrak{p} &\implies a \text{ or } b \in \mathfrak{p} \\ &\implies \frac{a}{s} \text{ or } \frac{b}{s'} \in S^{-1}\mathfrak{p} \\ &\implies S^{-1}\mathfrak{p} \text{ is prime} \end{aligned}$$

This then shows that the prime ideals of A disjoint from S are in bijection with prime ideal in $S^{-1}A$. Hence, if $\mathfrak{p}$ is prime and $(p) \cap S = \varnothing$, then $i(p) = p/1$ generates a prime ideal of $S^{-1}A$, so that $p/1$ is a prime element in $S^{-1}A$.

Now let $a/s \in S^{-1}A$. As A is a UFD, we have a factorization of $a = up_1 \dots p_k$ with p_i prime and u a unit. We have that $1/s$ is a unit, and for each $p_i/1$, if $(p_i) \cap S = \varnothing$, then $p_i/1$ is a prime in $S^{-1}A$ by the above.

If $(p_i) \cap S \neq \varnothing$, then $rp_i \in S$ for some $r \in A$. This gives that $p_i/1$ is a unit, however, since

$$\frac{r}{rp_i} \cdot \frac{p_i}{1} = 1$$

Thus, any prime p_i with $(p_i) \cap S \neq \varnothing$ becomes a unit in $S^{-1}A$. Combining this with the above, we may factorize a/s in $S^{-1}A$; uniqueness of this factorization follows by uniqueness of the factorization on a in A, since if we had two distinct factorizations, every prime of $S^{-1}A$ corresponds to some prime of A by the above logic.

6. Problem 6

Let A be a UFD and p a prime element. Show that the local ring $A_{(p)}$ is principal.

By the previous problem, $A_{(p)}$ is a UFD with maximal ideal $(p)A_{(p)}$. Given any other prime $p' \in A$, p' is not a unit, so $p' \in (p) \implies p' = up$ for some unit. Then, every x is of the form $x = up^n$, $n \in \mathbb{N}$, $u \in A^\times$.

Now, let $I \subset A$ be an ideal. Consider

$$\min\{n \in \mathbb{N} \mid x = up^n,\ x \in I\}$$

Choose $x \in I$ such that the minimum is achieved. The condition $x \in I$ ensures $(x) \subset I$.

For the reverse inclusion, let $y \in I$. Then, $y = u'p^m$ for $u' \in A^\times$, $m \geqslant n$. But,

$$\begin{aligned} y &= u'p^m \\ &= u^{-1}u'p^{m-n} \cdot up^n \\ &= u^{-1}u'p^{m-n}x \in (x) \end{aligned}$$

So that $y \in (x)$, and we conclude $(x) = I$. As I was arbitrary, we see that A is a PID.

7. Problem 7

Let A be a PID and $a_1, \ldots, a_n$ nonzero elements of A. Let $(a_1, \ldots, a_n) = (d)$. Show that d is the greatest common divisor for the a_i.

Suppose $(a_1, \ldots, a_n) = (d)$. It is clear that $d | a_i$ for every i, as

$$(a_i) \subset (a_1, \ldots, a_n) = (d)$$

Suppose now that some other d' divides each a_i. By definition, $(a_i) \subset (d')$, so that

$$\begin{aligned} (d) = (a_1, \dots, a_n) \subset (d') \\ \implies (d) \subset (d') \\ \implies d | d' \end{aligned}$$

So that d is the greatest common divisor, by definition.

8. Problem 8

Let p be a prime number and let A be the ring $\mathbb{Z}/p^r\mathbb{Z}$. Let G be the group of units in A, i.e. the group of integers prime to p, modulo p^r. Show that G is cyclic, except in the case when $p = 2$ and $r \geqslant 3$, in which case it is of type $(2, 2^{r-1})$.

Consider first the case for p an odd prime. We see that

$$(1+p)^{p^{n-1}} = \sum_{k=0}^{p^{n-1}} \binom{p^{n-1}}{k} p^k \equiv 1 \mod p^n$$

And,

$$\begin{aligned} (1+p)^{p^{n-2}} &= \sum_{k=0}^{p^{n-2}} \binom{p^{n-2}}{k} p^k \\ &= 1 + p^{n-1} + p^n \frac{(p^{n-2}-1)}{2} + \cdots + p^{p^{n-2}} \\ &\equiv 1 + p^{n-1} \mod p^n \end{aligned}$$

This implies that $p+1$ has order p^{n-1}, since if $(p+1)^m \equiv 1 mod p^n$ for some other m, then $m | p^{n-1}$. This gives that $(1+p)^m \equiv 1 \mod p^n$ for some $k < n-2$.

However, taking successive powers of p, we see that $(1+p)^{p^{n-2}} \equiv 1$, which has already shown to be impossible.

Now, if P denotes our Sylow p subgroup, consider the map

$$(\mathbb{Z}/p^n)^\times \to (\mathbb{Z}/p)^\times$$
$$x + (p^n) \mapsto x + (p)$$

The kernel of this map is precisely P, so,

$$(\mathbb{Z}/p^n)^\times / P \cong (\mathbb{Z}/p)^\times$$

It suffices to show that $(\mathbb{Z}/p)^\times$ is cyclic. Suppose then that every nonzero element has order strictly less than $p-1$. Then, choose the maximum of these orders, say, m. We see that

$$x^m - 1 \equiv 0$$

has $p-1$ solutions $\mod p$. But $m < p-1$, so this is impossible. Hence $(\mathbb{Z}/p)^\times$ is cyclic, and the subgroup of order $p-1$ in $(\mathbb{Z}/p^n)^\times$ must also be cyclic. Then,

$$(\mathbb{Z}/p^n)^\times \cong \mathbb{Z}/p^{n-1} \times \mathbb{Z}/(p-1)$$

is a cyclic group, as desired, generated by $(p+1)x$, where x is any order $p-1$ element.

Now we consider the $p = 2$ case. When $r < 3$, it is trivial that $(\mathbb{Z}/2)^\times$ and $(\mathbb{Z}/4)^\times$ are cyclic. Suppose now that $r \geqslant 3$. Then,

$$\begin{aligned}(1+2^2)^{2^{r-2}} &= \sum_{k=0}^{2^{r-2}} \binom{2^{r-2}}{k} 2^{2k} \\ &\equiv 1 \mod 2^r\end{aligned}$$

And,

$$\begin{aligned}(1+2^2)^{2^{r-3}} &= \sum_{k=0}^{2^{r-3}} \binom{2^{r-3}}{k} 2^{2k} \\ &\equiv 1 + 2^{r-1} \mod 2^r\end{aligned}$$

So, 5 has order 2^{r-2}, and, we may consider the map

$$(\mathbb{Z}/2^r)^\times \to (\mathbb{Z}/4)^\times$$

$$x + (2^r) \mapsto x + (4)$$

The kernel of this map is the subgroup generated by 5, so modding out this subgroup, we see the rest is cyclic of order 2, and

$$(\mathbb{Z}/2^r)^\times \cong (\mathbb{Z}/2^{r-2}) \times (\mathbb{Z}/2)$$

which completes the problem.

9. Problem 9

Let i denote the imaginary unit. Show that the ring $\mathbb{Z}[i]$, the Gaussian integers, is principal hence factorial. What are the units?

We can say even more than the problem asks: $\mathbb{Z}[i]$ is a Euclidean domain with norm $N(a+ib) = a^2 + b^2$. This is a trivial checking of definitions, where our Euclidean algorithm is computed by picking the nearest lattice point upon division by any other element.

Then, given any ideal $I \subset \mathbb{Z}[i]$, the element of minimal norm will generate the entirety of our ideal.

Since the norm is multiplicative, we also see that the only units will have norm 1. Hence, our units are

$$\{1, -1, i, -i\}$$

10. Problem 10

Let D be an integer $\geqslant 1$ and let R be the set of all elements $a + b\sqrt{-D}$ with a, $b \in \mathbb{Z}$.

(1) **Show that R is a ring.**

(2) **Using the fact that complex conjugation is an automorphism of $\mathbb{C}$, show that compex conjugation induces an automorphism of R.**

(3) **Show that if $D \geqslant 2$ then the only units of R are ± 1.**

(4) **Show that 3, $2+\sqrt{-5}$, $2-\sqrt{-5}$ are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$.**

(a). Let (x^2+D) denote the ideal generated by x^2+D. Then,

$$\mathbb{Z}[\sqrt{-D}] = \frac{\mathbb{Z}[x]}{(x^2+D)}$$

As the quotient of a ring, this is itself clearly a ring.

(b). First note that conjugation is stable on $\mathbb{Z}[\sqrt{-D}]$, so this is well defined. Since it is an automorphism of $\mathbb{C}$, restricting yields an automorphism of $\mathbb{Z}[\sqrt{-D}]$.

(c). Define our norm

$$N : \mathbb{Z}[\sqrt{-D}] \to \mathbb{Z}_{\geqslant 0}$$

$$a + b\sqrt{-D} \mapsto a^2 + Db^2$$

Then, $a+b\sqrt{-D}$ is a unit if and only if $N(a+b\sqrt{-D}) = 1$. If $b \geqslant 1$, $D \geqslant 2$, then $b^2D > 1$, so $b = 0$ if $N(a+b\sqrt{-D}) = 1$, implying $a^2 = 1$, so,

$$a = \pm 1$$

as asserted.

(d). Suppose that 3 is reducible. Observe that $N(3) = 9$, so it must factor as the product of two elements with norm 3. However, no such element can exist, so that 3 is irreducible.

Similarly, $N(2+\sqrt{-5}) = N(2-\sqrt{-5}) = 9$, so by the above these are also irreducible.

11. Problem 11

Let R be the ring of trigonometric polynomials. Show that R consists of all functions f on $\mathbb{R}$ which has an expression of the form

$$f(x) = a_0 + \sum_{n=1}^{n} (a_m \cos(mx) + b_m \sin(mx)$$

where a_0, a_m, b_m are real numbers. Define the trigonometric degree $\deg_{tr}(t)$ to be the maximum of the integers r and s such that $a_r,\ b_s \neq 0$. Prove that

$$\deg_{tr}(fg) = \deg_{tr}(f) + \deg_{tr}(g)$$

Deduce from this that R has no 0 divisors, and also deduce that the function $\sin(x)$ and $1 - \cos(x)$ are irreducible elements in that ring.

We may view $\mathbb{R}[\sin(t), \cos(t)]$ as a subring of $\mathbb{C}[e^{int}]$ (this is merely by Euler's formula). Hence we may find $c_i \in \mathbb{C}$ such that for $f(x) \in \mathbb{R}[\sin(t), \cos(t)]$,

$$\begin{aligned} f(x) &= \sum_{k=0}^{n} c_k \big(e^{it}\big)^k \\ &= \sum_{k=0}^{n} c_k \cos(kt) + ic_k \sin(kt) \end{aligned}$$

Taking the real part, set $a_k := \text{Re}(c_k)$, $b_k := \text{Re}(ic_k)$. Then,

$$f(x) = a_0 + \sum_{k=1}^{n} a_k \cos(kt) + b_k \sin(kt)$$

as desired. If we assume $\deg_{\text{tr}}(f) = r$, $\deg_{\text{tr}}(g) = s$, then f and g are polynomials of degree r and s, respectively, in $\mathbb{C}[e^{it}]$. Hence, their product is of degree $r + s$. Taking real parts, we deduce that

$$\deg_{\text{tr}}(fg) = \deg_{\text{tr}}(f) + \deg_{\text{tr}}(g)$$

Then, we see that $\sin(x)$ and $1-\cos(x)$ both have trigonometric degree 1. If these were to factor, it would be the product of a degree 0 and degree 1 polynomial. The degree 0 polynomials are merely constants, however, and all nonzero constants are units in $\mathbb{R}$. Hence, these are irreducible.

12. Problem 12

Let P be the set of positive integer and R the set of function defined on P with values ina commutative ring K. Define the sum in R to be the ordinary addition of function, and define the convolution product by the formula

$$(f*g)(m)=\sum_{xy=m} f(x)g(y)$$

where the sum is taken over all pair (x,y) of positive integer with $xy=m$.

(a) **Show that R is a commutative ring whose unit element is the function δ such that $\delta(1)=1$ and $\delta(x)=0$ for $x\neq 1$.**
(b) **A function f is said to be multiplicative if $f(mn)=f(m)f(n)$ whenever m and n are coprime. If f and g are multiplicative, show that $f*g$ is multiplicative.**
(c) **Let μ denote the Möbius function such that $\mu(1)=1$, $\mu(p_1\dots p_r)=(-1)^r$ if $p_1,\dots,p_r$ are distinct primes. Show that $\mu*\phi_1=\delta$, where ϕ_1 denotes the constant function having value 1.**

(a). Commutativity is a tautology. Addition is trivially an abelian group. It remains to show associativity and existence of identity. We

see:

$$\begin{aligned} f*(g*h)(m) &= \sum_{xy=m} f(x)\cdot(g*h)(y) \\ &= \sum_{xy=m} f(x)\sum_{ab=y} g(a)h(b) \\ &= \sum_{xab=m} f(x)g(a)h(b) \\ &= \sum_{yb=m} h(b)\sum_{ax=y} f(x)g(a) \\ &= \sum_{yb=m} h(b)(f*g)(y) \\ &= h*(f*g)(m) \\ &= (f*g)*h(m) \end{aligned}$$

Which yields associativity. Suppose now there is some identity $\delta(x)$. Then,

$$\begin{aligned} f*\delta(m) &= \sum_{xy=m} f(x)\delta(y) \\ &= f(m) \end{aligned}$$

Whence we deduce that $\delta(x)$ must satisfy

$$\delta(x) = \begin{cases} 1, & x=1 \\ 0, & \text{else} \end{cases}$$

Hence, we have a commutative ring with identity.

(b). Let f and g be multiplicative. Choose m, n coprime; the convolution has the equivalent form

$$\begin{aligned}(f * g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right)\\ &= \sum_{a|m,b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)\\ &= \sum_{a|m,b|n} f(a)g\left(\frac{m}{a}\right)f(b)g\left(\frac{n}{b}\right)\\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right)\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\\ &= (f * g)(m) \cdot (f * g)(n)\end{aligned}$$

So the convolution is also multiplicative.

(c). Suppose $n > 1$ (the $n = 1$ case is trivial). Let

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

We see:

$$\begin{aligned}(\mu * 1)(n) &= \sum_{d|n} \mu(d)\\ &= \sum_{i=1}^{k} \sum \mu(p_{m_1} \dots p_{m_i})\\ &= \sum_{i=1}^{k} \sum_{\text{Size } i \text{ subsets}} (-1)^i\\ &= \sum_{i=1}^{k} \binom{k}{i}(-1)^i\\ &= (1-1)^k = 0\end{aligned}$$

As desired. Suppose now that $f(n) = \sum_{d|n} g(d) = (\phi_1 * g)(n)$. Convolving with our Möbius function,

$$\begin{aligned}(\mu * f)(n) &= \mu * (\phi_1 * g)(n)\\ &= g(n)\end{aligned}$$

Which yields the Möbius inversion formula.

13. Problem 13

Prove every ideal of a Dedekind domain is finitely generated.

Suppose $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$. In particular, $1 \in \mathfrak{o}$, so there exist $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ with

$$\sum_i a_i b_i = 1$$

Claim: $\mathfrak{a} = (a_1, \dots, a_n)$. To see this, let $a \in \mathfrak{a}$. Then,

$$\begin{aligned} a &= a \cdot 1 \\ &= a \cdot \sum_i a_i b_i \\ &= \sum_i (ab_i) a_i \end{aligned}$$

Since $ab_i \in \mathfrak{o}$, we deduce that

$$a \in (\mathfrak{o}(a_1, \dots, a_n) = (a_1, \dots, a_n)$$

Hence $\mathfrak{a} = (a_1, \dots, a_n)$, as asserted.

14. Problem 14

Every ideal has a factorization are a product of prime ideals, uniquely determined up to permutation.

We consider the set Σ consisting of all ideals that cannot be written as the product of prime ideals.

Assuming Σ is nonempty, let $\mathfrak{a} \in \Sigma$ be a maximal element with respect to inclusion. Such an element exists by the previous problem, which shows that $\mathfrak{o}$ is Noetherian. If $\mathfrak{a} = \mathfrak{m}$, the result follows trivially since $\mathfrak{m}$ is prime.

If $\mathfrak{a} \subset \mathfrak{m}$ is properly contained, then $\mathfrak{a} = \mathfrak{m}\mathfrak{m}^{-1}\mathfrak{a}$, and $\mathfrak{m}^{-1}\mathfrak{a}$ strictly contains $\mathfrak{a}$ (because $\mathfrak{m}$ is proper).

By assumption, $\mathfrak{a}$ was maximal in Σ, so $\mathfrak{m}^{-1}\mathfrak{a} \notin \Sigma$. By definition this means that $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_k$ for prime ideals $\mathfrak{p}_i$. But then we see that $\mathfrak{a} = \mathfrak{m}\mathfrak{p}_1 \ldots \mathfrak{p}_k$ is a prime factorization for $\mathfrak{a}$, contradicting the definition of Σ.

It remains to show uniqueness of such a factorization. If

$$\mathfrak{p}_1 \ldots \mathfrak{p}_k = \mathfrak{q}_1 \ldots \mathfrak{q}_j$$

then without loss of generality we may assume $\mathfrak{p}_1 \supset \mathfrak{q}_1$. However, by symmetry the reverse containment also holds, and continuing inductively we find that $i = j$ and the ideals in both factorizations coincide.

15. Problem 15

Suppose $\mathfrak{o}$ has only one prime ideal $\mathfrak{p}$. Let $t \in \mathfrak{p}$ and $t \notin \mathfrak{p}^2$. Then $\mathfrak{p} = (t)$ is principal.

(t) has a prime factorization by the previous problem. Hence, write $(t) = \mathfrak{p}^n$ for some n. Since $t \notin \mathfrak{p}^2$ and $\mathfrak{p}^n \supset \mathfrak{p}^2$ for all $n \geqslant 2$, we deduce that $n = 1$, so that $(t) = \mathfrak{p}$.

It remains to show that such a t must exist. If not, then $\mathfrak{p} = \mathfrak{p}^2$. But this contradicts uniqueness of factorizations, so that $\mathfrak{p} \neq \mathfrak{p}^2$.

16. Problem 16

Let mfo be any Dedekind domain. Let $\mathfrak{p}$ be a prime ideal. Let $\mathfrak{o}_\mathfrak{p}$ be the localization at $\mathfrak{p}$. Show that $\mathfrak{o}_\mathfrak{p}$ is Dedekind and has only one prime ideal.

We have already shown that $\mathfrak{o}_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$. It suffices to show that there are no proper prime ideals of $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$. In fact, we can show even stronger that $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$ is a PID.

By the previous exercise, we may find a $t \in \mathfrak{p}\mathfrak{o}_\mathfrak{p}$ with $t \notin \left(\mathfrak{p}\mathfrak{o}_\mathfrak{p}\right)^2$. Then our maximal ideal is principal, in which case there are trivially no proper prime ideals, since else $(t) \subset \mathfrak{q}$ for some $\mathfrak{q} \in \operatorname{Spec}(\mathfrak{o}_\mathfrak{p})$.

17. Problem 17

As for the integers, we say that $\mathfrak{a} \mid \mathfrak{b}$ if there exists an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Prove:

(a) **$\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{b} \subset \mathfrak{a}$.**

(b) **Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals. Then $\mathfrak{a} + \mathfrak{b}$ is their greatest common divisor. In particular, show $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime if and only if $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$.**

(a). We prove the forward direction first. Since $\mathfrak{a}$ is an ideal, $\mathfrak{a}\mathfrak{c} \subset \mathfrak{a}$; hence

$$\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subset \mathfrak{a} \implies \mathfrak{a} \supset \mathfrak{b}$$

Conversely, suppose that $\mathfrak{a} \supset \mathfrak{b}$. Then, $\mathfrak{b} = \mathfrak{a}\mathfrak{a}^{-1}\mathfrak{b}$, so we may take $\mathfrak{c} := \mathfrak{a}^{-1}\mathfrak{b}$.

(b). Recall that $\mathfrak{a} + \mathfrak{b}$ is the minimal ideal with respect to inclusion containing both $\mathfrak{a}$ and $\mathfrak{b}$. That is, if some other $\mathfrak{c}$ divides both $\mathfrak{a}$ and $\mathfrak{b}$, this implies that $\mathfrak{c}$ must contain $\mathfrak{a} + \mathfrak{b}$. That is, $\mathfrak{c} | \mathfrak{a} + \mathfrak{b}$, as desired.

18. Problem 18

Prove that every nonzero prime is maximal. In particular, if $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are distinct primes, then the Chinese remainder theorem applies to their power $\mathfrak{p}_1^{r_1} \dots \mathfrak{p}_n^{r_n}$.

Let $\mathfrak{p}$ be a nonzero prime ideal of our Dedekind domain.

Claim: If $\mathfrak{p} = \mathfrak{a}\mathfrak{b}$, the $\mathfrak{p} \supset \mathfrak{a}$ or $\mathfrak{p} \supset \mathfrak{b}$. To prove this claim, suppose without loss of generality that $\mathfrak{p} \not\supset \mathfrak{a}$. We may find $a \in \mathfrak{a}$, $a \notin \mathfrak{p}$, and for every $b \in \mathfrak{b}$,

$$ab \in \mathfrak{p}$$

Since $a \notin \mathfrak{p}$, the definition of prime ideals gives that $b \in \mathfrak{p}$ for every $b \in \mathfrak{b}$; that is, $\mathfrak{p} \supset \mathfrak{b}$. Suppose now that $\mathfrak{p} \subset \mathfrak{a}$ for some ideal $\mathfrak{a}$. Then,

$$\mathfrak{p} = \mathfrak{a}(\mathfrak{a}^{-1}\mathfrak{p})$$

and by the above,

$$\mathfrak{p} \supset \mathfrak{a} \implies \mathfrak{p} = \mathfrak{a}, \text{ or}$$

$$\mathfrak{p} \supset \mathfrak{a}^{-1}\mathfrak{p} \implies \mathfrak{a} = \mathfrak{o}$$

Whence $\mathfrak{p}$ is maximal.

19. Problem 19

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals. Show that there exists an element $c \in K$ (the quotient field of $\mathfrak{o}$) such that $c\mathfrak{a}$ is an ideal relatively prime to $\mathfrak{b}$. In particular, every ideal class in Pic($\mathfrak{o}$) contains representative ideals prime to a given ideal.

Define $\nu_{\mathfrak{p}}$ on the nonzero ideals I of $\mathfrak{o}$ to be the exponent of the prime ideal $\mathfrak{p}$ in the factorization of I.

By Problem 16, we may find $t \in \mathfrak{p}$, $t \notin \mathfrak{p}^2$. Then, (t) has $\mathfrak{p}$ in its prime factorization, and similarly, (t^n) must have $\mathfrak{p}^n$ in its prime factorization.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct primes. Given any tuple $(\alpha_1, \ldots, \alpha_n)$, find x_i such that (x_i) has $p_i^{\alpha_i}$ as a prime factor. By the Chinese Remainder theorem, we may choose $x \in \mathfrak{o}$ wth $x \equiv x_i \mod \mathfrak{p}_i^{\alpha_i+1}$.

Now, let $\mathfrak{a}$, $\mathfrak{b}$ be given ideals. Find y as above so that $\nu_{\mathfrak{p}}((y)) = \nu_{\mathfrak{p}}(\mathfrak{a})$ for every $\mathfrak{p}|\mathfrak{a}$. Then, choose x satisfying

$$\nu_{\mathfrak{p}}((x)) = \begin{cases} 0, & \mathfrak{p}|\mathfrak{a} \\ \nu_{\mathfrak{p}}((y)), & \mathfrak{p}|(y),\ \mathfrak{p} \not|\mathfrak{a} \\ 0, & \mathfrak{p}|\mathfrak{b},\ \mathfrak{p} \not|(y) \end{cases}$$

Then, $\frac{x}{y}\mathfrak{a}$ is coprime to $\mathfrak{b}$. To see this, merely note that by construction, no prime containing $\mathfrak{b}$ can contain $\frac{x}{y}\mathfrak{a}$, since else $\mathfrak{p} \supset \mathfrak{a}$ or $\mathfrak{p} \supset \frac{x}{y}$. But $\nu_{\mathfrak{p}}((x)) = 0$, so $\mathfrak{p} \supset \mathfrak{a}$.

Hence, $\frac{x}{y}\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$, and the proof is complete.