congruence in algebraic number field

Canonical name	CongruenceInAlgebraicNumberField
Date of creation	2013-03-22 18:17:11
Last modified on	2013-03-22 18:17:11
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	8
Author	pahio (2872)
Entry type	Theorem
Classification	msc 13B22
Synonym	congruence in number field
Related topic	CongruenceRelationOnAnAlgebraicSystem
Related topic	ChineseRemainderTheoremInTermsOfDivisorTheory
Related topic	Congruences
Defines	residue class

Definition. Let α, β and κ be `http://planetmath.org/AlgebraicInteger`integers of an algebraic number field K and $\kappa \neq 0$. One defines

$$\alpha \equiv \beta \pmod{\kappa} \tag{1}$$

if and only if $\kappa \mid \alpha - \beta$, i.e. iff there is an integer λ of K with $\alpha - \beta = \lambda\kappa$.

Theorem. The congruence "$\equiv$" modulo κ defined above is an equivalence relation in the maximal order of K. There are only a finite amount of the equivalence classes, the *residue classes modulo* κ.

Proof. For justifying the transitivity of "$\equiv$", suppose (1) and $\beta \equiv \gamma \pmod{\kappa}$; then there are the integers λ and μ of K such that $\alpha - \beta = \lambda\kappa$, $\beta - \gamma = \mu\kappa$. Adding these equations we see that $\alpha - \gamma = (\lambda + \mu)\kappa$ with the integer $\lambda + \mu$ of K. Accordingly, $\alpha \equiv \gamma \pmod{\kappa}$.
Let ω be an arbitrary integer of K and $\{\omega_1, \omega_2, \ldots, \omega_n\}$ a minimal basis of the field. Then we can write

$$\omega = a_1\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n,$$

where the a_i's are rational integers. For $i = 1, 2, \ldots, n$, the division algorithm determines the rational integers q_i and r_i with

$$a_i = \mathrm{N}(\kappa)q_i + r_i, \quad 0 \leqq r_i < |\mathrm{N}(\kappa)|,$$

whence

$$\omega = \mathrm{N}(\kappa)(\underbrace{q_1\omega_1 + q_2\omega_2 + \ldots + q_n\omega_n}_{=\pi}) + (\underbrace{r_1\omega_1 + r_2\omega_2 + \ldots + r_n\omega_n}_{=\varrho}).$$

So we have

$$\omega = \mathrm{N}(\kappa)\pi + \varrho, \tag{2}$$

where π and ϱ are some integers of the field. If $\kappa^{(1)}, \kappa^{(2)}, \ldots, \kappa^{(n)}$ are the algebraic conjugates of $\kappa = \kappa^{(1)}$, then

$$\mathrm{N}(\kappa) = \underbrace{\kappa^{(1)}}_{\text{integer}} \underbrace{\kappa^{(2)} \cdots \kappa^{(n)}}_{\text{integer}} = \kappa\kappa' \in \mathbb{Z}.$$

Hence, κ divides $\mathrm{N}(\kappa)$ in the ring of integers of K, and (2) implies

$$\omega \equiv \varrho \pmod{\kappa}.$$

Since any number r_i has $|\mathrm{N}(\kappa)|$ different possible values $0, 1, \ldots, |\mathrm{N}(\kappa)|-1$, there exist $|\mathrm{N}(\kappa)|^n$ different ordered tuplets $(r_1, r_2, \ldots, r_n)$. Therefore there exist at most $|\mathrm{N}(\kappa)|^n$ different residues and residue classes in the ring.