Let $s(t) = t^n + \sum_{i=0}^{n-1} c_i \in \mathbb{Q}[t]$ be an irreducible monic polynomial with coefficients in $\mathbb{Q}$. The the Galois group G of $s(t)$ acts on the set $R \subset \bar{\mathbb{Q}}$ of roots of $s(t)$ in $\bar{\mathbb{Q}}$. In other words we have an imbedding of the group G into the symmetric group S_n. In particular for any $\sigma \in G$ we can talk about the decomposition of σ into a product of cycles.

Last time we have shown that the Galois group of the polynomial $t^5 - 6t + 3$ over $\mathbb{Q}$ is equal to S_5. Our computation was based on the understanding of the structure of the decomposition of $t^5 - 6t + 3 \in \mathbb{R}[t]$ in the product of irreducible factors. More precisely we have shown that the polynomial $s(t)$ have exactly two non-real roots in $\mathbb{C}$ and therefore $s(t) = (t - a_1)(t - a_2)(t - a_3)q(t), a_i \in \mathbb{R}$ where $q(t) \in \mathbb{R}[t]$ is an irreducible quadratic polynomial and therefore there exists $\sigma \in G$ which is a 2-cycle.. There is an analogous approach to an understanding of a Galois group of a polynomials $s(t) \in \mathbb{Z}[t]$ which uses the decomposition of the reduction of $\bar{s}(t) \in \mathbb{F}_p[t]$ of $s(t)$ mod p.

As you remember we have already used the reduction mod$p$ in the proof of the Eisenstein's criterion for irreducibility. The proof was based of the lemma of Gauss which says that an irreducible monic polynomial with coefficients in $\mathbb{Z}$ is irreducible in $\mathbb{Q}[t]$ iff it is irreducible in $\mathbb{Z}[t]$. So we can talk unambiguously about irreducible monic polynomials in $\mathbb{Z}[t]$.

Let $s(t) = t^n + \sum_{i=0}^{n-1} c_i \in \mathbb{Z}[t]$ be an irreducible monic polynomial and $\bar{s}(t) := t^n + \sum_{i=0}^{n-1} \bar{c}_i \in \mathbb{F}_p[t]$ where $\bar{c}_i$ is the reduction of c_i mod p. Then the Galois group G of $s(t)$ acts on the set $R \subset \bar{\mathbb{Q}}$ of roots of $s(t)$ in $\bar{\mathbb{Q}}$. In other words we have an imbedding of the group G into the symmetric group S_n. In particular for any $\sigma \in G$ we can talk about the decomposition of σ into a product of cycles.

Theorem 12.1. Assume that all the roots of $\bar{s}(t)$ in the algebraic closure $\bar{\mathbb{F}}_p$ are simple. Let $\bar{s}(t) = \prod_{i=1}^{a} \bar{q}_i(t)$ be the decomposition of $\bar{s}(t)$ in the product of irreducible polynomials $\bar{q}_i(t) \in \mathbb{F}_p[t]$. Then there exists an element $\sigma_i \in G$ which is a product of cycles of lengths $\deg(\bar{q}_i(t)), 1 \leq i \leq a$.

Example. Let $s(t) = t^5 - t - 1 \in \mathbb{Z}[t]$. Let $s_2(t) \in \mathbb{F}_2[t]$ be the reduction of $s(t)$ mod 2 and $s_5(t) \in \mathbb{F}_5[t]$ be the reduction of $s(t)$ mod 5. One can check that the reduction of $s_5(t)$ is irreducible and $s_2(t) = (t^2 + t + 1)(t^3 + t^2 + 1)$ is the decomposition of $s_2(t)$ in the product of irreducible factors. It follows now from Theorem 12.1 that there exists elements $\sigma, \tau \in G$ such that τ is a 5-cycle and σ is a product of a 2-cycle and a 3-cycle. But then σ^3 is an elementary transposition

and it follows from Lemma 11.3 c) that the subgroup of S_5 generated by (σ^3, τ) is equal to S_5. So $G = S_5$.

The proof of the Theorem 12.1 is based on the theory of extensions of rings. We don't have enough time to derive the Theorem 12.1 but will develop some important concepts which are used in the proof of Theorem 12.1.

We start with some results in the theory of free abelian groups.

Let Λ be a finitely generated abelian group and $\Lambda' \subset \Lambda$ a subgroup fo finite index d. For any number m the inclusion $i : \Lambda' \hookrightarrow \Lambda$ induces the homomorphism $i_m : \Lambda'/m\Lambda'/ \to \Lambda/m\Lambda$.

Lemma 12.1. a) If $m > 1$ is a number prime to d then the the homomorphism $i_m : \Lambda'/m\Lambda'/ \to \Lambda/m\Lambda$ is an isomorphism,

b) If Λ is a finitely generated abelian group without non-trivial elements of finite order then Λ is a finitely generated free abelian group. [That there exists $e_1, ...e_n \in \Lambda$ such that any element $\lambda \in \Lambda$ can be written uniquely as a sum $\lambda = \sum_{i=1}^n c_i e_i, c_i \in \mathbb{Z}$.

I'll leave the proof of Lemma 12.1 as a homework.

We will also need the following result from linear algebra.

Let V be a finite-dimensional $\mathbb{Q}$-vector space of dimension $n, (,) : V \times V \to \mathbb{Q}$ a nondegenerate symmetric bilinear form, $e_1, ..., e_n$ a basis of V such that $(e_i, e_j) \in \mathbb{Z}$ for all $1 \leq i, j \leq n$. Let B be an $n \times n$ matrix with elements $b_{ij} := (e_i, e_j)$ and $D := Det(B)$.

We denote by $\Lambda \subset V$ be the free abelian group generated by this basis and define $\Lambda^\vee := \{v \in V | (v, e_i) \in \mathbb{Z}$ for all $1 \leq i \leq n$. It is clear that $\Lambda \subset \Lambda^\vee$.

Lemma 12.2. a) $\Lambda^\vee$ is a free abelian group with n generators,

b) the factor group $\Lambda^\vee/\Lambda$ is finite and $|\Lambda^\vee/\Lambda| = |D|$,

c) if $A \subset \Lambda^\vee$ be an abelian subgroup such that $A \supset \Lambda$ the A is is a free abelian group with n generators.

I'll leave the proof of Lemma 12.2 as a homework.

Definition 12.1. a) Let $K \supset \mathbb{Q}$ be a finite extension. Given $\alpha \in K$ we denote by $\mathbb{Z}[\alpha]$ the subring of K generated by α. In other words $\mathbb{Z}[\alpha]$ is the set of all elements $\beta \in K$ which can be written in the form $\beta = \sum_{i=0}^n c_i \alpha^i$ where $c_i \in \mathbb{Z}$.

b) We say that an element $\alpha \in K$ is *integral* if the ring $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group. [That is there exists a set $\gamma_1, ..., \gamma_n \in \mathbb{Z}[\alpha]$ such that any element $\beta \in \mathbb{Z}[\alpha]$ can be written in the form $\beta = \sum_{i=0}^n c_i \gamma_i$ where $c_i \in \mathbb{Z}$].

Lemma 12.3. Let $K \supset \mathbb{Q}$ be a finite extension, $\alpha \in K$ .Then the following three conditions are equivalent.

a) α is a root of a monic polynomial $s(t)$ with coefficients in $\mathbb{Z}$,

b) α is integral,

c) there exists a module M over the ring $\mathbb{Z}[\alpha]$ such that M which is finitely generated abelian group without non0trivial elements of finite order.

Proof. $a) \Rightarrow b)$.

Assume a). Assume that $\alpha \in K$ is a root of a monic polynomial $s(t) = t^n + \sum_{i=0}^{n-1} c_i$ with coefficients in $\mathbb{Z}$. Let M be the set of elements in K which can be written in the form $\sum_{i=0}^{n} a_i \alpha^i, 0 \leq i < n, a_i \in \mathbb{Z}$. I claim that $M = \mathbb{Z}[\alpha]$. Of course it is sufficient to show that

$\alpha^i \in M$ for all $i > 0$. By the construction we have $\alpha^i \in M$ for $i < n$. Since $p(\alpha) := \alpha^n + \sum_{i=0}^{n-1} c_i \alpha^i = 0$ we have $\alpha^n = -\sum_{i=0}^{n-1} c_i \alpha^i \in M$. It is easy now to show by induction in i that $\alpha^i \in M$ for all $i > 0$.

$b) \Rightarrow c)$. Take $M := \mathbb{Z}[\alpha]$.

$c) \Rightarrow a)$. As follows from Lemma 12.1 there exists elements $m_1, ..., m_n \in M$ such that for any $m \in M$ there exists unique set $a_j \in \mathbb{Z}, 1 \leq j \leq n$ such that $m = \sum_{j=1}^{n} a_j m_j$.

For all $i, 1 \leq i \leq n$ we $\alpha m_i \in M$ and therefore there exists $a_{ij} \in \mathbb{Z}, 1 \leq i, j \leq n$ such that $\alpha m_i = \sum_{j=1}^{n} a_{ij} m_j$.

We denote by $T : K^n \to K^n$ the K-linear transformation given by $T(e_i) = \sum_{j=1}^{n} a_{ij} e_j$ where $e_j, 1 \leq j \leq n$ is the standard basis in K^n. Let $p(t) := Det(tId - T)$. Then [by the teorem of Hamilton-Caley] we have $p(T) =)$. Therefore $p(\alpha) = 0$. On the other hand it is clear that $p(t)$ is monic polynomial in $\mathbb{Z}[t]$.$\square$

Remark. If $\alpha \in K$ is a integral element and $s(t) = Irr(\alpha, \mathbb{Q}, t)$ then the natural homomorphism $\mathbb{Z}[t] \to \mathbb{Z}[\alpha], t \to \alpha$ defines a ring isomorphism $\mathbb{Z}[t]/(s(t)) \to \mathbb{Z}[\alpha]$.

Corollary. Let $K \supset \mathbb{Q}$ be a finite extension and $A \subset K$ be the set of integral elements. Then A is a subring of K.

Proof. We have to show that for any pair $a, b \in A$ the sum $a + b$ and the product ab are also integral. As follows from Lemma 12.3 it is sufficient to construct a subgroup $M \subset K$ which is invariant under the multiplication by $a + b$ and ab and which is finitely generated as an abelian group.

Let $M \subset K$ be the abelian subgroup generated by elements of the form $xy, x \in \mathbb{Z}[\alpha], y \in \mathbb{Z}[\beta]$. It is clear that M is invariant under the

multiplication by a and b and therefore is invariant under the multiplication by $a+b$ and ab. On the other hand if $x_i \in \mathbb{Z}[\alpha], y_j \in \mathbb{Z}[\beta], 1 \leq i \leq s, 1 \leq j \leq t$ are generators of the abelian groups $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ then the products $x_i y_j, , 1 \leq i \leq s, 1 \leq j \leq t$ generate the abelian group M.$\square$

Definition 12.2. The ring $A \subset K$ of integral elements of K is called the ring of *algebraic integers* in K.

Lemma 12.4. Let $L \subset \mathbb{Q}$ be a finite extension, $\alpha \in A$ be an integral element. Then $Tr_{L/\mathbb{Q}}(\alpha), N_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Proof. I'll only show that $Tr_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Let $s(t) = t^n + \sum_{i=0}^{n-1} c_i t^i \in \mathbb{Q}[t]$ be an irreducible monic polynomial with coefficients in $\mathbb{Z}$ such that $s(\alpha) = 0$. Then it follows from Lemma 9.1 that $Tr_{K(\alpha)/\mathbb{Q}}(\alpha) = -c_{n-1} \in \mathbb{Z}$. But than $Tr_{L/\mathbb{Q}}(\alpha) = [L : K(\alpha)] Tr_{K(\alpha)/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.$\square$

Example. Let $n \in \mathbb{Z} - \mathbb{Z}^2, K = \mathbb{Q}(\sqrt{n})$. Any element in K has a form $\alpha = a + b\sqrt{n}$. How to see when $\alpha \in A$?

As follows from Lemma 12.4 if $\alpha \in A$ then $Tr_{K/\mathbb{Q}}(\alpha)t, N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. In other words $2a \in \mathbb{Z}$ and $a^2 - nb^2 \in \mathbb{Z}$.

Conversely if $2a \in \mathbb{Z}$ and $a^2 - nb^2 \in \mathbb{Z}$ then α is a root of a monic polynomial $t^2 - Tr_{K/\mathbb{Q}}(\alpha)t + N_{K/\mathbb{Q}}(\alpha) = t^2 - 2at + (a^2 - nb^2)$ with coefficients in $\mathbb{Z}$. So we see that $\alpha \in A$ iff $2a \in \mathbb{Z}$ and $a^2 - nb^2 \in \mathbb{Z}$.

Lemma 12.5. Assume that n is an odd square free number. Then
a) if $n \equiv 3(mod)4$ then $2a \in \mathbb{Z}$ and $a^2 - nb^2 \in \mathbb{Z}$ iff $a, b \in \mathbb{Z}$,
b) if $n \equiv 1(mod)4$ then $2a \in \mathbb{Z}$ and $a^2 - nb^2 \in \mathbb{Z}$ iff either $a, b \in \mathbb{Z}$ or $2a, 2b, a - b \in \mathbb{Z}$.

I'll leave the proof of Lemma 12.5 as a homework.

Lemma 12.6. For any $\beta \in K$ there exists $n \in \mathbb{Z} - 0$ such that $n\beta$ is an integral element of K.

I'll leave the proof of Lemma 12.6 as a homework.

Proposition 12.1. The ring $A \subset K$ of integral elements of K is a finitely generated abelian group.

Proof. Choose any $\beta \in K$ such that $K = \mathbb{Q}(\beta)$. By lemma 12.6 there exists $n \in \mathbb{Z} - 0$ such that $\alpha := n\beta \in A$. Since $K = \mathbb{Q}(\beta)$ we have $K = \mathbb{Q}(\alpha)$ and therefore elements $1, \alpha, \alpha^2, ..., \alpha^{n-1}, n := [K : \mathbb{Q}]$ is a basis of the $\mathbb{Q}$-vector space K. We consider the $\mathbb{Q}$-bilinear form $(,)$ on K given by $(x, y) := Tr_{K/\mathbb{Q}}(xy)$. As we know from Lemma 10.4 the $\mathbb{Q}$-bilinear form $(,)$ on K is nondegenerate.

Let $\Lambda \subset K$ be the free abelian group generated by this basis and $\Lambda^\vee := \{v \in K| := \{v \in K|(v, \alpha^i) \in \mathbb{Z}$ for all $1 \leq i \leq n$. It is clear that $\Lambda \subset A \subset \Lambda^\vee$. So Proposition 12.1 follows from Lemma 12.2.$\square$

Let k be a field, $\bar{s}(t)$ be a polynomial such that all the roots of $\bar{s}(t)$ in $\bar{k}$ are simple. Consider the decomposition $\bar{s}(t) == \prod_{i=1}^m \bar{q}_i(t) \in k[t]$ be a product of irreducible polynomials and define fields $L_i := k[t]/(\bar{q}_i(t))$. The natural homomorphisms $f_i : k[t] \to L_i$, define homomorphisms $r_i := k[t]/(\bar{s}(t))] \to L_i$ and therefore a ring homomorphism $r : k[t]/(\bar{s}(t)) \to \oplus_{i=1}^m L_i$.

Lemma 12.7 . [The Chinese reminder theorem]. The homomorphism $r : K[t]/(\bar{s}(t))] \to \oplus_{i=1}^m L_i$ is an isomorphism.

I'll leave the proof of the Chinese reminder theorem as a homework.

Let $s(t) = t^n + \sum_{i=0}^{n-1} c_i \in \mathbb{Z}[t]$ be an irreducible monic polynomial, $K := \mathbb{Q}[t]/(s(t)), A \subset K$ the ring of integers in $K, \alpha \in A$ the image of t under the natural surjection $\mathbb{Q}[t] \to K$.

Let p be a prime number and $\bar{s}(t) \in \mathbb{F}_p[t]$ the reduction of $s(t)$ mod$p, \bar{A} := \mathbb{F}_p[t]/(\bar{s}(t))$. We denote by $\bar{\alpha} \in \bar{A}$ the image of t under the natural surjection $\mathbb{F}_p[t] \to \mathbb{F}_p[t]/(\bar{s}(t))$ and by $\bar{\alpha} \in \bar{A}$ the image of t. The isomorphism $\mathbb{Z}[t]/(s(t)) \to \mathbb{Z}[\alpha]$ [see the Remark after the proof of Lemma 12.3] defines a ring homomorphism $\phi' : \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to \bar{A}$.

Lemma 12.8 . If an irreducible monic polynomial $s(t) = t^n + \sum_{i=0}^{n-1} c_i \in \mathbb{Z}[t]$ is such that all the roots of $\bar{s}(t)$ in $\bar{\mathbb{F}}_p$ are simple then the ring homomorphism $\phi' : \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to \bar{A}$ is an isomorphism and it extends to an isomorphism $A/pA \to \bar{A}$.

Proof. We will use notations introduced in the proof of Proposition 12.1. We also consider $\bar{V} := \mathbb{F}_p[t]/(\bar{s}(t))$ as an $\mathbb{F}_p$ vector space and define an $\mathbb{F}_p$-linear map $tr : \bar{V} \to \mathbb{F}_p$ by $tr(\bar{x}) := Tr_{\bar{V}} A_{\bar{x})}$ where $A_{\bar{x}} : \bar{V} \to \bar{V}$ is the operator of the multiplication by $\bar{x} \in \bar{V}$. We consider a bilinear form $(,)_p : \bar{V} \times \bar{V} \to \mathbb{F}_p$ given by $(\bar{x}, \bar{y})_p := tr(\bar{x}\bar{y})$. Let $\bar{B}$ the be the matrix of the bilinear form $(,)_p$ in the basis $1, \bar{\alpha}, ..., \bar{\alpha}^{n-1}$. It is clear that $\bar{B}$ is equal to the reduction mod$p$ of the matrix B of the bilinear form $(,)$ in the basis $1, \bar{\alpha}, ..., \bar{\alpha}^{n-1}$.

Since the finite extension of $\mathbb{F}_p$ is separable it follows from Lemma 12.7 that the form $(,)_p : \bar{V} \times \bar{V} \to \mathbb{F}_p$ is not degenerate. So $Det(\bar{B}) \neq 0$ and therefore $Det(B)$ is prime to p. So Lemma 12.8 follows from Lemma 12.2.$\square$