Ash Notes
Chapter 1

Wiliam M. Faucette

If $p \equiv 1 \pmod 4$, then $(p-1)/2$ is even, so

$$1 \times 2 \times \cdots \times \frac{p-1}{2} \times -1 \times -2 \times \cdots \times -\frac{p-1}{2} = \left[\left(\frac{p-1}{2}\right)!\right]^2$$

But the left side is congruent modulo p to $(p-1)!$ and by Wilson's Theorem, this is congruent to -1 modulo p. So,

$$x = \left(\frac{p-1}{2}\right)!$$

is a solution to

$$x^2 \equiv -1 \pmod p$$

If $x^2 \equiv -1 \pmod p$, then p divides $x^2 + 1 = (x-i)(x+i)$ in $\mathbb{Z}[i]$. $p \nmid x \pm i$, so p is not prime in $\mathbb{Z}[i]$. The ring of Gaussian integers is a UFD, so $p = \alpha\beta$ for nonunits α, $\beta \in \mathbb{Z}[i]$.

The *norm* of $\alpha = a + bi \in \mathbb{Z}[i]$ is $N(\alpha) = a^2 + b^2$. Then

$$p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta) \text{ with } N(\alpha), N(\beta) > 1.$$

If $\alpha = x + yi \in \mathbb{Z}[i]$ This forces $N(\alpha) = N(\beta) = p$, so $x^2 + y^2 = p$.

Conversely, if $x^2 + y^2 = p$, then $p \equiv 1 \pmod 4$, since 3 isn't the sum of two squares modulo 4.

This argument relies on $\mathbb{Z}[i]$ being a UFD. In general, $\mathbb{Z}[\sqrt{m}]$ need not be a UFD.

---

1. Section 1.1

Definitions of field extension, algebraic element, integral over a subring, equation of integral dependence, algebraic integer (real or complex number integral over $\mathbb{Z}$). For all $d \in \mathbb{Z}$, $\sqrt{d}$ is an algebraic integer. Similarly, any n^{th} root of unity is an algebraic integer.

Five equivalent notions of $x \in R$ integral over a subring A:

(1) x is integral over A.

(2) The A-module $A[x]$ is finitely generated;

(3) x belongs to a subring B of R such that $A \subseteq B$ and B is a finitely generated A-module

(4) There is a subring B of R such that B is a finitely generated A-module and x *stabilizes* B, that is, $xB \subseteq B$.

(5) There is a faithful $A[x]$-module M finitely generated as an A-module

If $A \subseteq R$ is a subring and $x_1, \ldots, x_n \in R$ are integral over A, then $A[x_1, \ldots, x_n]$ is a finitely generated A-module.

Let A, B, and C be subrings of R. If C is integral over B and B is integral over A, then C is integral over A.

Definition of integral closure of A in R, integrally closed in R, an integral domain being closed, If x, y are integral over A, so are $x \pm y$ and xy. So the integral closure of A in R is a ring containing A.

The integral closure of A in R is integrally closed in R.

Any UFD is integrally closed (in its field of fractions).

2. Section 1.2

Definition of a multiplicative subset of a ring, localized ring, ring of fractions of R by S.

Construction of $S^{-1}R$. $S^{-1}R$ is a ring. If R is a domain, so is $S^{-1}R$. If R is a domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is the fraction field of R.

If $X \subseteq R$, define $S^{-1}X = \{x/s : x \in X, s \in S\}$. If I is an ideal of R, $S^{-1}I$ is an ideal of $S^{-1}R$. If I and J are ideals in R, then

(i) $S^{-1}(I + J) = S^{-1}(I) + S^{-1}(J)$

(ii) $S^{-1}(IJ) = S^{-1}(I)S^{-1}(J)$

(iii) $S^{-1}(I \cap J) = S^{-1}(I) \cap S^{-1}(J)$

(iv) $S^{-1}I$ is a proper ideal iff $S \cap I = \emptyset$.

Lemma. *Let $h : R \to S^{-1}R$ be the natural homomorphism of rings. If J is an ideal in $S^{-1}R$, then $I = h^{-1}J$, is an ideal in R and $S^{-1}I = J$. (Every ideal in $S^{-1}R$ is an extended ideal.)*

Lemma. *If I is any ideal of R, then $I \subseteq h^{-1}(S^{-1}I)$. There will be equality if I is prime and disjoint from S.*

Lemma. *If I is a prime ideal of R disjoint from S, then $S^{-1}I$ is a prime ideal of $S^{-1}R$.*

Theorem. *There is a one-to-one correspondence between prime ideals P of R that are disjoint from S and prime ideals Q of $S^{-1}R$, given by*

$$P \to S^{-1}P \quad \text{and} \quad Q \to h^{-1}(Q).$$

Definitions of multiplicative set, localization.

Proposition. *For a ring R, the following conditions are equivalent.*

(i) R is a local ring;

(ii) There is a proper ideal I of R that contains all nonunits of R;

(iii) The set of nonunits of R is an ideal.

Theorem. *Let R be a (commutative) ring (with 1) and P a prime ideal in R. Then R_P is a local ring.*

Note: It is convenient to write the ideal $S^{-1}I$ and IR_P.

Definition of localization of modules.