

MATH 123: ABSTRACT ALGEBRA II
SOLUTION SET # 4

GREGG MUSIKER

1. CHAPTER 11, SECTION 8

Problem 5 Prove that $A \supset A'$ implies that $AB \supset A'B$.

$AB = \sum_i \alpha_i \beta_i$ where $\alpha_i \in A$ and $\beta_i \in B$.

$A'B = \sum_i \gamma_i \beta_i$ where $\gamma_i \in A'$ and $\beta_i \in B$.

Since $\gamma_i \in A' \subset A$, $A'B \subset AB$.

Problem 6 Factor the principal ideal (14) into prime ideals explicitly in $R = \mathbb{Z}[\delta]$, where $\delta = \sqrt{-5}$.

(14) = (2)(7) in the integers. Is there another way to factor 14 in $\mathbb{Z}[\delta]$? In fact there is: by looking at the equation $14 = a^2 + 5b^2$, $a = 3, b = 1$ is a solution. So $(14) = (3 + \sqrt{-5})(3 - \sqrt{-5})$.

Ideal factorization will allow us to have a common refinement, letting

$A = (2, 3 + \sqrt{-5}), B = (7, 3 + \sqrt{-5}), (14) = A\bar{A}B\bar{B} = AB\bar{A}\bar{B}$.

Proof that this is the right factorization. $A\bar{A} = (4, 14, 6 + 2\sqrt{-5}, 6 - 2\sqrt{-5})$.

By the main lemma, $A\bar{A} = (n)$, an integral principal ideal. 2 divides every generator so $A\bar{A} \subset (2)$. $14 - 3(4) = 2$ so $A\bar{A} \supset (2)$ implies $A\bar{A} = (2)$. Similar logic proves $B\bar{B} = (7)$.

Proof that this A, \bar{A}, B, \bar{B} are prime. Since $A\bar{A} = (2)$ and $B\bar{B} = (7)$, the norm of these two ideals are prime, thus they are prime ideals.

Problem 7 Let P be a prime ideal of an integral domain R , and assume that existence of factorizations is true in R . Prove that if $a \in P$ then some irreducible factor of a is in P .

By the definition of prime ideal given in section 9, if $\alpha, \beta \in R$ s.t. $\alpha\beta \in P$ then $\alpha \in P$ or $\beta \in P$.

If a is irreducible, we're done ($a \in P$) so assume a is reducible. Then $a = \alpha_1 \alpha_2 \cdots \alpha_n$ as an irreducible factorization. (Note: This is not *the* factorization, it is a possible factorization, R need not be a UFD.)

By repeated application of the definition, α_1 or α_2 or \dots $\alpha_n \in P$.

2. CHAPTER 11, SECTION 9

Problem 2 Let $d = -14$. For each of the following primes p , determine whether or not p splits or ramifies in R , and if so, determine a lattice basis for a prime ideal factor of $(p) : 2, 3, 5, 7, 11, 13$.

By proposition (11.9.3), p stays prime in R if and only if $x^2 + 14$ is irreducible mod p .

Modding by p one gets the following equations:

If $p = 2, x^2 \equiv 0 \equiv x \cdot x \pmod{2}$. In fact (2) ramifies as $(2) = (2, \sqrt{-14})(2, \sqrt{-14})$.

If $p = 3, x^2 + 2 \equiv 0 \equiv (x+1)(x+2) \pmod{3}$. $(3) = (3, 1 + \sqrt{-14})(3, 1 - \sqrt{-14})$.

If $p = 5, x^2 + 4 \equiv 0 \equiv (x+1)(x+4) \pmod{5}$. $(5) = (5, 1 + \sqrt{-14})(5, 1 - \sqrt{-14})$.

If $p = 7, x^2 \equiv 0 \equiv x \cdot x \pmod{7}$. In fact (7) ramifies as $(7) = (7, \sqrt{-14})(7, \sqrt{-14})$.

If $p = 11, x^2 + 3 \equiv 0 \pmod{11}$ is irreducible by inspecting 1^2 through 6^2 . Thus (11) stays prime.

If $p = 13, x^2 + 1 \equiv 0 \equiv (x+5)(x+8) \pmod{13}$. $(13) = (13, 5 + \sqrt{-14})(13, 5 - \sqrt{-14})$.

One must check these ideal equivalences on the right. One can do this by the method problem 11.8.6 for example. Many people noticed the relation between the factors of $x^2 + 14$ and the lattice basis of the ideal factorization.

Proof of this correspondence. Let $p \equiv 2$ or $3 \pmod{4}$. Suppose $(p) = (p, a + b\sqrt{d})(p, a - b\sqrt{d}) = (p, p(a + b\sqrt{d}), p(a - b\sqrt{d}), a^2 - b^2d) = A\bar{A}$. If $a^2 - b^2d$ and p are relatively prime, $1 \in A\bar{A}$ which is a contradiction, thus $a^2 - b^2d \equiv 0 \pmod{p}$. Assuming that $b = 1$ like in all the above examples, $a^2 - d \equiv 0$. Thus $(p) = (p, a + \sqrt{d})(p, a' + \sqrt{d})$ only if there are a, a' that satisfy the equation $a^2 - d \equiv 0 \pmod{p}$. It turns out that a and a' are the two roots of this equation, which will be additive inverses of each other. But the ideal $(p, -a + \sqrt{d}) = (p, a - \sqrt{d})$.

Problem 3 (a) Suppose that a prime integer p remains prime in R . Prove that $R/(p)$ is then a field with p^2 elements.

Two good ways to this:

1) Since (p) remains prime ideal, and maximal since we are dealing with the ring of integers. However, in the ring of integers, prime ideals are maximal so $R/(p)$ is a field. The number of elements is p^2 by counting lattice points. Also, one could use the fact that $R/(p)$ is a finite integral domain which is a field.

2) Since p stays prime, by Prop 11.9.3, $g(x) = x^2 - d(x^2 - x + \frac{1}{4}(1-d))$ respectively if $d \equiv 1 \pmod{4}$ is irreducible over \mathbb{F}_p . But letting $F = \mathbb{F}_p[x]/(g(x)) = \mathbb{F}_p[\alpha]$ such that $g(\alpha) \equiv 0$. F will be a field made up of linear combinations of $a + b\alpha$ for $a, b \in \mathbb{F}_p$. p^2 such elements.

Problem 3 (b) Prove that if p splits in R , then $R/(p)$ is isomorphic to the product ring $\mathbb{F}_p \times \mathbb{F}_p$.

By proposition 11.9.3, $g(x) \equiv (x-a)(x-b)$ for $a, b \in \mathbb{F}_p$. One can create an isomorphism between $R/(p)$ and $\mathbb{F}_p \times \mathbb{F}_p$ by the following map:

Let $\phi : R/(p) = \mathbb{F}_p[x]/(g(x)) \rightarrow \mathbb{F}_p[x]/(x-a) \times \mathbb{F}_p[x]/(x-b)$ by $\phi(\bar{w}) = (\bar{y}, \bar{z})$ such that \bar{y} is the remainder when we set $x \equiv a$ and \bar{z} is the remainder when we set $x \equiv b$. Notice that either of these equivalences implies $g(x) \equiv 0$.

And $\mathbb{F}_p[x]/(x-a) \cong \mathbb{F}_p$ since setting $x \equiv a$ an element which is already in the field doesn't change \mathbb{F}_p .

Problem 4 Let p be a prime which splits in R , say $(p) = P\bar{P}$, and let $\alpha \in P$ be any element which is not divisible by p . Prove that P is generated as an ideal by (p, α) .

Let $\alpha = a + b\sqrt{d}$. Then $P\bar{P} = (p^2, p(a + b\sqrt{d}), p(a - b\sqrt{d}), a^2 - b^2d)$. If we want $(p) = P\bar{P}$, we need p divides all the generators (or alternatively no element outside of (p) in $P\bar{P}$) and $p \in P\bar{P}$.

$\alpha \in P$ implies that $a^2 - b^2d = \alpha\bar{\alpha} \in P\bar{P} = (p)$. Since p clearly divides all the other three generators, we know have that p divides all the generators. Thus no element which p doesn't divide could be in $P\bar{P}$.

Now we can run into a problem if p does not equal a linear combination of the generators. Then $p \notin P$. Notice we already used the condition $\alpha \in P$. Here we use p does not divide α . Assume $p \neq 2$ and p does not divide d . Then $p \nmid \alpha = a + b\sqrt{d}$ implies that $p \nmid a$ or $p \nmid b$.

If $p \nmid a$, then $C = p(\alpha + \bar{\alpha}) = 2ap$ is not divisible by p^2 since $p \neq 2$. Thus $\gcd(p^2, C) = p$ over the integers which means there is a \mathbb{Z} -linear combination such that $p \in R$.

If $p \nmid b$, then $C' = p(\alpha - \bar{\alpha})\sqrt{d} = 2bdp$ is not divisible by p^2 , thus $\gcd(p^2, C') = p$ over the integers.

Here we need additional reasoning for the cases of $p = 2$ and $p|d$.

However there is another way¹ to do this without the need to break it into cases.

Let $P = (p, \alpha)$. Then $(p^2, p\alpha, p\bar{\alpha}, N(\alpha)) = P\bar{P} = (p^2)$ or (p) by Prop (9.1). We require $P\bar{P} = (p)$ by the given hypotheses. Assume $P\bar{P} = (p^2)$. Then since P is a prime ideal (factorization into prime ideals is unique even when R is not a UFD), $P = (p)$. But then $(p, \alpha) = (p)$. It is clear that $p \in P$ but $P \subset (p)$ only if p divides all the generators. But by hypothesis, $p \nmid \alpha$. $\Rightarrow \Leftarrow$

Problem 7 Assume that $d \equiv 2$ or $3 \pmod{4}$. Prove that a prime integer p ramifies in R if and only if $p = 2$ or p divides d .

if $p = 2$ and $d \equiv 3 \pmod{4}$, then $(2, 1 - \sqrt{d})^2 = (4, 2 - 2\sqrt{d}, 1 + d - 2\sqrt{d}) = (2)$ since $d \equiv 1 \pmod{2}$ implies 2 divides all generators and $(2 - 2\sqrt{d}) - (1 + d - 2\sqrt{d}) = 1 - d \equiv 2 \pmod{4}$.

Some students tried to use the fact that (p) ramifies if and only if $x^2 - d = (x - \alpha)^2$. However, one can only use this fact if one shows it.

if $p|d$ (notice this covers the case $d \equiv 2 \pmod{4}$ and $p = 2$) then $(p, \sqrt{d})^2 = (p, \sqrt{d})(p, -\sqrt{d}) = (p^2, p\sqrt{d}, d) = (p)$ since $p|d$ implies that p divides all the generators, and d square-free implies that $\gcd(p^2, d)$ over the integers is p which means that there is a \mathbb{Z} -linear combination such that $p \in (p, \sqrt{d})^2$.

Converse: Assume there exists a $p \neq 2$ such that $(p) = (p, a + b\sqrt{d})^2 = (p^2, p(a + b\sqrt{d}), a^2 - 2ab\sqrt{d} + b^2d) = A$.

Then $A \subset (p)$ only if p divides all the generators, so $p|a^2 + b^2d$ and $p|2ab$. $p \nmid 2$ so $p|a$ or $p|b$. If $p|a$, $p|a^2 + b^2d$ implies $p|b^2d$ which implies $p|b$ or $p|d$. And $p|b$ implies $p|a$. But $p|a$ and $p|b$ implies that p^2 divides all the generators and thus $p \notin A$. $\Rightarrow \Leftarrow$ Thus it must be the case $p|a$ and $p|d$.

Problem 11 Prove Proposition (9.1), i.e. If P is a nonzero prime ideal of R , then there is an integer prime p so that either $P = (p)$ or $P\bar{P} = (p)$ and that conversely there is a prime ideal P of R so that either $P = (p)$ or $P\bar{P} = (p)$.

This proof followed reasoning from class on February 22nd. If $N(P) = p$, then $P\bar{P} = (p)$. If not assume $N(P) = p_1 \cdot p_2 \cdot \dots \cdot p_n$. However, if $n > 2$ then there exists a factorization of $P\bar{P}$ into further prime ideals. $\Rightarrow \Leftarrow$ Hence, $N(P) = p_1 \cdot p_2$ and $N(P) = N(\bar{P})$ implies $N(P) = p^2$ and $P\bar{P} = (p)(p)$ and $P = (p)$.

¹Thanks to Elizabeth Schemm

For the converse, $(p) = P_1 P_2 \dots P_n$. $p = \bar{p}$ implies $N(p) = p^2 = N(P_1) \dots N(P_n)$. Thus there are at most two prime ideals dividing (p) . If there is one, $P = (p)$. If there are two, $N(P_1)N(P_2) = p^2$ implies $N(P_1) = N(P_2) = p$ and thus $(p) = P\bar{P}$.

3. CHAPTER 11, SECTION 10

Problem 3 Let $R = \mathbb{Z}[\delta]$ where $\delta^2 = -6$.

Problem 3 (a) Prove that the lattices $P = (2, \delta)$ and $Q = (3, \delta)$ are prime ideals of R .

See Problem 11.8.1 on PS #3.

Problem 3 (b) Factor the principal ideal (6) into prime ideals explicitly in R .

See Problem 11.8.1 on PS #3.

Problem 3 (c) Prove that the ideal classes of P and Q are equal.

$P \sim Q$ if there exists τ and σ such that $\tau P = \sigma Q$. In this case let $\tau = \delta$ and $\sigma = -2$. $\tau P = (2\delta, -6) = (-6, 2\delta) = \sigma Q$.

Problem 3 (d) The Minkowski bound for R is $[\mu] = 3$. Using this fact, determine the ideal class group of R .

First some review: The Minkowski bound can be found by the computation, $\mu < \frac{4}{\pi} \Delta(R)$. Since $6 \equiv 2 \pmod{4}$, $\Delta(R) = \sqrt{6}$ the area of the fundamental rectangle.

Now using this bound, we need to look at the prime ideals dividing primes ≤ 3 , namely 2 and 3. Since these primes were already analyzed, there are a priori five equivalence classes of ideas: $\langle (1) \rangle$, $\langle P \rangle$, $\langle \bar{P} \rangle$, $\langle \bar{Q} \rangle$, and $\langle Q \rangle$. However, (2) and (3) both ramify so $P = \bar{P}$ and $Q = \bar{Q}$. Furthermore, by part (c), $P \sim Q$. Thus there are two classes: $\langle (1) \rangle$ and $\langle P \rangle$. The only group structure a two-element group can have is C_2 .