Advanced Algebra

Arup Pal

January–April, 2002
(Course given for M. Stat. 2nd year)

Indian Statistical Institute, Delhi Centre
7, SJSS Marg, New Delhi–110 016, India

Contents

Lecture 1

1 Groups

1.1 Definition

Example of a nonassociative operation. In $\mathbb{Z}$, take the operation $m \circ n = m^n$.

1.2 Examples

1. $(\mathbb{R}, +)$, $(\mathbb{R}\backslash\{0\}, \cdot)$.
2. $\mathbb{R}$ above replaced by $\mathbb{C}$, $\mathbb{Q}$ or $\mathbb{H}$.
3. $(\mathbb{Z}, +)$.
4. $(\mathbb{Z}_n, +)$.
5. $(\mathbb{Z}_p\backslash\{0\}, \cdot)$, p prime.
6. n^{th} roots of 1 with multiplication.
7. bijections of a set,
8. $\mathcal{S}_n$. $\mathcal{A}_n$.
9. homeomorphisms of a topological space,
10. isometric bijections of a metric space,

    Symmetry of a geometric object S (for us, a subset of $\mathbb{R}^2$ or $\mathbb{R}^3$) is a map from S to S that preserves distance, and maps S onto itself.
11. symmetries of various geometric figures, e.g. circle, square, rectangle, triangle and so on.

    The group of symmetries of a regular n-gon is called the **dihedral group** of order n, and is denoted by D_n.
12. vector spaces.
13. linear maps on a vector space under addition.

14. invertible linear maps on a vector space,
15. unitary operators on a Hilbert space.
16. $(M_n(\mathbb{C}), +)$, $M_n(\mathbb{R}), +)$.
17. $(GL(n, \mathbb{C}), \cdot)$, $(GL(n, \mathbb{R}), \cdot)$.
18. $(SL(n, \mathbb{C}), \cdot)$, $(SL(n, \mathbb{R}), \cdot)$, $O(n, \mathbb{R})$, $SO(n, \mathbb{R})$, $SU(n)$.
19. $SL(2, \mathbb{Z}_p)$.
20. fundamental group of a topological space.

Exercise 1.1 1.Let $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ denote rotation through an angle θ anticlockwise. Find $R_\theta(x, y)$. Does $\{R_\theta : \theta \in \mathbb{R}\}$ form a group under composition?

Same question for $\rho_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ where ρ_θ stands for reflection about the line making an angle θ with the x-axis.

What about the collection $\{R_\theta : \theta \in [0, 2\pi)\} \cup \{\rho_\theta : \theta \in [0, \pi)\}$?

1.3 Isomorphisms and homomorphisms

Role of isomorphisms: (i) to identify different groups so that one has to study lesser number of them, (ii) study one group and draw conclusions about another.

Lecture 2

Uniqueness of the identity, uniqueness of inverse of an element. Alternative conditions for being a group.

1.4 Direct products

1.5 Subgroups

Definition.
Intersection of subgroups.

Exercise 1.2 *A group can not be the union of two of its subgroups.*

relationship between homomorphisms and subgroups: Image and kernel of a homomorphism are subgroups of the original groups.

Order of an element, cyclic groups

Cosets: left, right and double cosets.

Lemma 1.3

1. *$Hx = Hy$ if and only if $xy^{-1} \in H$,*
2. *$xH = yH$ if and only if $x^{-1}y \in H$,*
3. *$HxK = HyK$ if and only if $y^{-1}Hx \in K$ if and only if $yKx^{-1} \in H$.*

Corollary 1.4 *Each of the above defines an equivalence relation in G.*

Remark 1.5 *$Hx = Hy$ does not imply $xH = yH$. An example where $Hx = Hy$ but $xH \neq yH$.*

Index of H in G is the number of distinct right (or left) cosets of H in G, and is normally denoted by $[G : H]$.

Theorem 1.6 (Lagrange's theorem) *If $|G| < \infty$, then $[G : H] = |G|/|H|$. In particular, $|H|$ divides $|G|$.*

Consequences:

1. If $a \in G$, then $o(a)|o(G)$.

2. If $a \in G$, then $a^{o(G)} = 1$.

3. $m, n \in \mathbb{Z}_+, (m, n) = 1$. Then $m^{\phi(n)} \equiv 1 \bmod n$.

4. If p is a prime, then $m^p \equiv m \bmod p$.

5. Any group of prime order is cyclic.

Lecture 3

1.6 Normal subgroups

A subgroup H in G is normal if $xHx^{-1} = H$ for all $x \in G$.

Theorem 1.7 *The following conditions are all equivalent:*

1. $xHx^{-1} = H$ *for all* $x \in G$,
2. $xHx^{-1} \subseteq H$ *for all* $x \in G$,
3. $xH \subseteq Hx$ *for all* $x \in G$,
4. $Hx \subseteq xH$ *for all* $x \in G$,
5. $Hx = xH$ *for all* $x \in G$,
6. *each right coset is a left coset,*
7. *each left coset is a right coset.*

1.7 Quotient groups

Natural map. Examples: $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$, $S^1 \cong \mathbb{R}/\mathbb{Z}$.

Lecture 4

1.8 Fundamental theorem of homomorphisms

Theorem 1.8 *Let $\phi : G \to H$ be a group homomorphism. Let $K = \ker \phi$, and $\pi : G \to G/K$ be the natural map. The there is a unique 1-1 homomorphism ψ from G/K to H such that $\phi = \psi \circ \pi$.*

1.9 Isomorphism theorems

Theorem 1.9 (first isomorphism theorem) *Let $N \triangleleft G$ and $H \leq G$. Then $HN/N \cong H/H \cap N$.*

Theorem 1.10 (second isomorphism theorem) *If $K \triangleleft G$, $H \leq G$ and $K \subseteq H$, then $G/H \cong (G/K)/(H/K)$.*

Lecture 5

1.10 Permutation groups

definition of cycles, Uniqueness of cycle decomposition, parity of a permutation, $\mathcal{A}_n$.
relationship between conjugacy classes and cycle structure

Theorem 1.11 (Cayley) *Any finite group is isomorphic to a subgroup of the permutation group.*

Lecture 6

order of a permutation, generators,

1.11 More on cyclic groups

Theorem 1.12 *Any two cyclic groups of the same order are isomorphic.*

Theorem 1.13 *If G is cyclic and $|G| = r$, then for each divisor d of r, there is exactly one subgroup H of order d, and $H = \{a \in G : a^d = 1\}$.*

If $G = <a>$, then $H = <a^{r/d}>$.

Theorem 1.14 *If $ab = ba$, and $o(a) = m$, $o(b) = n$, then there are integers r and s such that $o(a^r b^s) = l.c.m.(m, n)$.*

An example where $ab = ba$ but $o(ab) \neq l.c.m.(m, n)$: In $\mathcal{S}_{10}$, take $a = (1\,2)(3\,4\,5\,6\,7)$ and $b = (1\,2)(8\,9\,10)$.

Theorem 1.15 *A finite abelian group G is cyclic if and only if $|G| = \min\{n \in \mathbb{N} : a^n = 1\ \forall a \in G\}$.*

LECTURE 7

Proof of cayley's theorem,

Action of a group on a set, orbits, stabilizer.

Examples: action of the permutation group on the set $\{1, \ldots, n\}$. action of $GL(n, \mathbb{R})$, $O(n)$, $SO(n)$ etc on $\mathbb{R}^n$.

Special case: normalizers, centralizers, center, Class equation.

Applications of the class equation:

Proposition 1.16 *If* $|G| = p^n$*, where* p *is a prime, then* $|Z(G)| > 1$*.*

Proposition 1.17 *If* $|G| = p^2$*, where* p *is a prime, then* G *is abelian.*

Proof: (Use the fact that $G/Z(G)$ cyclic implies G abelian)

Lecture 8

Proposition 1.18 *If p divides $|G|$, then G has an element of order p.*

Proof for G abelian (does not require class equation), by induction on $|G|$: If G has no proper subgroup,then it has to be cyclic of prime order, in this case, p. So any its generators will have order p. Assume then that G has a proper subgroup H. If $p \nmid |G/H|$, then $p \mid |H|$ and by induction hypothesis, we are done. If $p \mid |G/H|$, then there is an $a \in G$ such that aH is of order p in G/H. Then $a^p \in H$. It follows that $(a^p)^{|H|} = 1$, and hence $(a^{|H|})^p = 1$. If $a^{|H|} = 1$, then $p \mid |H|$, so that we are through again by the induction hypothesis. And if $a^{|H|} \neq 1$ then $a^{|H|}$ is of order p.
Proof for nonabelian G (using class equation), by induction on $|G|$: If $p| \, |Z(G)|$, we are done. So assume $p \nmid |Z(G)|$. Then $p \nmid \sum \frac{|G|}{|N(a)|}$ and hence $p \nmid \frac{|G|}{|N(a)|}$ for some $a \notin Z(G)$. But that means $p \mid |N(a)|$, and by induction hypothesis, we are done. □

Theorem 1.19 (Sylow's theorem) *Let p be a prime and m, k be positive integers. Assume that $|G| = mp^k$. Then there exists a subgroup of G of order p^k and the number of such subgroups is $\equiv 1 \bmod p$.*

Proof: (by induction on $|G|$): If p^k divides any of the $|N(a)|$'s appearing in the second term of the class equation, we are done by induction hypothesis. Otherwise, p will divide the second term, and hence $p \mid |Z(G)|$. Let $a \in Z(G)$ be of order p. Let $N = <a>$. N is a normal subgroup of G of order p. Apply the induction hypothesis to the group G/N to get a subgroup of G/N of order p^{k-1}. Let $\pi : G \to G/N$ be the natural projection. Then $H := \pi^{-1}(K)$ is a subgroup of G of order p^k.

Proof using group action (due to P. X. Gallagher (1967)): Define $S = \{A \subseteq G : |A| = p^k\}$. Let $H_A = StabA = \{g \in G : gA = A\}$, $A \in S$. Then

1. $|S| = \binom{|G|}{p^k}$,
2. H_A acts on A,
3. orbits of H_A in A are precisely the right cosets of H_A contained in A,
4. since A is a disjoint union of orbits, each of which is a coset of H_A, we have $|H_A|$ divides $|A| = p^k$.

Define $S_0 = \{A \in S : |H_A| = p^k\}$. By the last observation above, $S - S_0 = \{A \in S : |H_A| = p^r : r < k\}$. Choose a $B \in S - S_0$. Look at its orbit under the action of G. Its size would be $|G|/|H_B|$ which is divisible by mp. Also, the orbit is contained in $S - S_0$. Thus $S - S_0$, being a disjoint union of such orbits, has size divisible by mp. Hence

$$|S| \equiv |S_0| \bmod mp. \tag{1.1}$$

Next we claim that S_0 is precisely the collection of all right cosets of subgroups of size p^k. To see this, take $A \in S_0$. Choose $x \in A$. Then $H_A x \subseteq A$. But we have $|A| = p^k = |H_A| = |H_A x|$. So $H_A x = A$. Conversely, if $A = Hx$, where H is a subgroup of size p^k, and $x \in$G, then $A \in S$ and $H_A = StabA = H$, so that $A \in S_0$. Therefore

$$\begin{aligned}
|S_0| &= (\#\text{ subgroups of size } p^k) \times (\#\text{ distinct right cosets of each such subgroup}) \\
&= n_k \times m.
\end{aligned}$$

Hence $|S| \equiv n_k m \bmod mp$. Consequently

$$n_k \equiv |S|/m \bmod p.$$

Finally show that $\frac{\binom{mp^k}{p^k}}{m} \equiv 1 \bmod p$. (Take G to be a cyclic group of order mp^k. Then we know that there exists exactly one subgroup of order p^k. Use the above congruence for this group to conclude that $\frac{\binom{mp^k}{p^k}}{m} \equiv 1 \bmod p$.) □

Definition 1.20 (Sylow p-subgroup)

Theorem 1.21 *Any two Sylow p-subgroups of G are conjugate.*

Proof: Let H and K be two Sylow p-subgroups. Define $\sim$ by $a \sim b$ if $HaK = HbK$. This is an equivalence relation, so G decomposes as a disjoint union of cosets HxK, i.e. there are $a_1, \ldots, a_r$ such that $G = \cup_i Ha_iK$, where the Ha_iK's are disjoint. So $|G| = \sum |Ha_iK| = |H| \sum \frac{|K|}{|a_i^{-1}Ha_i \cap K|}$. By our assumption, p does not divide $\sum \frac{|K|}{|a_i^{-1}Ha_i \cap K|}$. So for some i, we must have $|a_i^{-1}Ha_i \cap K| = |K|$, i.e. $a_i^{-1}Ha_i = K$. □

Corollary 1.22 *Let $|G| = mp^k$ where $p \nmid m$, and let n_k be as earlier. Then n_k divides m.*

Proof: Let $T = \{H \leq G : |H| = p^k\}$. Let G act on T by conjugation. By the forgoing theorem, the action is transitive. Hence $|T| = |G|/|StabH| = m/r$ where r is some divisor of m. Therefore this divides m. □

Lecture 9

Applications of Sylow's theorem: In each of the folowing cases, G has a nontrivial normal subgroup (assume p is an odd prime):

1. $|G| = 2^m p^n, \quad 2^k \not\equiv 1 \bmod p$ for $1 \leq k \leq m$,
2. $|G| = p^n q, \quad q \neq p, q \not\equiv 1 \bmod p$,
3. $|G| = ap, \quad p \nmid a, 1 + kp \nmid a$ for any $k \in \mathbb{N}$,
4. $|G| = p^k(p+1), \quad k > 1$,
5. $|G| = p^k(p^2 - 1), \quad k > 1, p \geq 3$,
6. $|G| = p^k(p+3)$.

Proposition 1.23 *If $|G| = p^k$, then any maximal subgroup of G is normal.*

Proposition 1.24 *If $|G| = p^k$, then any maximal subgroup is of index p in G.*

Proposition 1.25 (More on direct products) *Let $H_1, \ldots, H_n$ be subgroups of G. Suppose*

1. *$H_i \lhd G$ for all i,*
2. *$G = H_1 \ldots H_n$,*
3. *each $g \in G$ can be expressed uniquely as a product $h_1 \ldots h_n$, where $h_i \in H_i$.*

Then $G \cong H_1 \times \cdots \times H_n$.

The conditions (1)–(3) in the above proposition are equivalent to the following:

1. $H_i \lhd G$ for all i,
2. $G = H_1 \ldots H_n$,
3. $H_i \cap H_1 \ldots H_{i-1} H_{i+1} \ldots H_n = \varphi$,
4. elements of H_i and H_j commute for $i \neq j$.

Lecture 10

Proposition 1.26 *If $H, K \lhd G$, and $G = HK$, then $G/H \cap K \cong H/H \cap K \times K/H \cap K$.*

Corollary 1.27 $\mathbb{Z}_{p_1^{k_1} \ldots p_r^{k_r}} \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_r^{k_r}}$.

Corollary 1.28 $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ *if* $(m, n) = 1$.

Proposition 1.29 *If $|G| = p^k$ and G is cyclic, and x is an element in G of order less than p^k, then $x = y^p$ for some $y \in G$.*

Proof: Let g be a generator of G, and let $H = <g^p>$. Then H is a proper subgroup of G, and $x \in H$. Therefore for some n, $x = (g^p)^n = (g^n)^p$. □

Proposition 1.30 *Any finite abelian p-group is a direct product of cyclic p-groups.*

Proof: (by induction on $|G|$) Let H be a maximal subgroup of G. By induction hypothesis, there exist $H_1, \ldots, H_r$ such that H_i is cyclic of order p^{k_i}, $k_1 \geq k_2 \geq \cdots \geq k_r$, and $H = H_1 \times \cdots H_r$. Take $x \in G \backslash H$. Since $|G/H| = p$, we have $x^p \in H$, i. e. $x^p = x_1 x_2 \ldots x_r$, where $x_i \in H_i$.

Case I: $x^p = 1$. In this case, $G = <x> \times H_1 \times \cdots H_r$.

Case II: $x^p \neq 1$. First we claim that there exists an $z \in G \backslash H$ such that $z^p = z_1 \ldots z_r$ where $z_i \in H_i$ and each z_i is either 1 or is a generator for H_i. Let $j = \min\{i : z_i \neq 1\}$. Then $z^p = z_j z_{j+1} \ldots z_r$. $o(z^p) = o(z_j) = p^{k_j}$. Hence $o(z) = p^{k_j+1}$. Then $G = <z> \times K$, where $K = H_1 \times \cdots \times H_{j-1} \times H_{j+1} \times \cdots \times H_r$. (it is enough to show that $<z> \cap K = \{1\}$. If $z^m \in K$, then looking at the element $zK \in G/K$, we can conclude that $p \mid m$. Now if $0 < m < p^{k_j+1}$, then $0 < m/p < p^{k_j}$. But then $z^m = (z^p)^{m/p} = z_j^{m/p} \ldots z_r^{m/p}$. Since $H_j = <z_j>$ and $0 < m/p < p^{k_j}$, we can not have $z^m \in K$.) □

Proposition 1.31 *Let $|G| < \infty$, and $N \lhd G$. Let H be a Sylow p-subgroup of N. then $G = N_G(H)N$.*

Proof: Take $x \in G$. Then $xHx^{-1} \leq xNx^{-1} = N$, so that xHx^{-1} is also a Sylow p-subgroup of N. Hence there is an $y \in N$ such that $xHx^{-1} = yHy^{-1}$. But this means $y^{-1}x \in N_G(H)$. So $x = y(y^{-1}x) \in NN_G(H) = N_G(H)N$. □

Proposition 1.32 *If G is finite then the following are equivalent:*

1. *any Sylow subgroup is normal in G,*

2. *G is the direct product of its Sylow subgroups,*

3. *every maximal subgroup of G is normal in G.*

Proof: (2) $\Rightarrow$ (3): Let $H_1, \ldots H_r$ be Sylow subgroups such that $G = H_1 \times \cdots \times H_r$. Let K be a maximal subgroup of G. We want to show that $K \lhd G$.

Since $|H_1|, \ldots, |H_r|$ are pairwise coprime, we have $K = (K \cap H_1) \times \cdots \times (K \cap H_r)$. Now maximality of K implies that there is an i for which $K \cap H_i$ is maximal in H_i and for all $j \neq i$, $K \cap H_j = H_j$. Since H_i is a p-group, $K \cap H_i \lhd H_i$. Hence $K \lhd G$.

(3) $\Rightarrow$ (1): Let H be a Sylow subgroup of G. Then $H \leq N_G(H) \leq G$. Let K be a maximal subgroup of G such that $N_G(H) \leq K \leq G$. By assumption, $K \lhd G$. Also, since H is a Sylow subgroup of K, by the previous proposition, we get $G = N_G(H)K \leq K$. Thus we must have $N_G(H) = G$. $\square$

Theorem 1.33 *Any finite abelian group is direct product of cyclic p-groups.*

Proof: Proof follows from propositions 1.30 and 1.32. $\square$

1.12 Semidirect products

Definition, Examples: Weyl group $\mathcal{U}(\mathcal{H}) \circledS \mathcal{H}$, Dihedral group $D_n \cong \mathbb{Z}_2 \circledS \mathbb{Z}_n$.

Lecture 11

2 Rings

2.1 Definition

$(R, +, \cdot)$ is a ring with an identity if

1. $(R, +)$ is an abelian group,
2. $(R, \cdot)$ is an abelian semigroup with identity,
3. distributive laws hold.

2.2 Examples

1. $(\mathbb{Z}, +, \cdot)$.
2. $\mathbb{Z}$ above replaced by $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ or $\mathbb{H}$.
3. $(\mathbb{Z}_n, +, \cdot)$.
4. linear maps on a vector space under addition and composition.
5. $(M_n(\mathbb{C}), +, \cdot)$, $M_n(\mathbb{R}), +, \cdot)$.
6. $(M_n(R), +, \cdot)$, where R is a ring.
7. $\mathbb{Z}[\sqrt{2}] := \{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$, with addition and multiplication.
8. same as above with $\mathbb{Q}$ replacing $\mathbb{Z}$.
9. Real-valued functions on a space X with pointwise addition and multiplication.
10. $\mathbb{Z}[x] :=$ {polynomials in one indeterminate x and coefficients from $\mathbb{Z}$}, with usual sum and product.
11. Same as above with $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ replacing $\mathbb{Z}$.
12. More generally, take $R[x] :=$ {polynomials in one indeterminate x and coefficients from R}.

13. The space of all formal power series in one indeterminate x and with coefficients from a ring R.

2.3 Zero divisors

integral domains, division rings, fields, examples.

left zero-divisors, right zero-divisors

2.4 Units

elements with left inverse but no right inverse, elements with right inverse but no left inverse.

Set of units as a multiplicative group.

Proposition 2.1 *Let R be a commutative ring. Then $A \in M_n(R)$ is invertible if and only if* $\det A$ *is invertible in R.*

Corollary 2.2 *Let F be a field. Then $A \in M_n(F)$ is invertible if and only if* $\det A \neq 0$.

2.5 Quotient Rings

Alternative way of describing a normal subgroup in a group: Let $\sim$ be a congruence relation on G such that

1. $x \sim y, z \sim w \Rightarrow xz \sim yw$,
2. $x \sim y \Rightarrow x^{-1} \sim y^{-1}$.

Define $N = \{x \in G : x \sim 1\}$. Then $N \lhd G$, and $x \sim y$ if and only if $xN = yN$. Conversely, if $N \lhd G$, and we define $\sim$ by $x \sim y$ if $xN = yN$, then $\sim$ satisfies the two conditions listed above.

When we quotient G by N, we actually use this above congruence to identify certain elements in G.

For a ring, we say that a congruence relation is compatible with the ring structure if we have

1. $a \sim b, c \sim d \Rightarrow a + c \sim b + d, ac \sim bd$,
2. $a \sim b \Rightarrow -a \sim -b$.

In such a case, we can use this relation to identify elements in R, and give the resulting set a natural ring structure. Let us define, like in the case of a group, $I = \{a \in R : a \sim 0\}$. Then I must obey the following two conditions:

1. $a, b \in I \Rightarrow a - b \in I$,
2. $a \in I, b \in R \Rightarrow ab, ba \in I$.

Conversely, if I is such a structure, and we define $\sim$ by $a \sim b$ if $a - b \in I$, then it is a congruent relation compatible with the ring structure of R.

Lecture 12

2.6 More on ideals

Largest ideal contained in I and J is $I \cap J$.
Smallest ideal containing I and J is $I + J$.
In general, $IJ \subseteq I \cap J$.
Example where $IJ \subseteq I \cap J$, but $IJ \neq I \cap J$: $R = \mathbb{Z}, I = 4\mathbb{Z}, J = 6\mathbb{Z}, IJ = 24\mathbb{Z}, I \cap J = 12\mathbb{Z}$.
Examples of left and right ideals.

Proposition 2.3 *R is a division ring if and only if R and 0 are the only left ideals.*

Proposition 2.4 *Let R be commutative. Then R is a field if and only if R and 0 are the only ideals.*

2.7 Homomorphisms

homomorphisms$\leftrightarrow$ ideals.

Theorem 2.5 (Fundamental theorem of homomorphisms) *Let $\phi : R \to R'$ be a homomorphism. Let $K = ker\,\phi$. Then there exists an injective homomorphism ψ fom R/K to R' such that $\phi = \psi \circ \pi$, π being the natural projection map from R to R'.*

Lecture 13

An ideal I is said to be **maximal** if $I \subseteq J \subseteq R$ and J is an ideal implies $J = R$ or $J = I$. quotient ring by maximal ideals

Corollary 2.6 (First isomorphism theorem for rings) *Let R be a ring, S be a subring, and J be an ideal. Then $(S+J)/J \cong S/(S \cap J)$.*

Prime ring of a ring, characteristic.

2.8 Direct sum

2.9 An application

Theorem 2.7 (Chinese Remainder Theorem) *Let I_1 and I_2 be ideals in R such that $I_1 + I_2 = R$. Let $a_1, a_2 \in R$. Then there exists $a \in R$ such that $a \equiv a_i \bmod I_i, i = 1, 2$.*

Proof: It is enough to show that $(a_1 + I_1) \cap (a_2 \cap I_2)$ is nonempty, or, equivalently, that $(a_1 - a_2 + I_1) \cap I_2$ is nonempty. Since $I_1 + I_2 = R$, there exist $b_1 \in I_1$, $b_2 \in I_2$ such that $a_1 - a_2 = b_1 + b_2$. But then $a_1 - a_2 - b_1 = b_2 \in (a_1 - a_2 + I_1) \cap I_2$. □

Corollary 2.8 *Assume $I_1 + I_2 = R$. Let $I = I_1 \cap I_2$. Then $R/I \cong R/I_1 \oplus R/I_2$.*

Proof: Define $\phi : R \to R/I_1 \oplus R/I_2$ by $\phi(a) = (a + I_1) \oplus (a + I_2)$ and use the fundamental theorem. □

Lemma 2.9 *If $I + J = R$ and $I + K = R$, then $I + JK = R$.*

Theorem 2.10 (Chinese Remainder Theorem, general case) *Let $I_1, \ldots, I_n$ be ideals in R such that $I_i + I_j = R$ for $i \neq j$. Let $a_1, \ldots, a_n \in R$. Then there exists $a \in R$ such that $a \equiv a_i \bmod I_i, i = 1, \ldots, n$.*

Corollary 2.11 *Let m and n be two coprime integers. Then $\phi(mn) = \phi(m)\phi(n)$.*

Proof: Follows from the following two observations:

1. $\phi(m) = \#$ elements in $\mathbb{Z}_m$ that are not zero divisors,

2. $a \oplus b \in R_1 \oplus R_2$ is a zero divisor if and only if either a or b is a zero divisor.

Lecture 14

2.10 Field of fractions

Field of fractions of a commutative integral domain.

2.11 Various commutative domains

Explicit construction of the polynomial ring and the ring of formal power series in one variable over R. Degree of a polynomial.

Definition 2.12 An element $a \in R$ is **irreducible** if $a = bc$ implies either b or c (or both) is a unit. An element $a \in R$ is **prime** if $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Norm in $\mathbb{Z}$, units in $\mathbb{Z}$.

Proposition 2.13 *Any prime in a ring R is irreducible. The converse is not true in general.*

Example where an irreducible is not a prime: In $\mathbb{Z}[\sqrt{-5}]$, $9 = 3.3 = (2+\sqrt{-5})(2-\sqrt{-5})$, $21 = 3.7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$.

Definition 2.14 A ring R is called a **unique factorization domain** if any element can be expressed uniquely (up to permutation of factors and up to multiplication by units) as a finite product of irreducibles.

Definition 2.15 In a commutative ring R, an ideal I is said to be a **principal ideal** if $I = <a>$ for some $a \in R$.
A commutative ring is called a **principal ideal domain** if every ideal is a principal ideal.

Definition 2.16 A commutative integral domain R is called an **Euclidean domain** if there is a map $d : R \backslash \{0\} \to \mathbb{N}$ such that

1. $d(a) \leq d(ab)$ for all a, b.
2. for all $a, b \in R\backslash\{0\}$, there exist $q, r \in R$ satisfying $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$.

Examples: $\mathbb{F}[x]$, where $\mathbb{F}$ is a field.

Lecture 15

Proposition 2.17 *If R is a unique factorization domain, then any irreducible $a \in R$ is a prime.*

Proof: Let $p \in R$ be an irreducible, and suppose that $p \mid ab$. There exists a $c \in R$ such that $ab = pc$. Let $c = p_1 \cdots p_r$, $a = q_1 \cdots q_m$, $b = q_{m+1} \cdots q_{m+n}$ be decompositions of c, a and b into irreducibles. By uniqueness of the decomposition of $pc = ab$, p must be one of the q_j's, which means that it must divide either a or b. $\square$

Proposition 2.18 *Let R be an integral domain. Then R is a unique factorization domain if and only if every irreducible in R is a prime, and R contains no infinite sequence of elements $a_1, a_2, \ldots$, such that a_{i+1} is a proper factor of a_i for each i.*

Proof: Assume first that R is a unique factorization domain. We already know that any irreducible is a prime. We will now show that if b is a proper factor of a, then it must be a product of strictly lesser number of irreducibles than a. If b is a proper factor of a, then there is a nonunit c such that $a = bc$. Let $a = p_1 \cdots p_r$, $b = q_1 \cdots q_m$, $c = q_{m+1} \cdots q_{m+n}$ be the decomposition of a, b and c respectively into irreducibles. By uniqueness, we must have $r = m + n$, and since c is a nonunit, $n > 0$. So $m < r$. Hence if $\{a_i\}$ is a sequence in R such that a_{i+1} is a proper factor of a_i for each i, then for some n, a_n must be irreducible. Now again use uniqueness of factorizations to show that an irreducible does not have any proper factor.

Next let us assume that R satisfies both the conditions in the proposition. We will show that R is a unique factorization domain. Using the second condition, we will first show that any element admits an irreducible factor and in fact admits a decomposition into irreducibles. The fact that each irreducible is a prime will then ensure that such a decomposition is unique.

Take $a \in R$. Either a is an irreducible, in which case we are done, or there are b and c such that $a = a_1 b_1$. Again, either a_1 is an irreducible, in which case we are done, or a_1 is a proper factor of a. Now repeat the argument with a replaced by a_1, and continue the process. Because of the second condition, at some stage, we must have a_n irreducible.

By the above argument, there is an irreducible p_1 such that $a = p_1 b_1$. Next write b_2 as $b_2 = p_3 b_3$ where p_2 is irreducible. Continuing in this manner, thanks to the second condition, one would reach a stage where b_n will be a unit, so that we will have $a = p_1 p_2 \cdots p_n$, i.e. a product of irreducibles. $\square$

Proposition 2.19 *Let R be an integral domain. Then R is a unique factorization domain if and only if any two elements in R admit a g.c.d. and R contains no infinite sequence of elements $a_1, a_2, \ldots$, such that a_{i+1} is a proper factor of a_i for each i.*

Remark 2.20 1. The above results hold for any commutative semigroup with identity where cancellation holds.
2. The second condition (in each of the propositions) ensures existence of a factorization into irreducibles.

Proposition 2.21 *Any Euclidean domain is a principal ideal domain.*

Proof: This is essentially an imitation of the proof that $\mathbb{Z}$ is a principal ideal domain. □

Proposition 2.22 *Let R be a principal ideal domain. Let J_i be an ascending chain of ideals in R. Then the J_i's must be equal from some stage onwards.*

Proof: Each J_i is of the form a_iR. Let $J = \cup J_i$. Its easy to see that J is also an ideal, and hence is of the form aR for some a. Now $a \in aR = \cup a_iR$. So $a \in a_nR$ for some n. But then $a_iR = aR$ for all $i \geq n$. □

Observe that $a \mid b$ if and only if $bR \subseteq aR$, and as a consequence, $aR = bR$ if and only if $a = b$ up to multiplication by a unit. It follows from the above proposition that in a principal ideal domain, one can not have a sequence $\{a_i\}$ such that each a_{i+1} is a proper factor of a_i.

Proposition 2.23 *Any principal ideal domain is a unique factorization domain.*

Proof: It is enough to show that each irreducible is a prime. Observe that if $(a, b) = 1$, then there exist $c, d \in R$ such that $ac + bd = 1$. ($aR + bR$ is an ideal, hence a principal ideal of the form dR. But then $d \mid a$ and $d \mid b$. So $(a, b) = 1$ implies $aR + bR = R$, hence the conclusion). Now suppose p is an irreducible, $p \mid ab$ and $p \nmid a$. Then $(p, a) = 1$; so there exist $c, d \in R$ such that $pc + ad = 1$. Therefore $pcb + dab = b$. But this implies $p \mid b$. □

Lecture 16

2.12 Polynomial rings over commutative rings

Theorem 2.24 *Let R, S be commutative rings, $\phi : R \to S$ be a ring homomorphism and $u \in S$. Then there is a unique extension $\phi_u : R[x] \to S$ such that $\phi_u|_R = \phi$ and $\phi(x) = u$.*

Corollary 2.25 *Let $R \subseteq S$ be commutative rings, and $u \in S$. Then $R[u] \cong R[x]/I$ where I is an ideal in $R[x]$ such that $I \cap R = \Phi$.*

Theorem 2.26 *If R is a commutative integral domain, then $R[x_1, \ldots, x_n]$ is also a commutative integral domain, having the same units as R.*

Theorem 2.27 (Euclidean algorithm in $R[x]$) *Let $f(x), g(x) \in R[x]$, $g(x) \neq 0$. Let the degree of $g(x)$ be m and let the coefficient of x^m in $g(x)$ be c. Then there exists a $k \in \mathbb{Z}_+$ and polynomials $q(x), r(x) \in R[x]$ such that $c^k f(x) = q(x)g(x) + r(x)$ and $deg\, r(x) < deg\, g(x)$.*

Proposition 2.28 (Remainder theorem) *Let $p \in R[x]$, and $a \in R$. Then there is a unique $q \in R[x]$ such that $p[x] = (x-a)q[x] + p(a)$.*

Proposition 2.29 (Factor theorem) *Let $p \in R[x]$, $a \in R$. Then $x - a$ divides p if and only if $p(a) = 0$.*

Theorem 2.30 *If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is an Euclidean domain (hence a principal ideal domain).*

Remark 2.31 *$\mathbb{F}[x_1, \ldots, x_n]$ is not a principal ideal domain if $n > 1$. (the ideal of all polynomials with constant term zero is not a principal ideal)*

Lemma 2.32 *Let R be a UFD and $\mathbb{F}$ its field of fractions. Let $f(x) \in \mathbb{F}[x]$. Then there exist an $r \in \mathbb{F}$ and $g(x) \in R[x]$, $g(x)$ primitive, such that $f(x) = rg(x)$. Moreover, such a decomposition is unique (up to multilpication by units in R).*

Proof: Existence: Let $f(x) = r_0 + r_1 x + \ldots + r_n x^n$, where $r_i = a_i/b_i$, $a_i, b_i \in R$, have no common divisors. Let $b = b_0 \cdots b_n$. Then there exist $c_0, \ldots, c_n$ such that $f(x) = (b)^{-1}(c_0 + c_1 x + \ldots + c_n x^n)$. Let $d = g.c.d.(c_0, \ldots, c_n)$ and let d_i be such that $c_i = dd_i$ for all i. Let

$g(x) = d_0 + d_1 x + \ldots + d_n x^n$, and let $r = db^{-1}$. Then $f(x) = rg(x)$ is a decomposition of the required type.

Uniqueness: Let $f(x) = rg(x) = sp(x)$ be two such decompositions, where $r = ab^{-1}$ and$s = cd^{-1}$, $a, b, c, d \in R$. We then have $adg(x) = bcp(x)$. Let $e = g.c.d.(ad, bc)$, $ad = e\alpha$, $bc = e\beta$. If α is not a unit, then it does not divide bc, but divides $bcp(x)$. So $p(x)$ cannot be primitive. Similarly, if β is not a unit, $g(x)$ can not be primitive. Thus there is a unit u in R such that $ad = ubc$. But then $r = us$ and $ug(x) = p(x)$. □

Lecture 17

Lemma 2.33 *If $f(x)$ and $g(x)$ are associates in $\mathbb{F}[x]$ and they are both primitive elements of $R[x]$, then they are associates in $R[x]$.*

Proof: Follows from the uniqueness part in the earlier lemma. $\square$

Lemma 2.34 *Let R be a UFD. The product of two primitive polynomials is primitive.*

Proof: If $f(x)$ and $g(x)$ are primitive but $h(x) = f(x)g(x)$ is not, then there exists an irreducible p such that $p \nmid f(x)$, $p \nmid g(x)$ but $p \mid h(x)$. Since p is an irreducible, it is prime and hence $R/(p)$ is an integral domain. So $R/(p)[x]$ is also an integral domain. But the image of $f(x)$ and $g(x)$ are nonzero elements here whereas the image of their product $h(x)$ is zero. $\square$

Lemma 2.35 *Let R be a UFD. $f(x)$ be an element in $R[x]$ with positive degree. If $f(x)$ is irreducible in $R[x]$, then it is irreducible in $\mathbb{F}[x]$.*

Proof: Since $f(x)$ is irreducible in $R[x]$, it is primitive. Now assume if possible that $f(x)$ is reducible in $\mathbb{F}[x]$. Write $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{F}[x]$ and are both of positive degree. By one of the lemmas above, there exist $r, s \in \mathbb{F}$ and $g'(x)$ and $h'(x)$ in $R[x]$, both primitive, such that $g(x) = rg'(x)$, $h(x) = sh'(x)$. So $f(x) = rsg'(x)h'(x)$. Since $g'(x)h'(x)$ is primitive, this implies rs is a unit in R, which means $f(x)$ is reducible in $R[x]$. $\square$

Theorem 2.36 *If R is a unique factorization domain, then $R[x]$ is also a unique factorization domain.*

Proof: We have to show two things: first, a factorization exists, and second, it is unique.

Existence: Start with $f(x) \in R[x]$. Write $f(x) = dp(x)$ where $d \in R$ and $p(x)$ is primitive. Let $d = d_1 \dots d_r$ be a factorization of d into irreducibles in R. Next, either $p(x)$ is irreducible or there exist $p_1(x)$ and $p_2(x)$ in $R[x]$, both of positive degree, such that $p(x) = p_1(x)p_2(x)$. Since $p(x)$ is primitive, so also are $p_1(x)$ and $p_2(x)$. This, along with the observation that any primitive polynomial of degree 1 is irreducible, tells us that $f(x)$ admits a factorization into irreducibles.

Uniqueness: Assume that $f(x)$ has two factorizations $f(x) = d_1 \dots d_r p_1(x) \dots p_n(x)$ and $f(x) = d'_1 \dots d'_s p'_1(x) \dots p'_m(x)$, where d_i and d'_i are elements of R and $p_i(x)$ and $p'_i(x)$ all have positive degree. Since the $p_i(x)$'s and $p'_i(x)$'s are irreducible in $R[x]$, they are primitive elements of $R[x]$ and are irreducible in $\mathbb{F}[x]$. It follows that $d_1 \dots d_r = d'_1 \dots d'_s$ and $p_1(x) \dots p_n(x) = p'_1(x) \dots p'_m(x)$. Since R is a UFD, we have $r = s$ and each d_i is an assocoiate of some d'_j and vice versa. Again $\mathbb{F}[x]$ is an Euclidean domain, hence is a UFD. So $m = n$ and (after some permutation) each $p_i(x)$ is an associate of $p'_i(x)$ in $\mathbb{F}[x]$. These are primitive elements of $R[x]$. So they are actually associates in $R[x]$. Thus we get uniqueness of the factorization. □

By repeated application, one has:

Corollary 2.37 *If R is a unique factorization domain, then $R[x_1, \dots, x_n]$ is a unique factorization domain.*

Definition 2.38 (Minimum polynomial)

Proposition 2.39 *Let u be algebraic over $\mathbb{F}$ with minimum polynomial $f(x)$. If $f(x)$ is irreducible in $\mathbb{F}[x]$, then $\mathbb{F}[u]$ is a field. If $f(x)$ is reducible, then $\mathbb{F}[u]$ is not a domain.*

Theorem 2.40 *Let $\mathbb{F}$ be a field and let f be a polynomial of degree n in $\mathbb{F}[x]$. Then f has at most n distinct roots in $\mathbb{F}$.*

Corollary 2.41 *Any finite subgroup of the multiplicative group of nonzero elements in a field is cyclic.*

Lecture 18

2.13 Applications to number theory

Theorem 2.42 (Four square theorem) *Any positive integer can be written as a sum of squares of four integers.*

Let $\mathbb{K}$ be the set of integer quaternions.

Lemma 2.43 *Let $\alpha \in \mathbb{K}$. Then α is a unit if and only if $N(\alpha) = 1$. The following are all the units in $\mathbb{K}$: ± 1, $\pm i$, $\pm j$, $\pm k$, $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$.*

Lemma 2.44 *Let $\alpha \in \mathbb{K}$. There exists a unit $u \in \mathbb{K}$ such that αu has integer coordinates.*

Lemma 2.45 *Let $\alpha \in \mathbb{K}$ and $N(\alpha)$ be odd. Then there exists a unit $u \in \mathbb{K}$ such that αu has non-integer coordinates.*

Lemma 2.46 *Let $\alpha \in \mathbb{K}$, $m \in \mathbb{N}$. There exists a $q \in \mathbb{K}$ such that $N(\alpha - mq) < m^2$.*

Lemma 2.47 *Let $\alpha \in \mathbb{K}$, $\beta \in \mathbb{K}$. There exists a $q \in \mathbb{K}$ such that $N(\alpha - \beta q) < N(\beta)$.*

Proposition 2.48 *Every right ideal in $\mathbb{K}$ is a principal right ideal.*

Proposition 2.49 *Let $\alpha \in \mathbb{K}$, $\beta \in \mathbb{K}$. Then there exists a $d \in \mathbb{K}$ such that*

1. *$d \mid_l \alpha$, $d \mid_l \beta$,*
2. *if $c \mid_l \alpha$ and $c \mid_l \beta$, then $c \mid_l d$.*

If d' is another element of $\mathbb{K}$ having the same properties as d, then there is a unit u such that $d' = du$.

Proof: Define $J = \{\alpha a + \beta b : a, b \in \mathbb{K}\}$. Since this is a right ideal, it is a principal right ideal and hence there is a $d \in \mathbb{K}$ such that $J = d\mathbb{K}$. □

Lecture 19

Proposition 2.50 *Let $\alpha \in \mathbb{K}$, $m \in \mathbb{N}$. Then the following conditions are equivalent:*

1. $(\alpha, m)_l = 1$,

2. $(N(\alpha), m) = 1$,

3. $(N(\alpha), m^2) = 1$.

Proof: (1)$\Rightarrow$ (2): There exist $a, b \in \mathbb{K}$ such that $\alpha a = 1 - mb$. Hence $N(\alpha)N(a) = 1 - mb - m\bar{b} + m^2 N(b)$. Therefore $(N(\alpha), m) \mid 1$, so that $(N(\alpha), m) = 1$.

(2)$\Rightarrow$ (3): Clear.

(3)$\Rightarrow$ (1): If $(\alpha, m)_l = d$, then $N(d) \mid N(\alpha)$ and $N(d) \mid m^2$. Since $(N(\alpha), m^2) = 1$, we have $N(d) = 1$, i.e. d is a unit. $\square$

Lemma 2.51 *If p is an odd prime, then there exist $x, y \in \mathbb{N}$ such that $1 + x^2 + y^2 = mp$ for some integer m, $0 < m < p$.*

Proof: Write $S_1 = \{x^2 : 0 \le x \le \frac{p-1}{2}, x \in \mathbb{Z}\}$, $S_2 = \{-1 - y^2 : 0 \le y \le \frac{p-1}{2}, y \in \mathbb{Z}\}$. Then $|S_1| = |S_2| = \frac{p+1}{2}$, but both are contained in $\mathbb{Z}_p$ which is of size p. So $S_1 \cap S_2 \ne \phi$. $\square$

Proposition 2.52 *If p is a prime in $\mathbb{N}$, then it is not an irreducible in $\mathbb{K}$.*

Proof: If $p = 2$, then the decomposition $p = (1+i)(1-i)$ shows that p is not irreducible.

If p is odd, choose x and y as in the forgoing lemma and let $\alpha = 1 + xi + yj$. Then $(N(\alpha), p) = p \ne 1$. So $(\alpha, p)_l = d \ne 1$. Write $p = dp'$. If p' is a unit, then it follows that $p \mid_l \alpha$, which can not be true. Thus none of d or p' is a unit. So p is not irreducible. $\square$

Proof of the four square theorem:

LECTURE 20

2.14 Quadratic residues

Definition 2.53 Let p be a prime number. An integer a is said to be a **quadratic residue modulo** p if $x^2 - a$ has a root in $\mathbb{Z}_p$.

Define the **Legendre symbol** $\left(\frac{a}{p}\right)$ by the following prescription:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \bmod p, \\ 1 & \text{if } a \not\equiv 0 \bmod p \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \not\equiv 0 \bmod p \text{ and } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Lemma 2.54 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *for all* $a, b \in \mathbb{Z}$.

Proof: Let G be the multiplicative group of nonzero elements of $\mathbb{Z}_p$, and let $S = \{x^2 : x \in G\}$. Then $|G| = p - 1$ and $|S| = (p-1)/2$. Observe that for $a \in G$,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in S, \\ -1 & \text{if } a \notin S. \end{cases}$$

Clearly, $a \in S$ and $b \in$S together imply $ab \in S$. Also, it is not too difficult to show that if $a \notin S$ and $b \in S$ then $ab \notin S$. So it remains to show that $a \notin S$, $b \notin S$ together imply $ab \in S$. For this observe that $|aS| = |S| = \frac{p-1}{2}$, aS and S are disjoint and consequently, $aS = G \backslash S$. Now for $b \notin S$, $ab \notin aS$. Hence $ab \in S$. □

Lemma 2.55 *If p is an odd prime, then* $\left(\frac{a}{p}\right) = 1$ *if and only if* $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Corollary 2.56 $\left(\frac{-1}{p}\right) = 1$ *if* $p \equiv 1 \bmod 4$.

Corollary 2.57 *If* $p \equiv 1 \bmod 4$, *then* p *is not a prime in* $\mathbb{Z}[i]$.

Remark 2.58 *Every irreducible is prime in* $\mathbb{Z}[i]$.

Theorem 2.59 *Let p be a prime such that* $p \equiv 1 \bmod 4$. *Then p can be written as a sum of squares of two integers.*

Corollary 2.60 *Let* $n \in \mathbb{N}$. *If any prime of the form* $4m + 3$ *appears with even power in the prime decomposition of* n, *then* n *can be written as a sum of squares of two integers.*

Lecture 21

3 Algebraic Number fields

Definition 3.1 A complex number is called **algebraic** if it is the root of some polynomial over $\mathbb{Q}$.

Proposition 3.2 *An algebraic number λ satisfies a unique irreducible monic polynomial equation g(x)=0 over $\mathbb{Q}$. Every polynomial of which λ is a root is divisible by $g(x)$.*

Definition 3.3 Degree of λ is the degree of $g(x)$ above.

Proposition 3.4 *An algebraic number of degree n is a root of a polynomial of degree n over $\mathbb{Z}$.*

Definition 3.5 An algebraic number is called an **algebraic integer** if it is a root of some monic polynomial with integer coefficients.

Proposition 3.6 *Let $\mathbb{K}$ be the set of all algebraic numbers. Then $\mathbb{K} \cap \mathbb{Q} = \mathbb{Z}$.*

Proposition 3.7 *Let $f(x)$, $g(x)$ and $h(x)$ be monic polynomials over $\mathbb{Q}$ such that $f(x) = g(x)h(x)$. If $f(x)$ has integer coefficients, then $g(x)$ and $h(x)$ must have integer coefficients.*

Proof: Let m and n be integers such that $mg(x)$ and $nh(x)$ are primitive polynomials over $\mathbb{Z}$ (Exercise: show that such a choice is possible). Then $mnf(x) = mng(x)h(x) = mg(x)nh(x)$. the right hand side, being a product of two primitive polynomials, is primitive. But since $f(x)$ has integer coeficients, this can happen only if $mn = \pm 1$, i.e. if both m and n are ± 1. □

Proposition 3.8 *Monic minimum polynomial of an algebraic integer has integer coefficients.*

Proof: Let λ be an algebraic integer and let $f(x)$ be its minimal monic polynomial. Since λ is an algebraic integer, there is a monic polynomial $g(x)$ over $\mathbb{Z}$ of which it is a root. But then $f(x) \mid g(x)$, i.e. there is a polynomial $h(x)$ in $\mathbb{Q}[x]$ such that $f(x)h(x) = g(x)$. Using the earlier result, we now conclude that $f(x)$ (as well as $h(x)$) has integer coefficients. □

Theorem 3.9 *The set of algebraic numbers form a field.*

Proposition 3.10 *Let λ be an algebraic number. Then there exists an integer $n \in \mathbb{N}$ such that $n\lambda$ is an algebraic integer.*

Proof: Let $f(x) = a_0x^k + a_1x^{k-1} + \ldots + a_k$ be a polynomial in $\mathbb{Z}[x]$ of which λ is a root. Take $n = a_0$ and $g(x) = a_0^{k-1}f(\frac{x}{a_0})$. Then $g(x)$ is a monic polynomial over $\mathbb{Z}$ and $n\lambda$ is a root of $g(x)$. $\square$

Definition 3.11 Let $\mathbb{F}$ be an algebraic number field. An element $\alpha \in \mathbb{F}$ is called an **integer in** $\mathbb{F}$ if it is an algebraic integer. An integer α in $\mathbb{F}$ is said to **divide** another integer β in $\mathbb{F}$ if there exists an integer γ such that $\beta = \alpha\gamma$. An element α in $\mathbb{F}$ is called a **unit** if it is a unit in the set of integers in $\mathbb{F}$.

Lecture 22

4 Quadratic fields

Let ξ be algebraic over $\mathbb{Q}$. Assume that the degree of the minimum polynomial of ξ is two. Then we call $\mathbb{Q}[\xi]$ a quadratic field over $\mathbb{Q}$, or simply a quadratic field. Clearly, ξ will be of the form $a + b\sqrt{m}$, where $a, b \in \mathbb{Q}$, and m is a square-free integer. Consequently, $\mathbb{Q}[\xi] = \mathbb{Q}[\sqrt{m}]$.

Denote by D the set of all algebraic integers contained in $\mathbb{Q}[\sqrt{m}]$. Elements of D are called the integers in the quadratic field $\mathbb{Q}[\sqrt{m}]$.

Proposition 4.1 *Let m be square-free. If $m \not\equiv 1 \bmod 4$, then $D = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$. If $m \equiv 1 \bmod 4$, then $D = \{a + b\sqrt{m} : a, b$ are both integers or both half-integers$\}$.*

Proof: Take an element $\frac{a+b\sqrt{m}}{c} \in \mathbb{Q}[\sqrt{m}]$, where $a, b, c \in \mathbb{Z}$, $c > 0$ and the g.c.d. of a, b and c is 1. Its minimal polynomial is $x^2 - \frac{2a}{c}x + \frac{a^2 - mb^2}{c^2}$. The element $\frac{a+b\sqrt{m}}{c}$ is an algebraic integer if and only if both $\frac{2a}{c}$ and $\frac{a^2-mb^2}{c^2}$ are integers, i.e. if $c \mid 2a$ and $c^2 \mid a^2 - mb^2$.
Claim: $(a, c) = 1$.
(There exists an $f \in \mathbb{Z}$ such that $a^2 - mb^2 = c^2 f$. Hence if $(a, c) = d$, then $d^2 \mid mb^2$. Since m is squarefree, if $d > 1$, we can get hold of a factor d_1 of d such that $d_1 \mid b$ and $d_1 \neq 1$. But then g.c.d.(a, b, c) can not be 1.)
Since $c \mid 2a$, we must have $c = 1$ or $c = 2$. If $c = 2$, then a is odd, $4 \mid a^2 - mb^2$ and hence $mb^2 \equiv 1 \bmod 4$. So $m \equiv 1 \bmod 4$ and b is odd. Thus if $m \not\equiv 1 \bmod 4$, then c must be 1, i.e. $D = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$. $\square$

Remark 4.2 *Let*

$$\rho = \begin{cases} \frac{1}{2}(1 + \sqrt{m}) & \text{if } m \equiv 1 \bmod 4, \\ \sqrt{m} & \text{if } m \not\equiv 1 \bmod 4. \end{cases}$$

Then $D = \{a + b\rho : a, b \in \mathbb{Z}\}$.

4.1 Units in a quadratic field

Definition 4.3 An element u is called a **unit** if $u \in D$ and if u divides 1 in D.

Define $N : D \to \mathbb{Q}$ by $N(a + b\sqrt{m}) = a^2 - mb^2$. It is easy to see that the range of N is contained in $\mathbb{Z}$.

Proposition 4.4 *α is an integer in $\mathbb{Q}[\sqrt{m}]$ if and only if $\bar{\alpha}$ is an integer in $\mathbb{Q}[\sqrt{m}]$.*

Corollary 4.5 *If α is an integer in $\mathbb{Q}[\sqrt{m}]$, then $N(\alpha)$ is a rational integer.*

Exercise 4.6 *Give a counterexample to show that the converse of the above statement is not true.*

Proposition 4.7 *$u \in D$ is a unit if and only if $N(u) = \pm 1$.*

Proof: If u is a unit, then $N(u) \mid N(1) = 1$, so that $N(u) = \pm 1$. Conversely, if $N(u) = \pm 1$, then since $N(u) = u\bar{u}$, $u \mid 1$, so that u is a unit. □

Proposition 4.8 *Let $m < 0$. Then the following is a complete list of units in $\mathbb{Q}[\sqrt{m}]$:*
$m = -1$: ± 1, $\pm\sqrt{-1}$.
$m = -3$: ± 1, $\frac{1}{2}(\pm 1 \pm \sqrt{-3})$.
$m \neq -1, m \neq -3$: ± 1.

Proposition 4.9 *There are infinitely many units in any real quadratic field.*

Lemma 4.10 *Let x and y be two nonzero reals such that x/y is irrational, and let n be a positive integer. There exist two integers $a, b \in \mathbb{Z}$ such that*

$$|ax + by| \leq (|x| + |y|)/n, \quad |a| \leq n, \quad |b| \leq n.$$

Proof: Assume without any loss in generality that $x, y > 0$. Define $Q(i,j) = ix + jy$, $i, j \in \{0, 1, \ldots, n\}$. Observe that

1. $Q(i,j) = Q(i',j')$ if and only if $i = i'$, $j = j'$,

2. $\#\{Q(i,j) : i,j\} = (n+1)^2$, and

3. $0 \leq Q(i,j) \leq n(|x| + |y|)$.

Hence there exist two pairs of integers (i,j) and (i',j') such that $|Q(i,j) - Q(i',j')| \leq (|x| + |y|)/n$. Now take $a = i - i'$, $b = j - j'$. □

Corollary 4.11 *Let m be positive, squarefree. Then there exists a (rational) integer k such that the equation $a^2 - b^2 m = k$ has infinitely many integral solutions.*

Proof: Take $x = 1$ and $y = \sqrt{m}$ in the earlier proposition. Then for any positive integer n, there exist integers a and b such that

$$|a + b\sqrt{m}| \leq (1 + \sqrt{m})/n, \quad |a| \leq n, \quad |b| \leq n.$$

Observe that such a and b, we also have $|a - b\sqrt{m}| \leq (1+\sqrt{m})n$. Therefore, for each positive integer n, there are integers a_n and b_n such that $|a_n| \leq n$, $|b_n| \leq n$, and

$$|a_n + b_n\sqrt{m}| \leq (1+\sqrt{m})/n, \quad |a_n^2 - mb_n^2| \leq (1+\sqrt{m})^2. \tag{4.2}$$

Next, note that thanks to the first condition above, there are infinitely many distinct pairs among the (a_n, b_n)'s. Now, because of the second condition, there is a (rational) integer k such that $a_n^2 - b_n^2 m = k$ for infinitely many pairs (a_n, b_n). □

Exercise 4.12 *Show that there exists a (rational) integer k such that the equation $a^2 - b^2 m = k$ has infinitely many integral solutions (a, b) with $a > 0$.*

Lemma 4.13 *Let m be positive, squarefree. Then the equation $a^2 - b^2 m = 1$ has infinitely many integral solutions.*

Proof: We will show that given any positive integer N, there are at least N solutions of the above equation.

By the exercise above, there is a k and at least $Nk^2 + 1$ pairs of integers (a, b) with $a > 0$ such that $a^2 - mb^2 = k$. Among these, there exist at least $N+1$ pairs $(a_0, b_0), \ldots, (a_N, b_N)$ such that $a_i \equiv a_j \bmod k$ and $b_i \equiv b_j \bmod k$ for $0 \leq i, j \leq N$. Write $\beta_i = \frac{a_i + b_i\sqrt{m}}{a_0 + b_0\sqrt{m}}$, $i = 1, \ldots, N$. We will show that the β_i's are distinct, $N(\beta_i) = 1$ for all i and each β_i is of the form $c + d\sqrt{m}$ where c and d are rational integers. That would complete the proof.

First, β_i's are clearly distinct, because the pairs (a_i, b_i) are all distinct. $N(\beta_i) = 1$ because $N(a_i + b_i\sqrt{m}) = k$ for all i. It remains to show that each β_i is of the form $c + d\sqrt{m}$ where c and d are rational integers.

$$\beta_i = 1 + \frac{(a_i - a_0) + (b_i - b_0)\sqrt{m}}{a_0 + b_0\sqrt{m}} \tag{4.3}$$

$$= 1 + \frac{(a_i - a_0) + (b_i - b_0)\sqrt{m}}{k}(a_0 - b_0\sqrt{m}) \tag{4.4}$$

Since $k \mid a_i - a_0$ and $k \mid b_i - b_0$, the result follows. □

Lecture 23

4.2 Primes and irreducibles

Proposition 4.14 *Let α be an integer in $\mathbb{Q}[\sqrt{m}]$. If $N(\alpha) = \pm p$, where p is a rational prime, then α is ireducible.*

Proof: Follows from the fact that $\alpha = \beta\gamma$ implies $N(\alpha) = N(\beta)N(\gamma)$. $\square$

Proposition 4.15 *Any integer in $\mathbb{Q}[\sqrt{m}]$ can be factored as a product of irreducible integers.*

Proof:

Definition 4.16 We say that an algebraic number field $\mathbb{K}$ has the **unique factorization property** if the set of integers in $\mathbb{K}$ is a UFD. The field $\mathbb{K}$ is called **Euclidean** if the set of integers is an Euclidean domain.

We know that any Euclidean quadratic field has the unique factorization property.

Proposition 4.17 $\mathbb{Q}[\sqrt{m}]$ *is Euclidean for the following values of m:* 2, 3, -1, -2, -3, -7, -11.

Proof: Take two integers α and β in $\mathbb{Q}[\sqrt{m}]$ with $\beta \neq 0$. We will chose an integer $\gamma = r + s\sqrt{m}$ such that $|N(\alpha - \beta\gamma)| < |N(\beta)|$.
Case I. $m \in \{2, 3, -1, -2\}$.
Write $\alpha/\beta = a + b\sqrt{m}$, where $a, b \in \mathbb{Q}$. Choose $r, s \in \mathbb{Z}$ such that $|r - a| \leq 1/2$, $|s - b| \leq 1/2$. Then

$$\begin{aligned} N(\alpha - \beta\gamma) &= N(\beta)N(\alpha/\beta - \gamma) \\ &= N(\beta)((a-r)^2 - m(b-s)^2). \end{aligned}$$

Now for $m > 0$, we have

$$-\frac{m}{4} \leq (a-r)^2 - m(b-s)^2 \leq (a-r)^2 \leq \frac{1}{4},$$

and for $m < 0$, we have

$$0 \leq (a-r)^2 - m(b-s)^2 \leq \frac{1}{4}(1-m).$$

Proof in this case follows from these two inequalities.

Case II. $m \in \{-3, -7, -11\}$.

In this case, choose r and s in such a way that $2r, 2s \in \mathbb{Z}$, $|2b - 2s| \leq 1/2$, $2r \equiv 2s \bmod 2$, and $|2a - 2r| \leq 1$. $\square$

Remark 4.18 Let $m < 0$. $\mathbb{Q}[\sqrt{m}]$ has unique factorizatrion property for the following values of m: -1, -2, -3, -7, -11, -19, -43, -67, -163.

Proposition 4.19 *If $\mathbb{Q}[\sqrt{m}]$ has the unique factorization property, then for any prime π in $\mathbb{Q}[\sqrt{m}]$, there is a unique rational prime p such that $\pi \mid p$.*

Proof: Let $p := \min\{n \in \mathbb{N} : \pi \mid n\}$. This set is nonempty, since $\pi \mid N(\pi)$. Let us first show that p must be a rational prime. If not, there would exist positive (rational) integers p_1 and p_2, $1 < p_i < p$, such that $p = p_1 p_2$. Since π is a prime in $\mathbb{Q}[\sqrt{m}]$, either $\pi \mid p_1$ or $\pi \mid p_2$, in either case contradicting the definition of p. Next, if there are two distinct rational primes p and q such that π divides both, then π must divide 1, because there exist rational integers a and b such that $pa + qb = 1$. $\square$

Proposition 4.20 *Suppose $\mathbb{Q}[\sqrt{m}]$ has the unique factorization property. Then any rational prime p is either a prime in $\mathbb{Q}[\sqrt{m}]$ or a product of two (not necessarily distinct) primes in $\mathbb{Q}[\sqrt{m}]$.*

Proof: Suppose that p is not an irreducible in $\mathbb{Q}[\sqrt{m}]$. Then there exist integers α, β such that $p = \alpha\beta$ and none is a unit. But then $p^2 = N(p) = N(\alpha)N(\beta)$ and $N(\alpha)$ and $N(\beta)$ are both integers different from ± 1. So we must have $N(\alpha) = \pm p$, $N(\beta) = \pm p$. This means both α and β are ireducibles in $\mathbb{Q}[\sqrt{m}]$. Since $\mathbb{Q}[\sqrt{m}]$ has the unique factorization property, α and β are primes. $\square$

Remark 4.21 The last two propositions give us all the primes in $\mathbb{Q}[\sqrt{m}]$.

Proposition 4.22 *Let p be an odd rational prime such that $p \not| m$. Then p is a product of two primes in $\mathbb{Q}[\sqrt{m}]$ if and only if $\left(\frac{m}{p}\right) = 1$.*

Proof: First assume that $\left(\frac{m}{p}\right) = 1$. Then there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv m \bmod p$, i.e. $p \mid x^2 - m = (x + \sqrt{m})(x - \sqrt{m})$. But since p is odd, $p \not| x \pm \sqrt{m}$. So p is not a prime. By the previous proposition, it is the product of two primes.

Next assume that p is the product of two primes in $\mathbb{Q}[\sqrt{m}]$. Then there exist primes α and β in $\mathbb{Q}[\sqrt{m}]$ with $N(\alpha) = \pm p$ and $N(\beta) = \pm p$ such that $p = \alpha\beta$. Write $\alpha = a + b\sqrt{m}$. Then $a^2 - mb^2 = \pm p$, so that $(2a)^2 - m(2b)^2 = \pm 4p$. Now, if $p \mid b$, then it must also divide a and consequently $p^2 \mid a^2 - mb^2 = \pm p$, which is impossible. So $p \nmid b$ and hence $p \nmid 2b$. Therefore, there exists an $y \in \mathbb{Z}$ such that $2by \equiv 1 \bmod p$. But then $(2ay)^2 \equiv m(2by)^2 \equiv m \bmod p$. Thus $\left(\frac{m}{p}\right) = 1$. $\square$

Proposition 4.23 *Assume that* $\mathbb{Q}[\sqrt{m}]$ *has the unique factorization property. Let* p *be a rational prime such that* $p \mid m$*. Then* p *is the associate of the square of a prime in* $\mathbb{Q}[\sqrt{m}]$*.*

Proof: First observe that $\sqrt{m}$ is a prime in $\mathbb{Q}[\sqrt{m}]$. Now if $p = |m|$, then $p = \pm\sqrt{m}\sqrt{m}$, so that we are done. Assume then that $p < |m|$. Note that $m = p \cdot \frac{m}{p} = \sqrt{m}\sqrt{m}$, and $p \nmid \sqrt{m}$. So p is not a prime in $\mathbb{Q}[\sqrt{m}]$. So there exist primes α and β in $\mathbb{Q}[\sqrt{m}]$ with $N(\alpha) = \pm p$ and $N(\beta) = \pm p$ such that $p = \alpha\beta$. Since α is a prime, $\alpha \mid \sqrt{m}$, so that $\alpha^2 \mid m$. Since $N(\alpha) = \pm p$ and $p^2 \nmid m$, $\alpha \nmid m/p$. Therefore $\alpha^2 \mid p$. Finally, $N(p/\alpha^2) = 1$, i.e. p/α^2 is a unit. $\square$

Lecture 24

4.3 An application

We will use the arithmetic developed for the field $\mathbb{Q}[\sqrt{-3}]$ to show that the equation $x^3+y^3=z^3$ has no integer solutions apart from the trivial ones where one of x, y and z is allowed to be zero.

We have already seen that $\pi := \sqrt{-3}$ is a prime in $\mathbb{Q}[\sqrt{-3}]$. We also know that the following list gives all the units in $\mathbb{Q}[\sqrt{-3}]$: ± 1, $\frac{1}{2}(\pm 1 \pm \sqrt{-3})$. Denote the unit $\frac{1}{2}(1+\sqrt{-3})$ by ω.

Lemma 4.24 *The following are all the associates of* π*:* $\pm(1-\omega)$, $\pm(1-\omega^2)$, $\pm\pi$

Proof: (**Exercise!**).

Lemma 4.25 *Any integer in* $\mathbb{Q}[\sqrt{-3}]$ *is congruent to exactly one of* 0, 1 *or* -1 *modulo* π.

Proof: Take any integer $a+b\pi \in \mathbb{Q}[\sqrt{-3}]$. Then $a+b\pi = \pi(b+a\pi)+4a$, so that $a+b\pi \equiv 4a \bmod \pi$. Now $\pi \mid 3$, and $4a$ is congruent to 0, 1 or -1 modulo 3. Hence the result. □

One can restate the above lemma as follows: for any integer γ in $\mathbb{Q}[\sqrt{-3}]$, $\pi \mid \gamma(\gamma-1)(\gamma+1)$.

Proposition 4.26 *Let* α *and* β *be integers in* $\mathbb{Q}[\sqrt{-3}]$ *not divisible by* π*. Then we have the following:*

1. $\alpha \equiv 1 \bmod \pi \Rightarrow \alpha^3 \equiv 1 \bmod \pi^4$,
2. $\alpha \equiv -1 \bmod \pi \Rightarrow \alpha^3 \equiv -1 \bmod \pi^4$,
3. $\alpha^3+\beta^3 \equiv 0 \bmod \pi \Rightarrow \alpha^3+\beta^3 \equiv 0 \bmod \pi^4$,
4. $\alpha^3-\beta^3 \equiv 0 \bmod \pi \Rightarrow \alpha^3-\beta^3 \equiv 0 \bmod \pi^4$.

Proof: We will prove part 1. Other parts will follow from that.

Assume $\alpha \equiv 1 \bmod \pi$. Then there is an integer γ such that $\alpha = 1+\pi\gamma$. Then

$$\begin{aligned}
\alpha^3 &= 1+3\pi\gamma+3\pi^2\gamma^2+\pi^3\gamma^3 \\
&= 1-\pi^3\gamma-9\gamma^2+\pi^3\gamma^3 \\
&= 1+\pi^3(\gamma^3-\gamma)-\pi^4\gamma^2 \\
&= 1+\pi^3\gamma(\gamma-1)(\gamma+1)-\pi^4\gamma^2.
\end{aligned}$$

By the previous lemma, $\alpha^3 \equiv 1 \bmod \pi^4$. □

Proposition 4.27 *Suppose α, β and γ are integers in $\mathbb{Q}[\sqrt{-3}]$ such that $\alpha^3+\beta^3+\gamma^3=0$. If g.c.d.$(\alpha,\beta,\gamma)=1$, then π divides one and exactly one of α, β and γ.*

Proof: Use the forgoing proposition. □

Proposition 4.28 *Suppose there are integers α, β and γ in $\mathbb{Q}[\sqrt{-3}]$ such that $\pi \nmid \alpha\beta\gamma$, and units u, v and a positive rational integer r such that $\alpha^3+u\beta^3+v(\pi^r\gamma)^3=0$. Then $u=\pm 1$ and $r \geq 2$.*

Proof: Since $r>0$, it follows that $\alpha^3+u\beta^3 \equiv 0 \bmod \pi^3$. It follows from proposition 4.26 that $\alpha^3+u\beta^3 \equiv \pm 1 + u(\pm 1) \equiv 0 \bmod \pi^3$. Looking at all possible values of u, it follows that $\pm 1 + u(\pm 1)$ can take the following values: 2, 0, -2, $\pm(1\pm\omega)$, $\pm(1\pm\omega^2)$. Only zero in this list is divisible by π^3. Hence $\pm 1+u(\pm 1)=0$, which implies $u=\pm 1$.

Again using proposition 4.26, we get $\alpha^3 \pm \beta^3 \equiv 0 \bmod \pi^3 \Rightarrow \alpha^3\pm\beta^3 \equiv 0 \bmod \pi \Rightarrow \alpha^3\pm\beta^3 \equiv 0 \bmod \pi^4$. It follows then that $\pi^4 \mid v(\pi^r\gamma)^3$, so that $r \geq 2$. □

Proposition 4.29 *There do not exist integers α, β and γ in $\mathbb{Q}[\sqrt{-3}]$, a unit v and a positive rational integer $r \geq 2$ such that $\alpha^3+\beta^3+v(\pi^r\gamma)^3=0$.*

Proof: Suppose there exist integers α, β and γ in $\mathbb{Q}[\sqrt{-3}]$, a unit v and a positive rational integer $r \geq 2$ such that $\alpha^3+\beta^3+v(\pi^r\gamma)^3=0$. Without loss in generality, we can assume that g.c.d.$(\alpha,\beta,\gamma)=1$, and $\pi \nmid \gamma$. By proposition 4.27, it follows that $\pi \nmid \alpha$, $\pi \nmid \beta$. Thus if there exist integers α, β and γ in $\mathbb{Q}[\sqrt{-3}]$, a unit v and a positive rational integer $r \geq 2$ such that $\alpha^3+\beta^3+v(\pi^r\gamma)^3=0$, then there exists a triplet of integers (α,β,γ), a unit v and a rational integer $r \geq 2$ such that

$$\begin{aligned} \alpha^3+\beta^3+v(\pi^r\gamma)^3 &= 0, \\ g.c.d.(\alpha,\beta,\gamma)=1, &\qquad \pi \nmid \alpha\beta\gamma. \end{aligned} \tag{4.5}$$

Since for any such triplet, $N(\alpha^3\beta^3\pi^{3r}\gamma^3)$ is a positive rational integer, we can choose a triplet (α,β,γ) for which $N(\alpha^3\beta^3\pi^{3r}\gamma^3)$ is minimum.

We will now construct another triplet $(\alpha_0,\beta_0,\gamma_0)$ for which $N(\alpha_0^3\beta_0^3\pi^{3r}\gamma_0^3) < N(\alpha^3\beta^3\pi^{3r}\gamma^3)$. This would contradict the existence of (α,β,γ), which would in turn imply that our initial assumption is wrong.

Since $r \geq 2$, we have $\alpha^3+\beta^3 \equiv 0 \bmod \pi^6$. Note that $\alpha^3+\beta^3=(\alpha+\beta)(\alpha+\omega\beta)(\alpha+\omega^2\beta)$. Let us first show that

1) if ρ is any prime that divides any two of the three factors above, then ρ is an associate of π, and

2) difference of any two of the above factors is divisible by π, but not by π^2.

It follows from (1) and (2) above that if a, b and c denote respectively the highest powers of

π that divide $(\alpha+\beta)$, $(\alpha+\omega\beta)$ and $(\alpha+\omega^2\beta)$, then $a+b+c=3r$, a, b, c must be 1, 1 and $3r-2$ in some order, and $\frac{\alpha+\beta}{\pi^a}$, $\frac{\alpha+\omega\beta}{\pi^b}$ and $\frac{\alpha+\omega^2\beta}{\pi^c}$ have no common factor.

Since $\alpha^3+\beta^3+v(\pi^r\gamma)^3=0$, we have $\frac{(\alpha+\beta)}{\pi^a}\frac{(\alpha+\omega\beta)}{\pi^b}\frac{(\alpha+\omega^2\beta)}{\pi^c}=-v\gamma^3$. Therefore, upto multiplication by units, each of $\frac{\alpha+\beta}{\pi^a}$, $\frac{\alpha+\omega\beta}{\pi^b}$ and $\frac{\alpha+\omega^2\beta}{\pi^c}$ must be the cube of an integer, i.e. there are units u_1, u_2, u_3 and integers α_0,β_0 and γ_0 such that $\frac{\alpha+\beta}{\pi^a}=u_1\alpha_0^3$, $\frac{\alpha+\omega\beta}{\pi^b}=u_2\beta_0^3$ and $\frac{\alpha+\omega^2\beta}{\pi^c}=u_3\gamma_0^3$. It follows then that $u_1\pi^a\alpha_0^3+\omega u_2\pi^b\beta_0^3+\omega^2u_3\pi^c\gamma_0^3=0$. Assume without loss in generality that $a=1=b$ (Show that there is really no loss in generality!). Then if we write $u_0=\omega u_2/u_1$ and $v_0=\omega^2u_3/u_1$, then u_0 and v_0 are units and $\alpha_0^3+u_0\beta_0^3+v_0\pi^{3r-3}\gamma_0^3=0$. By proposition 4.28, $u_0=\pm1$ and $r-1\geq 2$. Then $(\alpha_0,\pm\beta_0,\gamma_0)$ is a triplet, along with units v_0 and rational integer $r-1\geq 2$ that satisfy equations (4.5), and

$$\begin{aligned}
N(\alpha_0^3\beta_0^3\pi^{3r-3}\gamma_0^3) &= N(\pi^{-3}(\alpha+\beta)(\alpha+\omega\beta)(\alpha+\omega^2\beta)) \\
&= N(\pi^{-3}\pi^{3r}\gamma^3) \\
&< N(\alpha^3\beta^3\pi^{3r}\gamma^3).
\end{aligned}$$

Finally, we come to the proofs of the statements (1) and (2). □

Theorem 4.30 *The equation $x^3+y^3+z^3=0$ has no integer solutions in $\mathbb{Q}[\sqrt{-3}]$.*

Proof: Assume if possible that there are nonzero integers α, β and γ such that $\alpha^3+\beta^3+\gamma^3=0$. Assume without loss of generality that g.c.d.$(\alpha,\beta,\gamma)=1$. From proposition 4.27, π divides exactly one of α, β and γ. Suppose $\pi\mid\gamma$. Let $r\in\mathbb{N}$ be such that $\pi^r\mid\gamma$, $\pi^{r+1}\nmid\gamma$. Write $\gamma=\pi^r\delta$. Then $\pi\nmid\alpha\beta\delta$, and $\alpha^3+\beta^3+(\pi^r\delta)^3=0$. By proposition 4.28, $r\geq 2$, and then by the previous proposition, this is impossible. □