Groups and Fields
Lecture Notes

Lior Silberman

These are rough notes for the fall 2009 course. Problem sets and solutions were posted on an internal website.

Contents

Bibliography 63

CHAPTER 1

Introduction

Lior Silberman, lior@Math.UBC.CA, http://www.math.ubc.ca/~lior
Office: Math Building 229B
Phone: 604-827-3031

1.1. About the course

Course plan.

1.2. Problems to be discussed

Classification of groups.
Duplicating the cube, trisecting the angle, squaring the circle.
Insolubility of the quintic.
Cyclotomic extensions.

1.3. Definitions

1.3.1. Set Theory.

NOTATION 1. We write $\emptyset$ for the empty set, $[n] = \{0, \ldots, n-1\}$ for the standard set of size n.

NOTATION 2. For a set A write:

$$\bigcup A \stackrel{\text{def}}{=} \{x \mid \exists y \in A : x \in y\}, \qquad \bigcap A \stackrel{\text{def}}{=} \{x \mid \forall y \in A : x \in y\},$$

$$\mathcal{P}(A) = \{a \mid a \subseteq A\}.$$

For two sets A, B we write $A \cup B, A \cap B$ for $\bigcup\{A,B\}$ and $\bigcap\{A,B\}$ respectively. Also write

$$A \setminus B \stackrel{\text{def}}{=} \{x \in A \mid x \notin B\} \qquad A \Delta B \stackrel{\text{def}}{=} (A \setminus B) \cup (B \setminus A),$$

$$A \times B \stackrel{\text{def}}{=} \{x \mid \exists a \in A, b \in B : x = (a,b)\}.$$

DEFINITION 3. A *relation* on a set S is any subset $R \subset S \times S$. We write xRy for $(x,y) \in R$, and for $A \subset S$ also $R[A] = \{y \mid \exists x \in A : (x,y) \in R\}$. We call a relation:

(1) *Reflexive* if $\forall x \in S : xRx$;
(2) *Symmetric* if $\forall x, y \in S : xRy \leftrightarrow yRx$;
(3) *Transitive* if $\forall x, y, z \in S : (xRy \wedge yRz) \rightarrow xRz$;

If $S' \subset S$ we write $R \restriction_{S'}$ for the *induced relation* $R \cap S' \times S'$.

DEFINITION 4. A relation which is reflexive and transitive is called a *partial order*. A partial order is called a *linear order* if for every distinct $x, y \in S$ exactly one of xRy and yRx holds. A subset of a A partially ordered set S is called a *chain* if $R \restriction_A$ is a linear order on A.

If $(S, \leq)$ is a partial order and $A \subset S$ we say $m \in S$ is an *upper bound* for A if for any $a \in A$ we have $a \leq m$. We say $m \in S$ is *maximal* if for any $m' \in S$ such that $m \leq m'$ we have $m = m'$. Note that maximal elements are not necessarily upper bounds for S.

AXIOM 5. *(Zorn's Lemma) Let $(S, \leq)$ be a partial order such that every chain in S has an upper bound. Then S has maximal elements.*

DEFINITION 6. A *function* is a set f of ordered pairs such that $\forall x, y, y' \; ((x,y) \in f \wedge (x,y') \in f) \rightarrow y = y'$. For a function f write $\mathrm{Dom}(f) = \{x \mid \exists y : (x,y) \in f\}$, $\mathrm{Ran}(f) = \mathrm{Im}(f) = \{y \mid \exists x : (x,y) \in f\}$ for its domain and range (image), respectively, and if $x \in \mathrm{Dom}(f)$ write $f(x)$ for the unique y such that $(x,y) \in f$. Say that f is a function *from X to Y* if $\mathrm{Dom}(f) = X$ and $\mathrm{Ran}(f) \subset Y$, in which case we write $f : X \rightarrow Y$. Write Y^X for the set of functions from X to Y.

Given a function f and $A \subset \mathrm{Dom}(f)$ write $f[A]$ for the *image* $\{f(x) \mid x \in A\}$ and $f \restriction_A$ for the *restriction* $\{(x,y) \in f \mid x \in A\}$. This is a function with domain A and range $f[A]$.

Say that a function f is *injective* if $\forall x, x' : (f(x) = f(x')) \rightarrow (x = x')$; say that $f : X \rightarrow Y$ is *surjective* if $f[X] = Y$, *bijective* if it is injective and surjective.

AXIOM 7. *(Axiom of Choice) Let X be a set. Then there exists a function c with domain X such that for all $x \in X$ such that x is non-empty, $c(x) \in x$.*

FACT 8. *Under the usual axioms of set theory, AC is equivalent to Zorn's Lemma.*

NOTATION 9. Let A be a function with domain I. We write:

$$\bigcup_{i\in I} A(i) \stackrel{\text{def}}{=} \bigcup \text{Ran}(A), \qquad \bigcap_{i\in I} A(i) \stackrel{\text{def}}{=} \bigcap \text{Ran}(A)$$

and

$$\times_{i\in I} A(i) \stackrel{\text{def}}{=} \{f \mid f \text{ is a function with domain } I \text{ and } \forall i \in I\colon f(i) \in A(i)\}\ .$$

Note that the axiom of choice is the following assumption: let A be a function on I such that for all $i \in I$, $A(i)$ is non-empty. Then $\times_{i\in I} A_i$ is non-empty.

DEFINITION 10. For two sets A, B write $|A| \leq |B|$ if there exists an injective function $f\colon A \to B$, $|A| = |B|$ if these exists a bijection between A and B. Both relations are clearly transitive and reflexive. The second is clearly symmetric.

THEOREM 11. *(Cantor-Schroeder-Bernstein)* $|A| \leq |B|$ *and* $|B| \leq |A|$ *together imply* $|A| = |B|$. *(Using Zorn's Lemma) Given* A, B *at least one of* $|A| \leq |B|$ *and* $|B| \leq |A|$ *holds.*

NOTATION 12. For sets A, B write $B^A = \{f \subset A \times B \mid f \text{ is a function with } \text{Dom}(f) = A\}$. For a set A and a cardinal κ We set $\binom{A}{\kappa} = \{x \in \mathcal{P}(A) \mid |x| = \kappa\}$ (read "A choose κ").

1.3.2. Groups.

DEFINITION 13. A *group* is a quadruplet $(G, e, \imath, \cdot)$ where $e \in G$, $\imath\colon G \to G$, $\cdot\colon G \times G \to G$ and:

(1) $\forall g, h, k \in G\colon (g \cdot h) \cdot k = g \cdot (h \cdot k)$ [associative law].
(2) $\forall g \in G\colon e \cdot g = g$ [identity].
(3) $\forall g \in G\colon \imath(g) \cdot g = e$ [inverse].

Call the group G *Abelian* (or *commutative*) if for all $x, y \in G$, $g \cdot h = h \cdot g$.

EXAMPLE 14. The *symmetric group* on X is the set S_X of all bijections $X \to X$, with the composition operation.

NOTATION 15. We then write S_n for $S_{[n]}$ ("the symmetric group on n letters").

LEMMA 16. *Let* G *be a group,* $g, h \in G$. *Then* $g \cdot e = g$, $g \cdot \imath(g) = e$, *and the equations* $gx = h$ *and* $xg = h$ *have unique solutions. In particular the identity elements and inverses are unique, and we usually write* g^{-1} *for* $\imath(g)$.

DEFINITION 17. A non-empty subset $H \subset G$ is a *subgroup* if $e \in H$ and if $\imath(H), H \cdot H \subset H$. In that case we write $H < G$, and $(H, e, \imath \restriction_H, \cdot \restriction_{H\times H})$ is a group. The subgroup H is *normal* (denoted $H \lhd G$) if for all $g \in G$, ${}^gH = gHg^{-1} = H$.

When $H < G$ write $G/H = \{gH \mid g \in G\}$, $H\backslash G = \{Hg \mid g \in G\}$, and $[G : H]$ for the cardinality of either of these sets (the *index*) of H in G. $\imath$ induces a bijection between G/H and $H\backslash G$.

THEOREM 18. *(Lagrange) Let* $H < G$. *Then there is a set-theoretic bijection between* $H \times G/H$ *and* G. *In particular, if* $|G|$ *is finite then* $|H| \mid |G|$.

LEMMA 19. *If* N *is normal in* G *we have* $G/N = N\backslash G$ *and setting* $aN \cdot bN \stackrel{def}{=} abN$ *defines a group structure on* G/N. *We write* q_N *for the map* $g \mapsto gN$.

DEFINITION 20. Let H, G be groups. A map $f\colon H \to G$ is a *group homomorphism* if $f(ab) = f(a)f(b)$ for all $a, b \in H$. This implies that $f(e_H) = e_G$ and that $f \circ \iota_H = \iota_G \circ f$. The set of homomorphisms will be denoted $\mathrm{Hom}(H, G)$. The *kernel* of $f \in \mathrm{Hom}(H, G)$ is the set $\mathrm{Ker}(f) = \{h \in H \mid f(h) = e_G\}$. The *image* of f is the set $\mathrm{Im}(f) = \mathrm{Ran}(f)$. When $N \lhd G$ the map q_H is a group homomorphism called the *quotient map*.

FACT 21. *Let $f \in \mathrm{Hom}(H, G)$. Then f is a monomorphism iff it is injective, an epimorphism iff it is surjective, and an isomorphism iff it is bijective.*

LEMMA 22. *Let $f \in \mathrm{Hom}_R(H, G)$. Then $\mathrm{Ker}(f) \lhd H$, $\mathrm{Im}(f) < G$. Moreover there is a unique isomorphism $\bar{f}\colon H/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ such that $\bar{f} \circ q_{\mathrm{Ker}(f)} = f$.*

Let $H, N < G$ with N normal. Then $HN < G$, N is normal in HN, $H \cap N$ is normal in H, and $HN/N \simeq H/H \cap N$.

Finally, let $N \lhd G$. Then q_N induces an order- and normality-preserving bijection between subgroups of G containing N and subgroups of G/N. If $N < H < G$ and $H \lhd G$ as well then $G/H \simeq (G/N)/(N/H)$.

DEFINITION 23. If $X \subset G$ write $\langle X \rangle \stackrel{\text{def}}{=} \bigcap \{H < G \mid X \subset H\}$ for subgroup *generated* by X.

EXAMPLE 24. The *infinite cyclic groups* is the additive group of $\mathbb{Z}$; the *finite cyclic groups* are its quotients $C_n \simeq (\mathbb{Z}/n\mathbb{Z}, +)$, $n \in \mathbb{Z}_{\geq 1}$.

LEMMA 25. *If $x \in G$ then $\langle x \rangle$ is isomorphic to a cyclic group. The order of $\langle x \rangle$ is called the* order *of x and is equal to the smallest $n \geq 1$ such that $x^n = e$.*

NOTATION 26. We write C_n for the cyclic group of order n, $D_{2n} = C_2 \ltimes C_n$ for the dihedral group of order $2n$ ($\{\pm 1\} \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting on $(\mathbb{Z}/n\mathbb{Z}, +)$ by multiplication).

1.3.3. Rings. All rings in this course are commutative unless noted otherwise.

DEFINITION 27. A (commutative) *ring* is a quintuple $(R, 1, 0, +, \cdot)$ consisting of a set R, two elements $0, 1 \in R$ and two binary operations $+, \cdot\colon R \times R \to R$, such that:

(1) $(R, 0, +)$ is an Abelian group;
(2) $\forall x, y, z \in R\colon (x \cdot y) \cdot z = x \cdot (y \cdot z)$ [associative law];
(3) $\forall x \in R\colon 1 \cdot x = x \cdot 1 = x$ [multiplicative identity];
(4) $\forall x, y \in R\colon x \cdot y = y \cdot x$ [commutative law];
(5) $\forall x, y, z \in R\colon x \cdot (y + z) = x \cdot y + x \cdot z \wedge (y + z) \cdot x = y \cdot x + z \cdot x$ [distributive law];
(6) $0 \neq 1$ [non-degeneracy].

LEMMA 28. *Let R be a ring.*

(1) *The neutral elements are unique.*
(2) *For any $r \in R$ we have $0 \cdot r = r \cdot 0 = 0$.*

EXAMPLE 29. (Rings)

(1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/m\mathbb{Z}$.
(2) For a ring R and a set X, the space of functions R^X with point-wise operations.

DEFINITION 30. Let R, S be rings. The map $f\colon R \to S$ is a *ring homomorphism* if:

(1) $f(0_R) = 0_S$.
(2) $f(1_R) = 1_S$.

(3) For all $x, y \in R$, $f(x +_R y) = f(x) +_S f(y)$.
(4) For all $x, y \in S$, $f(x \cdot_R y) = f(x) \cdot_S f(y)$.

The set of homomorphisms from R to S will be denoted $\mathrm{Hom}(R, S)$.

LEMMA 31. *Let $f \in \mathrm{Hom}(R,S)$. Then f is a monomorphism iff it is injective, an epimorphism iff it is surjective, and an isomorphism iff it is bijective.*

DEFINITION 32. Let R be a ring, and let $r \in R$.

(1) Say that r is *invertible* (or that it is a *unit*) if these exists $\bar{r} \in R$ such that $r \cdot \bar{r} = \bar{r} \cdot r = 1_R$. Write $R^\times$ for the set of units.
(2) Say that r is *reducible* if $r = ab$ for some non-units $a, b \in R$, *irreducible* otherwise.
(3) Say that r is a *zero-divisor* if these exists a non-zero $s \in R$ such that $rs = 0$ or $sr = 0$.

LEMMA 33. *Let $r \in R$ be invertible. Then it has a unique multiplicative inverse, to be denoted r^{-1} from now on. Writing $R^\times$ for the set of invertible elements, $(R^\times, 1, \cdot)$ is a group.*

NOTATION 34. Call $R^\times$ the multiplicative group *of R*.

DEFINITION 35. An additive subgroup $I \subset R$ is an *ideal* if for all $r \in R$ and $a \in I$, $ra \in I$. We write $I \lhd R$.

LEMMA 36. *There is a unique ring structure on the additive group R/I such that the quotient map $q_I \colon R \to R/I$ is a ring homomorphism.*

The kernel of any ring homomorphism is an ideal; if $f \in \mathrm{Hom}(R,S)$ then there exists a unique isomorphism $\bar{f} \colon R/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ so that $f = \bar{f} \circ q_{\mathrm{Ker}(f)}$.

1.3.4. Fields.

DEFINITION 37. We say that a ring R is:

(1) An *integral domain* if its only zero-divisor is 0_R, that is if (0) is a prime ideal.
(2) A *field* if its only non-unit is 0_R, that is if (0) is a maximal ideal..

EXAMPLE 38. $\mathbb{Z}$ is an integral domain; $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}/m\mathbb{Z}$ is an integral domain iff m is prime, in which case it is a field.

LEMMA 39. *Let F be a field, R a ring, and $f \in \mathrm{Hom}(F,R)$. Then f is injective.*

1.3.5. Modules (not a pre-requisite).

Let R be a ring.

DEFINITION 40. An R-module is a quadruplet $(V, \underline{0}, +, \cdot)$ where $(V, \underline{0}, +)$ is an abelian group , and $\cdot \colon R \times V \to V$ is such that:

(1) For all $\underline{v} \in V$, we have $1_R \cdot \underline{v} = \underline{v}$.
(2) For all $\alpha, \beta \in R$ and $\underline{v} \in V$, $\alpha \cdot (\beta \cdot \underline{v}) = (\alpha\beta) \cdot \underline{v}$ ($\alpha\beta$ denotes the product in R).
(3) For all $\alpha, \beta \in R$ and $\underline{u}, \underline{v} \in V$, $(\alpha + \beta)(\underline{u} + \underline{v}) = \alpha \cdot \underline{u} + \beta \cdot \underline{u} + \alpha \cdot \underline{v} + \beta \cdot \underline{v}$ (note that the RHS is meaningful since addition is associative and commutative).

If V, W are R-modules we call a map $f \colon V \to W$ a *homomorphism of R-modules* if it is a homomorphism of abelian groups such that for all $\alpha \in R$ and $\underline{v} \in V$, $f(\alpha \cdot \underline{v}) = \alpha \cdot f(\underline{v})$. Write $\mathrm{Hom}_R(V, W)$ for the set of R-module homomorphisms from V to W (the R may be omitted when clear from context). The kernel and image of a homomorphism are its kernel and image as a map of abelian groups.

LEMMA 41. *Let $f \in \mathrm{Hom}_R(V,W)$. Then f is a monomorphism iff it is injective, an epimorphism iff it is surjective, and an isomorphism iff it is bijective.*

EXAMPLE 42. Let X be a set, R a ring. Then R^X has the structure of an R-module under the *diagonal action* of R. We usually write R^n for $R^{[n]}$.

Complex conjugation is an element of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C},\mathbb{C})$ but not of $\mathrm{Hom}_{\mathbb{C}}(\mathbb{C},\mathbb{C})$.

LEMMA 43. *Let V be an R-module. Then for every $\underline{v} \in V$ we have $0_R \cdot \underline{v} = \underline{0}$.*

DEFINITION 44. Let V be an R-module. An subgroup $W \subset V$ is an *R-submodule* if for all $\alpha \in R$ and $\underline{w} \in W$, $\alpha\underline{w} \in W$.

LEMMA 45. *Let $f \in \mathrm{Hom}_R(V,W)$. Then $\mathrm{Ker}(f) \subset V$ and $\mathrm{Im}(f) \subset W$ are R-submodules.*

1.3.6. Vector spaces. Let F be a field. F-modules are called *vector spaces over F*; homomorphism of F-modules are called *F-linear maps*.

DEFINITION 46. Let V be a vector space over F, and let $S \subset V$. Say that S is *linearly dependent* if there exist $r \geq 1$ and finite sequences $\{\underline{v}_i\}_{i=1}^r \subset S$, $\{\alpha_i\}_{i=1}^r \subset F$ with $\underline{v}_i$ pairwise distinct and the the α_i not all zero such that

$$\sum_{i=1}^{r} \alpha_i \underline{v}_i = \underline{0}.$$

The empty sum (the case $r = 0$) is by definition equal to $\underline{0}$. Call S *linearly independent* if it is not dependent. Finally, say that $\underline{v} \in V$ *depends* on S if $\underline{v}$ is a linear combination of vectors from S (in particular, $\underline{0}$ depends on every set). Say that S *spans* a set $W \subset V$ if every $\underline{v} \in W$ depends on S and write $\mathrm{Span}(S)$ for the set of vectors depending on S. Finally say that $B \subset V$ is a *basis* if it is linearly independent and spans V.

LEMMA 47. $\mathrm{Span}(S) = \bigcap\{W \mid S \subset W \subset V \text{ and } W \text{ is a subspace}\}$. *In particular the span of S is the minimal subspace containing S.*

LEMMA 48. *Every vector space has a basis. In fact, every linearly independent set can be extended to a basis and every spanning set contains a basis. Moreover, any two bases of a vector space V have the same cardinality, called the* dimension *of V and denoted* $\dim_F V$.

THEOREM 49. *Let U,V be vector spaces over F. Let B,C be bases for U,V respectively. Then $\mathrm{Hom}_F(U,V)$ is in bijection with $\{A \in M_{B\times C}(F) \mid \forall b \in B : \#\{c \in C \mid A_{bc} \neq 0\} < \infty\}$.*

DEFINITION 50. Let V be an n-dimensional vector space over F. Let $A\colon V^n \to F$ be a non-zero alternating form. For $\varphi \in \mathrm{End}_F(V)$ we have $A \circ \varphi = cA$ for some $c \in F$. Set $\det(\varphi) = c$ and call it the *determinant* of F.

DEFINITION 51. Let x be a formal variable, and let $P_\varphi(x) = \det(xI - \varphi) \in F[x]$ be the *characteristic polynomial* of F. Then $P_\varphi(0) = (-1)^n \det(\varphi)$. Let t be the coefficient of x^{n-1} in $P_\varphi(A)$. We set $\mathrm{Tr}(A) = -t$.

THEOREM 52. *Fix a basis $\{\underline{v}_i\}_{i=1}^n$ for V, and let $A \in M_n(F)$ be the matrix associated to φ. Then $\det(A) = \sum_{\pi\in S_n} \mathrm{sgn}(\pi) \prod_{i=1}^n A_{i,\sigma(i)}$ and $\mathrm{Tr}(A) = \sum_{i=1}^n A_{ii}$.*

THEOREM 53. *(Cayley-Hamilton) $P_\varphi(\varphi) = 0$.*

Math 422/501: Problem set 1 (due 16/9/09)

Some group theory

1. (Cyclic groups)
   (a) Show that the infinite cyclic group $\mathbb{Z}$ is the unique group which has non-trivial proper subgroups and is isomorphic to all of them.
   (b) [optional] which groups have no non-trivial proper subgroups?

2. (Groups with many involutions) Let G be a finite group, and let $I = \left\{g \in G \mid g^2 = e\right\} \setminus \{e\}$ be its subset of *involutions* (e is the identity element of G).
   (a) Show that G is abelian if it has *exponent* 2, that is if $G = I \cup \{e\}$.
   (b) Show that G is abelian if $|I| \geq \frac{3}{4}|G|$.

Some polynomial algebra

3. Show that $(x-y)$ divides $(x^n - y^n)$ in $\mathbb{Z}[x,y]$. Conclude that for any ring R, polynomial $P \in R[x]$ and element $a \in R$ such that $P(a) = 0$ one has $(x-a)|P$ in $R[x]$.
4. Let R be an integral domain, $P \in R[x]$, $\{a_i\}_{i=1}^k \subset R$ distinct zeroes of P. Show that $\prod_i (x-a_i)|P$ in $R[x]$. Give a counterexample when R has zero-divisors.
5. Let $\mathcal{V}_n(x_1,\ldots,x_n) \in M_n(\mathbb{Z}[x_1,\ldots,x_n])$ be the *Vandermonde matrix* $(\mathcal{V}_n)_{ij} = x_i^{j-1}$. Let $V_n(\underline{x}) = \det(\mathcal{V}_n(\underline{x})) \in \mathbb{Z}[\underline{x}]$. Show that there exists $c_n \in \mathbb{Z}$ so that $V_n(\underline{x}) = c_n \prod_{i>j}(x_i - x_j)$.
   Hint: Consider V_n as an element of $(\mathbb{Z}[x_1,\ldots,x_{n-1}])[x_n]$.
6. Setting $x_n = 0$ show that $c_n = c_{n-1}$, hence that $c_n = 1$ for all n.

Some abstract nonsense

DEFINITION. Let G, H be groups, and let $f\colon G \to H$ be a homomorphism. Say that f is a *monomorphism* if for every group K and every two distinct homomorphisms $g_1, g_2\colon K \to G$, the compositions $f \circ g_1, f \circ g_2\colon K \to H$ are distinct. Say that f is an *epimorphism* if for every group K and every two distinct homomorphisms $g_1, g_2\colon H \to K$ the compositions $g_i \circ f\colon G \to K$ are distinct.

7. Show that a homomorphism of groups is a monomorphism iff it is injective, an epimorphism iff it is surjective.

8. (Variants)
   (a) Same as 7, but replace "group" with "vector space over the field F" and "homomorphism" with "F-linear map".
   (b) Consider now the case of rings and ring homomorphisms. Show that monomorphisms are injective, but show that there exist non-surjective epimorphisms.

*9. Replacing "groups" with "Hausdorff topological spaces" and "homomorphism" with "continuous map" show that:
   (a) A continuous map is a monomorphism iff it is injective.
   (b) A continuous map is an epimorphism iff its image is dense.

CHAPTER 2

Group theory

2.1. Group actions

DEFINITION 54. Let G be a group, X a set. A left (right) *action* of G on X is a map $\cdot\colon G\times X\to X$ (respectively $\cdot\colon X\times G\to X$) so that:

(1) $\forall x\in G\colon e\cdot x=x$ (respectively $x\cdot e=x$).
(2) $\forall g,h\in G, x\in X: g\cdot(h\cdot x)=x$ (respectively, $(x\cdot g)\cdot h=x$.

Let G act on the left on the sets X,Y. A map $f\colon X\to Y$ is said to be *G-equivariant* if $f(g\cdot x)=g\cdot f(x)$ for all $g\in G$, $x\in X$.

LEMMA 55. *(Group actions) Let G be a group, X a set.*

(1) *Let $\cdot$ be a left action of G on X. Then $(x,g)\mapsto g^{-1}x$ is a right action. Conversely, let $\cdot$ be a right action. Then $(g,x)\mapsto x\cdot g^{-1}$ is a left action.*
(2) *For each $g\in G$ the map $\sigma_g(x)=gx$ is a permutation of X, and the map $g\mapsto\sigma_g$ is a homomorphism $G\mapsto S_X$.*
(3) *Conversely, if $\sigma\colon G\to S_X$ is a homomorphism then $(g,x)\mapsto(\sigma(g))(x)$ is a left action of G on X.*

DEFINITION 56. Let G be a group. *A G-set* is a pair $(X,\cdot)$ where X is a set, $\cdot$ a left action of G on X. For G-sets X,Y we have $\mathrm{Hom}_G(X,Y)$ for the set of G-equivariant maps between them.

REMARK 57. When we talk about a group acting on a structure, we usually assume that the action preserves the structure.

EXAMPLE 58. (group actions)

(1) For any group G and set X we have the *trivial action* $g\cdot x=x$ for all g,x.
(2) For any set X, the symmetric group S_X acts on X.
(3) For a ring R, the group $R^\times$ acts on R by multiplication.
(4) Let F be a field, V a vector space, $\mathrm{GL}(V)=\mathrm{End}(V)^\times$. Then $\mathrm{GL}(V)$ acts on V,
(5) $G=(V,E)$ a finite graph. $\mathrm{Aut}_G=\{f\in S_V\mid\forall e\in E: f(e)\in E\}$.
(6) Let (X,d) be a metric space. Then $\mathrm{Isom}(X,d)$ acts on X.
(7) $\pi_1(M)$ acts on $\tilde{M}$.

EXAMPLE 59. Let G be a group. Then we have the *left-regular action* $(g,h)\mapsto gh$ and the *conjugation action* $(g,h)\mapsto ghg^{-1}={}^gh$. In both cases G acts on itself.

THEOREM 60. *(Cayley [**1**]) The left-regular action $G\mapsto S_G$ is an injective map. In other words, a group of order n is isomorphic to a subgroup of S_n.*

PROPOSITION 61. *The following are group actions:*

(1) *$G\circlearrowright X$. Then G acts on $\mathcal{P}(X)$ by $gA=\{ga\mid a\in A\}$. In fact, for a cardinal α G acts on $\binom{X}{\alpha}$.*

(2) $G \circlearrowright X$, $Y \subset X$ *is* G-invariant *($gY = Y$ for all g). Then* $G \circlearrowright Y$.
(3) *G a group acting on X, Y. Then Y^X is a G-set where for $f\colon X \to Y$ we set* $(gf)(x) = g \cdot_Y \left(f(g^{-1} \cdot_X x)\right)$.
(4) *$\{X_i\}_{i\in I}$ are G-sets. Then their* disjoint union $\bigcup_{i\in I}(X \times \{i\})$ *is a G-set with the action $g \cdot (x,i) = (gx,i)$ for any $g \in G$, $i \in I$, $x \in X_i$. It is a product in the category of G-sets.*
(5) *$\{X_i\}_{i\in I}$ are G-sets. Then their* Cartesian product $\prod_{i\in I} X_i$ *is a G-set with the action $(gf)(i) = g \cdot (f(i))$ for any $g \in G$, $f \in \prod_i X_i$, $i \in I$.*
(6) *G a group acting on X, $H < G$. Then $(h,x) \mapsto hx$ is an H-action of H on X denoted* $\mathrm{Res}^G_H X$.
(7) *H a group acting on X, $H < G$. Let* $\mathrm{Ind}^G_H X = \left\{f\colon G \to X \mid f(gh) = h^{-1}f(g)\right\}$. *This is a G-set where $(gf)(g') = f(g^{-1}g')$.*

DEFINITION 62. Say that a G-set X is *transitive* or that it is an *orbit* if for all $x, y \in X$ there exists $g \in G$ so that $gx = y$.

EXAMPLE 63. The G action on G/H is transitive.

Fix a group G and a G-set X.

LEMMA 64. *Then the relation $x \sim y \iff \exists g \in G : gx = y$ is an equivalence relation. The equivalence classes are called the* orbits *of the action. The set of orbits is denoted $G\backslash X$, and the orbit of x is denoted $\mathcal{O}(x)$ or $G \cdot x$.*

COROLLARY 65. $X = \bigsqcup_{\mathcal{O}\in G\backslash X} \mathcal{O}$.

DEFINITION 66. For $x \in X$ write $G_x = \mathrm{Stab}_G(x) = Z_G(x)$ for the *stabilizer* subgroup $\{g \in G \mid gx = x\}$.

LEMMA 67. $G_{gx} = gG_xg^{-1} = {}^gG_x$.

PROPOSITION 68. *Let X be a G-set, $x \in X$. Then $f\colon G \cdot x \to G/G_x$ given by $f(gx) = gG_x$ and $h\colon G/G_x \to X$ given by $h(gG_x) = gx$ are inverse G-morphisms.*

THEOREM 69. *Isomorphism classes of transitive G-sets are in bijection with conjugacy classes of subgroups of G.*

COROLLARY 70. *Let X be a G-set, and let $R \subset X$ be a set of representatives for the orbits. Then we have an isomorphism of G-sets $X \simeq \bigsqcup_{x\in R} G/G_x$. In particular, we have the* class formula

$$|X| = \sum_{x\in R} [G : G_x]\,. \tag{2.1.1}$$

Math 422/501: Problem set 2 (due 23/9/09)

Direct and semidirect products

1. Let G be a group, and let A, B be subgroups of G so that B is normal and $A \cap B = \{e\}$.
   (a) Show that $A \ltimes B = \{a \cdot b \mid a \in A, b \in B\}$ is a subgroup of G; and that every element of it can be uniquely written as a product $a \cdot b$. We call this subgroup the *internal semidirect product* of A, B.
   (b) Assuming that A is normal as well show that $ab = ba$ for all $a \in A$, $b \in B$. In that case we say that the subgroup AB is the *internal direct product* of A, B.

2. Let G, H be groups. Let $G \times H = \{(g,h) \mid g \in G, h \in H\}$ and give it the group structure $(g,h) \cdot (g',h') = (gg', hh')$. Show that this makes $G \times H$ into a group (called the *direct product* of G, H) and find normal subgroups $\bar{G}, \bar{H} < G \times H$ isomorphic to G, H respectively so that $G \times H$ is the internal direct product of $\bar{G}$ and $\bar{H}$.

3. Let G, H be groups and let G act on H by automorphisms (in other words, for each $g \in G$ you are given a group isomorphism $\alpha_g : H \to H$ such that $\alpha_{gh} = \alpha_g \circ \alpha_h$). Give the set $G \times H$ the group structure $(g',h') \cdot (g,h) = \left(g'g, \alpha_{g^{-1}}(h')h\right)$. Show that this gives a group structure called the *semidirect product* $G \ltimes H$. Show that the semidirect product contains subgroups $\bar{G}, \bar{H}$ with $\bar{H}$ normal such that $G \ltimes H$ is the internal semidirect product of G, H.

p-Groups

4. Let G be a non-abelian group of order p^3, p a prime. Show that $Z(G)$ has order p and that $G/Z(G) \simeq C_p \times C_p$.

Cyclic group actions and cycle decompositions

5. Let G be a group acting on a set X, and let $g \in G$. Show that a subset $Y \subset X$ is invariant under the action of the subgroup $\langle g \rangle$ of G iff $gY = Y$. When Y is finite show that assuming $gY \subset Y$ is enough.

6. For $\alpha \in S_n$ write $\mathrm{supp}(\alpha)$ for the set $\{i \in [n] \mid \alpha(i) \neq i\}$.
   (a) Show that $\mathrm{supp}(\alpha)$ is invariant under the action of $\langle \alpha \rangle$.
   (b) Show that if $\mathrm{supp}(\alpha) \cap \mathrm{supp}(\beta) = \emptyset$ then $\alpha\beta = \beta\alpha$.

7. (Cycle decomposition) Call $\sigma \in S_n$ a *cycle* if its support is a single orbit of $\langle\sigma\rangle$, in which case we call the size of the support the *length* of the cycle.
   (a) Let $\alpha \in S_n$, and let $O \subset [n]$ be an orbit of $\langle\alpha\rangle$ of length at least 2. Show that there exists a unique cycle $\beta \in S_n$ supported on O so that $\alpha \restriction_O = \beta \restriction_O$ (that is, the restrictions of the functions α, β to the set O are equal).
   (b) Let $\alpha \in S_n$ and let $\{\beta_O \mid O \text{ an orbit of } \langle\alpha\rangle\}$ be the set of cycles obtained in part (a). Show that they all commute and that their product is α.
   (c) Show that every element of S_n can be written uniquely as a product of cycles of disjoint support.
   (d) Consider the action of $[4]_{35} = 4 + 35\mathbb{Z} \in \mathbb{Z}/35\mathbb{Z}$ by multiplication on $\mathbb{Z}/35\mathbb{Z}$. Decompose this permutation into a product of cycles.

8. (The conjugacy classes of S_n)
   (a) Let $\alpha, \beta \in S_n$ with α a cycle. Show that $\beta\alpha\beta^{-1}$ is a cycle as well.
   (b) Show that $\alpha, \beta \in S_n$ are conjugate iff for each $2 \leq l \leq n$ the number of cycles of length l in their cycle decomposition is the same.
   Hint: Constructs a bijection from $[n]$ to $[n]$ that converts one partition into orbits into the other.

Affine algebra

DEFINITION 71. Let F be a field, V/F a vector space. An *affine combination* is a formal sum $\sum_{i=1}^n t_i \underline{v}_i$ where $t_i \in F$, $\underline{v}_i \in V$ and $\sum_{i=1}^n t_i = 1$. If V, W are vector spaces then a map $f\colon V \to W$ is called an *affine map* if for every affine combination in V we have

$$f\left(\sum_{i=1}^n t_i \underline{v}_i\right) = \sum_{i=1}^n t_i f(\underline{v}_i) .$$

9. (The affine group) Let U, V, W be vector spaces over F, $f\colon U \to V$, $g\colon V \to W$ affine maps.
   (a) Show that $g \circ f\colon U \to W$ is affine.
   (b) Assume that f is bijective. Show that its set-theoretic inverse $f^{-1}\colon V \to U$ is an affine map as well.
   (c) Let $\mathrm{Aff}(V)$ denote the set of invertible affine maps from V to V. Show that $\mathrm{Aff}(V)$ is a group, and that it has a natural action on V.
   (d) Assume that $f(\underline{0}_U) = \underline{0}_V$. Show that f is a linear map.
10. (Elements of the affine group)
   (a) Given $\underline{a} \in V$ show that $T_{\underline{a}}\underline{x} = \underline{x} + \underline{a}$ ("translation by $\underline{a}$") is an affine map.
   (b) Show that the map $\underline{a} \mapsto T_{\underline{a}}$ is a group homomorphism from the additive group of V to $\mathrm{Aff}(V)$. Write $\mathbb{T}(V)$ for the image.
   (c) Show that $\mathbb{T}(V)$ acts transitively on V. Show that the action is *simple*: for any $\underline{x} \in V$, $\mathrm{Stab}_{\mathbb{T}(V)}(\underline{x}) = \{T_{\underline{0}}\}$.
   (d) Fixing a basepoint $\underline{0} \in V$, show that every $A \in \mathrm{Aff}(V)$ can be uniquely written in the form $A = T_{\underline{a}}B$ where $\underline{a} \in V$ and $B \in \mathrm{GL}(V)$. Conclude that $\mathrm{Aff}(V) = \mathbb{T}(V) \cdot \mathrm{GL}(V)$ setwise.
   (e) Show that $\mathbb{T}(V) \cap \mathrm{GL}(V) = \{1\}$ and that $\mathbb{T}(V)$ is a normal subgroup of $\mathrm{Aff}(V)$. Show that $\mathrm{Aff}(V)$ is isomorphic to the semidirect product $\mathrm{GL}(V) \ltimes (V, +)$.

Additional (not for credit)

A. Let F be a finite field with q elements, V/F a vector space of dimension n. Find a formula for the *Gaussian binomial coefficient* $\binom{n}{k}_q$, the number of k-dimensional subspaces of V. Show that this is a polynomial in q and that its limit as $q \to 1$ is the usual binomial coefficient $\binom{n}{k}$.

B. Let F be a field, V a finite-dimensional F-vector space. A *flag* in V is a nested sequence $\{0\} = W_0 \subsetneq W_1 \subsetneq \cdots \subsetneq W_k \subsetneq W_{k+1} = V$ of subspaces of V. An ordered basis $\{\underline{v}_i\}_{i=1}^n \subset V$ is said to be *adapted* to W if for all j, $W_j = \operatorname{Span}\{\underline{v}_i\}_{i=1}^{d_k}$ where $d_j = \dim W_j$.
   (a) Show that $G = \mathrm{GL}(V)$ acts on the space of flags.
   (b) Find the orbits of the action and find which are isomorphic G-sets. Point stabilizers are called *parabolic subgroups*.
   (c) Let F be finite (say with q elements). Find the size of each orbit.
   Hint: The set of subspaces of V containing W is in bijection with the set of subspaces of the quotient vector space V/W.
   (d) Let $B < G$ be the stabilizer of a maximal flag ("Borel subgroup"). Find the order of B, hence the order of G.

2.2. p-groups

THEOREM 72. *(Cauchy) Let G be a finite group of order divisible by the prime p. Then G has an element of order p.*

PROOF. By induction on the order of G we may assume that every proper subgroup of G has order prime to p. Now if G has a proper normal subgroup N then from $|G| = |N| \cdot |G/N|$it follows that G/N has order divisible by p. Let gN have order p in G/N. Let r be the order of g in G. Then the order of gN in G/N divides r, so $g^{\frac{r}{p}}$ has order p.

Finally, assume G is simple and has no proper subgroups of order divisible by p, and consider the action of G on itself by conjugation. Every non-central conjugacy class has size divisible by p (the index of the centralizer is divisible by p). It follows that $p \mid |Z(G)|$, and since the center is normal that by $G = Z(G)$. It follows that G is cyclic group of prime order, and we are done. □

COROLLARY 73. *Let G be a finite group, p a prime. Then every element of G has order a power of p iff the order of G is a power of p.*

DEFINITION 74. Call G a p-group if every element of G has order a power of p.

Observe that if G is a finite p-group then the index of every subgroup is a power of p. It follows that every orbit of a G-action has either size 1 or size divisible by p. By the class equation we conclude that if G is a finite p-group and X is a finite G-set, we have:

$$|X| \equiv |\{x \in X \mid \mathrm{Stab}_G(x) = G\}| \mod p. \tag{2.2.1}$$

THEOREM 75. *Let G be a finite p-group. Then $Z(G) \neq 1$.*

PROOF. Let G act on itself by conjugation. The number of conjugacy classes of size 1 must be divisible by p. □

It follows that all groups of order p^2 are abelian, and in fact isomorphic to one of C_p and $C_p \times C_p$.

2.3. Sylow Subgroups

REMARK 76. Pronounce "Silof" not "sigh-low".

DEFINITION 77. Let G be a group, p a prime number. A *Sylow p-subgroup* of G is a maximal (under inclusion) p-subgroup of G.

It is immediate from Zorn's lemma that Sylow p-subgroups exist, in fact that every p-subgroup is contained in a maximal one. If G is finite then Cauchy's Theorem 72 implies that for $p \mid |G|$ the Sylow p-subgroups are non-trivial.

THEOREM 78. *(Sylow) Let G be a finite group of order $n = p^e m$ where p is a prime, $e \geq 1$, and $(p,m) = 1$. Them:*

1. *All Sylow p-subgroups are conjugate.*
2. *Their number is a divisor of m congruent to 1 modulu p.*
3. *They all have order p^e.*

PROOF. Let $\mathcal{F}$ denote the set of Sylow p-subgroups. G acts on this set by conjugation since the definition of Sylow subgroups is a group automorphism invariant. For $P \neq Q \in \mathcal{F}$ we have $P \cap N_G(Q) = \emptyset$ (otherwise $(P \cap N_G(Q)) \ltimes Q$ would be a p-subgroup of G properly containing Q. Letting $P \in \mathcal{F}$ act on $\mathcal{F}$ be conjugation it follows that P has exactly one fixed point, P itself. By equation (2.2.1) it follows that the number of subgroups is congruent to 1 modulu p. In fact, the same applies to the orbit $\mathcal{O} = \{{}^g P\}_{g \in G}$. If there was $Q \in \mathcal{F} \setminus \mathcal{O}$ then Q would act on $\mathcal{O}$ without fixed points, implying that $|\mathcal{O}| \equiv 0\,(p)$ which is impossible. Claim (1) thus follows, and from $[G : N_G(P)] = |\mathcal{F}| \equiv 1\,(p)$ we conclude that the number of subgroups is a divisor of m (it is a divisor of G prime to p) and that $p^e \| |N_G(P)|$. Regarding claim (3), if $N_G(P)$ is a proper subgroup of G then we are done by induction so it remains to consider the case of P normal in G, in which case it suffices to show that $[G : P]$ is prime to p. Indeed, were p to divide the order of G/P then Cauchy's Theorem would give a subgroup of order p in this group. Its preimage in G would be a p-subgroup properly containing P, which is not possible. □

EXAMPLE 79. Classification of groups. Let $p < q$ be odd primes.

(1) Groups of order $2p$ are either cyclic or dihedral: there must be a unique (hence, normal) subgroup P of order p. Next, $\mathrm{Aut}(P)$ contains a unique element of order 2.
(2) Groups of order pq are either cyclic or (if $q \equiv 1\,(p)$) isomorphic to the semidirect product $\left\langle x, y \mid x^p = y^q = 1, xyx^{-1} = y^{\frac{q-1}{p}} \right\rangle$. Indeed a Sylow q-subgroup must be unique, and it has an automorphism of order p iff $p \mid q-1$.
(3) Groups of order 30 are never simple. Indeed, if the Sylow 5-subgroups are not normal there are 6 of them, contributing 24 elements of order 5. If the Sylow 3-subgroups are not normal there are 10 of them, contributing 20 elements of order 3. Since C_3 has no automorphism of order 5 and C_5 has no automorphism of order 5, it follows that in either case the 3-subgroup and 5-subgroup commute element-wise. It follows that the number of such subgroups is a divisor of 2, hence that G has a normal cyclic subgroup of order 15, on which an involution acts by an automorphism. There are 4 choices for this automorphism, giving four isomorphism classes of groups of order 30.
(4) Groups of order 36 are never simple: If there is not one Sylow 3-subgroup there are 4 of them, say $Q_1, \ldots, Q_4$. The conjugation action on this set gives a homomorphism $G \to S_4$. It is not injective and the kernel furnishes the desired subgroup.

Math 422/501: Problem set 3 (due 30/9/09)

Groups of small order

1. Let m be a positive integer. Let C_m be the cyclic group of order m. Show that $\mathrm{Aut}(C_m) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.
   Hint: Fix a generator g of C_m, and given $\varphi \in \mathrm{Aut}(C_m)$ consider $\varphi(g)$.

2. (Quals September 2008) Show that every group of order 765 is Abelian.
   Hint: To start with, let G act by conjugation on a normal Sylow p-subgroup.

3. Let G be a group of order 36 and assume that it does not have a normal Sylow 3-subgroup. Obtain a non-trivial homomorphism $G \to S_4$ and conclude that G is not simple.

Index calculations

4. Let G be a group, $H < G$ a subgroup of finite index. Show that there exists a normal subgroup $N \lhd G$ of finite index such that $N \subset H$.
   Hint: You can get inspiration from problem 3.

5. (Normal p-subgroups)
   (a) Let G be a finite group, $N \lhd G$ a normal subgroup which is a p-group. Use the conjugacy of Sylow subgroups to show that N is contained in every Sylow p-subgroup of G.
   (b) Now let G be any group, $N \lhd G$ a normal subgroup which is a p-group. Let $P < G$ be another p-subgroup. Show that PN is a p-subgroup of G and conclude that N is contained in every Sylow p-subgroup of G.

Commutators

Let G be a group. For $x, y \in G$ write $[x,y] = xyx^{-1}y^{-1}$ for the *commutator* of x, y. Write G' for the subgroup of G generated by all commutators and call it the *derived subgroup* of G.

6. (The Abelianization)
   (a) Show that $x, y \in G$ commute iff $[x,y] = e$.
   (b) Show that G' is a normal subgroup of G.
   Hint: Show that it is enough to show that the set of commutators is invariant under conjugation. Then show that $g[x,y]g^{-1}$ is a commutator.
   (c) Show that $G^{\mathrm{ab}} = G/G'$ is abelian.
   (d) Let A be an Abelian group, and let $f \in \mathrm{Hom}(G,A)$. Show that $G' \subset \mathrm{Ker}\, f$. Conclude that f can be written uniquely as the composition of the quotient map $G \twoheadrightarrow G^{\mathrm{ab}}$ and a map $f^{\mathrm{ab}} \colon G^{\mathrm{ab}} \to A$.
   OPTIONAL Let G, H be groups and let $f \in \mathrm{Hom}(G,H)$. Does f extend to a map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$?

7. (Groups of Nilpotence degree 2) Let G be group, $Z = Z(G)$ its center.
   (a) Show that the commutator $[x,y]$ only depends on the classes of x,y in $G/Z(G)$.
   From now on assume that G is non-Abelian but that $A = G/Z$ is.
   (b) Show that $G' < Z(G)$.
   Hint: 6(d).
   (c) Show that the commutator map of G descends to an anti-symmetric bi-linear pairing $[\cdot,\cdot] : A \times A \to Z(G)$.

8. Let G be a non-abelian group of order p^3.
   (a) Show that $Z(G) < G'$.
   Hint: 6(b) and general properties of p-groups.
   (b) Show that $Z(G) = G'$.
   Hint: Show that $G/Z(G)$ is abelian and use 7(b).

Optional: Example of a Sylow subgroup

A. Let k be field, V a vector space over k of dimension n. A *maximal flag* F in V is a sequence $\{0\} = F_0 \subsetneq F_1 \subseteq \cdots \subsetneq F_n = V$ of subspaces. Let $\mathcal{F}(V)$ denote the space of maximal flags in V.
   (a) Show that the group $\mathrm{GL}(V)$ of all invertible k-linear maps $V \to V$ acts transitively on $\mathcal{F}(V)$.
   (b) Let $F \in \mathcal{F}(V)$ and let $B < \mathrm{GL}(V)$ be its stabilizer. Let $N = \left\{ b \in B \mid \forall j \geq 1 \forall \underline{v} \in F_j : b\underline{v} - \underline{v} \in F_{j-1} \right\}$. Show that N is a normal subgroup of B.
   (c) Show that $B/N \simeq (k^\times)^n$.

B. Assume $|k| = q = p^r$ for a prime p. Let $V = k^n$, Let $G = \mathrm{GL}(V) = \mathrm{GL}_n(F)$, and let $B \subset G$ be the point stabilizer of the *standard flag* $V_k = \mathrm{Span}\left\{\underline{e}_j\right\}_{j=1}^k$ where $\underline{e}_j$ is the jth vector of the standard basis.
   (a) What is $|\mathcal{F}(F^n)|$?
   Hint: For each one-dimensional subspace $W \subset V$ show that the set flags containing W is in bijection with the set flags $\mathcal{F}(V/W)$.
   (b) Show that q is relatively prime to $|\mathcal{F}(V)|$. Conclude that B contains a Sylow p-subgroup of G.
   (c) Show that N is a Sylow p-subgroup of G.

Optional: Infinite Sylow Theory

C. Let G be any group, $P < G$ a p-subgroup of finite index. We will show that Sylow's Theorems apply in this setting.
   (a) Show that G has a normal p-subgroup N of finite index.
   (b) Show that every Sylow p-subgroup contains N.
   (c) Deduce a version of Sylow's Theorem for G from Sylow's Theorems for G/N.

2.4. Solvable groups

- Composition Series
- Statement of Jordan-Hölder

DEFINITION 80. Call a group G *solvable* if there exist subgroups $G_0 = G \supset G_1 \supset G_2 \supset \cdots \supset G_k = \{e\}$ so that $G_{i+1} \lhd G_i$ and G_i/G_{i+1} are normal for all $0 \leq i \leq k-1$.

REMARK 81. A finite group is solvable iff its composition factors are cyclic p-groups.

EXAMPLE 82. Every finite p-group is solvable.

PROOF. The composition factors are simple p-groups. Every such group is a cyclic p-group. □

EXAMPLE 83. S_3 is solvable.

PROOF. The subgroup of elements of order 3 is Abelian and of index 2. □

LEMMA 84. *Every group of order* 12 *is solvable, hence S_4 is solvable.*

PROOF. Let G have order 12, and let $\mathcal{P}$ be its set of 2-Sylow subgroups. $|\mathcal{P}| \in \{1,3\}$ since it must be an odd divisor of 12. If $\mathcal{P}$ has a unique member then G has a normal subgroup of order 4. Otherwise the conjugation action of G on $\mathcal{P}$ gives a homomorphism $G \to S_3$. It is not injective since $|G| = 12 > 6 = |S_3|$, and therefore has a non-trivial kernel $N = \bigcap \mathcal{P}$ (the point stabilizer of each Sylow subgroup is itself since each is a maximal subgroup in our case). N is abelian (it has order 2 or $4 = 2^2$) And G/N is solvable (it either has order $6 = 2 \cdot 3$ or 3). □

PROPOSITION 85. *Every group of order p^2q is solvable.*

PROOF. Assume the Sylow p-subgroups are not normal. Then these are $\{P_1, \ldots, P_q\}$ and $q \equiv 1\,(p)$. It follows that $q - 1 \geq p$. Next, if the Sylow q-Subgroups are not normal then there are p^2 of them, and $p^2 \equiv 1\,(q)$. But then q divides one of $p-1$ and $p+1$ so $q \leq p+1$. We conclude $q = p+1$, which is only possible if $q = 3$, $p = 2$ and $|G| = 12$. □

FACT 86. *(later this week) S_n, $n \geq 5$ is not solvable.*

PROPOSITION 87. *Let G be a group, H a subgroup, N a normal subgroup.*

(1) *If G is solvable then so are H and G/N.*
(2) *If N and G/N are solvable then so is G.*

PROOF. Let $\{G_i\}_{i=0}^k$ be a series as in the definition. Set $H_i = H \cap G_i$, and let $h \in H_i$ and $g \in H_{i+1}$. Then $hgh^{-1} \in H$ and $ghg^{-1} \in G_{i+1}$ so $hgh^{-1} \in H_{i+1}$. Composing the inclusion $H_i \hookrightarrow G_i$ with the quotient map $G_i \to G_i/G_{i+1}$ gives a map $H_i \to G_i/G_{i+1}$ with kernel $H_i \cap G_{i+1} = H_{i+1}$. It follows that H_i/H_{i+1} embeds in G_i/G_{i+1} and in particular that it is commutative. Next, let $q\colon G \to G/N$ be the quotient map and set $\bar{N}_i = q(G_i) = G_iN/N$. Then $\bar{N}_0 = G/N$, $\bar{N}_k = \{e_{G/N}\}$ and since G_i normalizes G_{i+1} and N it normalizes $G_{i+1}N$, so its image $\bar{N}_i$ normalizes $\bar{N}_{i+1}$. Finally, the map $G_i \to \bar{N}_i/\bar{N}_{i+1}$ is surjective and its kernel contains G_{i+1}. It follows that $\bar{N}_i/\bar{N}_{i+1}$ is a quotient of the abelian group G_i/G_{i+1} hence abelian.

Conversely, let $N = N_0 \supset N_1 \supset \cdots \supset N_k = \{e\}$ and let $\bar{G}_0 = G/N \supset \bar{G}_1 \supset \cdots \supset \bar{G}_l = \{eN\}$ be normal series with abelian quotients in N and G/N, respectively. For $0 \leq i \leq l$ let G_i be the inverse image of $\bar{G}_i$, and for $i \leq l \leq l+k$ let $G_i = N_{i-l}$. This is a normal series and the quotients come from the two series combined. □

EXAMPLE 88. Every finite p-group is solvable.

PROOF. Let G be a finite p-group. Then $Z(G)$ is non-trivial and solvable, and $G/Z(G)$ is solvable by induction. □

2.5. Continuation (30/9/09)

- Hall π-subgroups and π'-subgroups; Hall's Theorem
- Feit-Thompson.
- Classification of FSG.
- Nilpotent groups and commutators.
- Finite groups are nilpotent iff they are direct products of p-groups.

2.6. S_n and A_n (30/9/09)

LEMMA 89. *Let $k,l \geq 0$ and let $a,b,c_1,\cdots,c_k,d_1,\cdots,d_l \in [n]$ be distinct. Then*

$$\begin{aligned}(ab)(ac_1\cdots c_k bd_1\cdots d_k) &= (ac_1\cdots c_k)(bd_1\cdots d_k)\\ (a,b)(ac_1\cdots c_k)(bd_1\cdots d_k) &= (ac_1\cdots c_k bd_1\cdots d_k)\,.\end{aligned}$$

COROLLARY 90. *S_n is generated by the transpositions.*

PROOF. The Lemma shows that every cycle is a product of a transposition and shorter cycles. Moreover, every element of S_n is a product of cycles. □

DEFINITION 91. For $\sigma \in S_n$ write $\operatorname{sgn}(\sigma) = (-1)^{n-t}$ where t is the number of cycles in the decomposition of σ (including fixed points!).

EXAMPLE 92. If β is a cycle of length l then $\operatorname{sgn}(\beta) = (-1)^{l-1}$. Indeed, β has $n-l$ fixed points.

LEMMA 93. *Let $a \neq b$. Then* $\operatorname{sgn}((ab)\sigma) = -\operatorname{sgn}(\sigma)$.

PROOF. Let $\sigma = \prod_{j=1}^{t} \beta_j$ be the cycle decomposition of σ, where we may assume $a \in \operatorname{supp}(\beta_1)$ without loss of generality. If $b \in \operatorname{supp}(\beta_1)$ as well then $(ab)\sigma$ is the product of $t+1$ disjoint cycles by the first part of Lemma 89. Otherwise, we may assume $b \in \operatorname{supp}(\beta_2)$. Then $(ab)\sigma$ is the product of $t-1$ cycles by the second part of the Lemma. □

PROPOSITION 94. $\forall \alpha,\beta \in S_n : \operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$.

PROOF. Let $T = \{\alpha \in S_n \mid \forall \beta \in S_n : \operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)\}$. By Lemma 93 T contains all transpositions. T is also closed under multiplication: if $\alpha,\alpha' \in T$ and $\beta \in S_n$ then:

$$\begin{aligned}\operatorname{sgn}\big((\alpha\alpha')\beta\big) &= \operatorname{sgn}\big(\alpha(\alpha'\beta)\big) && \text{(associativity)}\\ &= \operatorname{sgn}(\alpha)\operatorname{sgn}(\alpha'\beta) && \alpha \in T\\ &= \operatorname{sgn}(\alpha)\operatorname{sgn}(\alpha')\operatorname{sgn}(\beta) && \alpha' \in T\\ &= \operatorname{sgn}(\alpha\alpha')\operatorname{sgn}(\beta) && \alpha \in T\,.\end{aligned}$$

That $T = S_n$ now follows from Corollary 90. □

DEFINITION 95. $A_n = \operatorname{Ker}(\operatorname{sgn})$. It is a normal subgroup of S_n of index 2.

LEMMA 96. *(Generation and conjugacy in A_n) Let $n \geq 5$.*

(1) *All cycles of length* 3 *are conjugate in* A_n..
(2) *All elements which are a product of two disjoint transpositions are conjugate in* A_n.

THEOREM 97. *A_n is simple if $n \geq 5$.*

PROOF. Let $N \lhd A_n$ be normal and non-trivial and let $\sigma \in N \setminus \{\mathrm{id}\}$ have a maximal number of fixed points. Assume σ moves at least $1,2,3,4,5$ with $\sigma(1) = 2$, $\sigma(2) = 3$ and let $\gamma = (345)\sigma(345)^{-1}\sigma^{-1} \in N$. Then γ fixes every point that σ does, and also $\gamma(2) = 2$ but $\gamma(3) = 4$, a contradiction. Thus either γ is a product of disjoint transpositions or $\gamma = (123)$. In the first case another conjugation trick also gives $(123) \in N$. We are now done by the Lemma. □

2.7. Omitted

Characteristic subgroups, minimal normal subgroups and the socle, characteristically simple groups.

Every solvable group has a normal abelian subgroup.

Math 422/501: Problem set 4 (due 7/10/09)

Solvable groups

1. Show the following are equivalent:
   (a) Every finite group of odd order is solvable.
   (b) Every non-abelian finite simple group is of even order.
   Aside: That (a) holds is a famous Theorem of Feit and Thompson (1963).

2. Let F be a field. Let $G = \mathrm{GL}_n(F)$, let $B < G$ be the subgroup of upper-triangular matrices, $N < B$ the subgroup of matrices with 1s on the diagonal. Next, for $0 \leq j \leq n-1$ write N_j for the matrices with 1s on the main diagonal and 0s on the next j diagonals. When $n = 4$ we have:
   $$N = N_0 = \left\{ \begin{pmatrix} 1 & * & * & * \\ & 1 & * & * \\ & & 1 & * \\ & & & 1 \end{pmatrix} \right\}, N_1 = \left\{ \begin{pmatrix} 1 & 0 & * & * \\ & 1 & 0 & * \\ & & 1 & 0 \\ & & & 1 \end{pmatrix} \right\}, N_2 = \left\{ \begin{pmatrix} 1 & 0 & 0 & * \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix} \right\} \text{ etc}$$
   .
   (a) Show that $N \lhd B$ and that $B/N \simeq (F^\times)^n$ (direct product of n copies).
   (b) For each $0 \leq j < n-1$, $N_{j+1} \lhd N_j$ and $N_j/N_{j+1} \simeq F^{n-j-1}$ (direct products of copies of the additive group of F).
   (c) Conclude that B is solvable.

DEFINITION. Let G be a group. The *derived series* of G is the sequence of subgroups defined by $G^{(0)} = G$ and $G^{(i+1)} = \left(G^{(i)}\right)'$ (commutator subgroups).

3. Let G be a group and assume $G^{(k)} = \{e\}$. Show that G is solvable.

4. Let G be a solvable group, say with normal series $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_k = \{e\}$. Show that $G^{(i)} < G_i$ for all i. Conclude that G is solvable iff the derived series terminates.

OPTIONAL Let $S_\infty \subset S_{\mathbb{N}}$ denote the set of permutations of *finite support*.
   (a) Show that $S_\infty = \bigcup_n S_n$ with respect to the natural inclusion of $S_n = S_{[n]}$ in S_∞.
   (b) Let $A_\infty = \bigcup_n A_n$ with respect to the same inclusion. Show that A_∞ is a subgroup of S_∞ of index 2.
   (c) Show that A_∞ is simple.

CHAPTER 3

Fields and Field extensions

3.1. Rings of Polynomials (5/10/09)

DEFINITION 98. Let R be a ring. A *formal power series over R in the variable x* is a formal sum

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

with $a_i \in R$, that is a function $a\colon \mathbb{Z}_{\geq 0} \to R$. We write $R[[x]]$ for the set of these formal power series. For $f, g \in R[[x]]$ for the form $f = \sum_{i\geq 0} a_i x^i$, $g = \sum_{j\geq 0} b_j x^j$ and $r \in R$. We make the following definitions:

$$\begin{aligned} f+g &\stackrel{\text{def}}{=} \sum_{i\geq 0} (a_i + b_i) x^i; \\ f\cdot g &\stackrel{\text{def}}{=} \sum_{k\geq 0} \left(\sum_{i+j=k} a_i b_j \right) x^k; \\ \alpha \cdot f &\stackrel{\text{def}}{=} \sum_{i\geq 0} (\alpha a_i) x^i. \end{aligned}$$

PROPOSITION 99. *These definitions give $R[[x]]$ the structure of a commutative R-algebra. $R[[x]]$ is an integral domain iff R is. Note that the additive group of $R[[x]]$ is isomorphic to the countable direct product of copies of the additive group of R.*

LEMMA 100. *The subset $R[x] \subset R[[x]]$ of formal power series with finitely many non-zero coefficients is a subalgebra. The subset of polynomials of the form rx^0, $r \in R$, is a further subalgebra isomorphic to R and we identify the two.*

DEFINITION 101. $R[x]$ is called the *ring of polynomials over R in the variable x*. For a non-zero $f \in R[x]$ set $\deg(f) = \max\{i \mid a_i \neq 0\}$ and call it the *degree* of f, call $a_{\deg(f)}$ the *leading coefficient*, and call f *monic* if $a_{\deg(f)} = 1$ (we also set $\deg(0) = -\infty$).

From now on assume that the ring R is a field F.

LEMMA 102. *(Degree valuation) Let $f, g \in F[x]$. Then $\deg(fg) = \deg(f) + \deg(g)$ and $\deg(f+g) \leq \max\{\deg f, \deg g\}$, with equality if $\deg f \neq \deg g$.*

COROLLARY 103. *Let $f, g \in F[x]$. Then*

(1) *(zero-divisors) $fg = 0$ only if one of f, g is zero.*
(2) *(units) $fg = 1$ only if $\deg f = \deg g = 0$ and $fg = 1$ in R.*

THEOREM 104. *(Division with remainder) Let $f, g \in F[x]$ with $f \neq 0$. Then there exists unique $q, r \in F[x]$ with $\deg r < \deg f$ so that*

$$g = qf + r.$$

COROLLARY 105. *$F[x]$ is a principal ideal domain. An ideal $I \lhd F[x]$ is prime iff it is maximal, iff $I = (f)$ with f irreducible.*

3.1.1. Divisors, GCD, LCM and unique factorization.

DEFINITION 106. $f, g, h \in F[x]$.

- Say that f *divides* g, or that g is a *multiple* of f is there exists h such that $fh = g$.
- Say that f is *irreducible* if whenever $f = gh$ one of g, h is a unit, reducible if $f = gh$ for some g, h both of degree at least 1.
- Say that f is *prime* if whenever $f|gh$ we have either $f|g$ or $f|h$ (or both).
- If $f, g \in F[x]$ and $f = \alpha g$ for $\alpha \in F^\times$ we say that f, g are *associate*. This is an equivalence relation, and every equivalence class has a unique monic member.

DEFINITION 107. Let $f, g \in F[x]$. A *greatest common divisor* of f, g is the monic polynomial h of maximal degree which divides both of them.

THEOREM 108. *Let f, g be polynomials. Then the Euclidean algorithm will compute a GCD, which can be written in the form $hf + kg$ for some $h, k \in F[x]$.*

PROPOSITION 109. *Every polynomial can be written as a product of irreducibles. A polynomial is irreducible iff it is prime. Every polynomial has a unique factorization into primes (up to associates).*

3.1.2. Irreducibility in $\mathbb{Q}[x]$.

THEOREM 110. *(Gauss) Let $f \in \mathbb{Z}[x]$. Be irreducible. Then f is irreducible in $\mathbb{Q}[x]$ as well.*

PROOF. Assume that f is reducible in $\mathbb{Q}[x]$, and let $a \in \mathbb{Z}_{\geq 1}$ be minimal such that

$$af = gh$$

For $g, h \in \mathbb{Z}[x]$ for degree at least 1 (that a exists follows from clearing denominators). If $a = 1$ we are done, so let p be a prime divisor of a. Letting bar denotes reductions mod p we have:

$$\bar{0} = \bar{g}\bar{h} \text{ in } (\mathbb{Z}/p\mathbb{Z})[x].$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, we have without loss of generality that $\bar{g} = \bar{0}$, in other words that every coefficient of g is divisible by p. It then follows that

$$\frac{a}{p} f = \frac{g}{p} h \text{ in } \mathbb{Z}[x],$$

a contradiction to the minimality of a. □

THEOREM 111. *(Eisenstein) Let $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ and let p be a prime such that: $p \nmid a_n$, $p|a_i$ for $0 \leq i \leq n-1$ but $p^2 \nmid a_0$. Then f is irreducible in $\mathbb{Q}[x]$.*

PROOF. Assume that $f = gh$. Say that $\deg(g) = r$, $\deg(h) = s$ with leading coefficients b_r and c_s, respectively. Then $r + s = n$ and $b_r c_s = a_n$. In particularly, both b_r and c_s are prime to p. Reducing modulu p we find $\bar{a}_n x^n = \bar{g}\bar{h}$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. It follows that $\bar{g} = \bar{b}_r x^r$ and $\bar{h} = \bar{c}_s x^s$. Assuming $\deg(g), \deg(h) \geq 1$ this means that the constant coefficients of g, h are both divisible by p, which would make the constant coefficient of f divisible by p^2. Otherwise one of g, h is an integer, so f, g are associates in $\mathbb{Q}[x]$. □

EXAMPLE 112. The cyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = \sum_{j=0}^{p-1} x^j$ is irreducible.

PROOF. The map $x \mapsto y+1$ and $y \mapsto x+1$ are isomorphisms of $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$. It follows that it is enough to consider the irreducibility of $\Phi_p(y+1) = \frac{(y+1)^p-1}{y} = y^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} y^{j-1}$. Since $p|\binom{p}{j}$ for $1 \leq j \leq p-1$ and $\binom{p}{1} = p$ is not divisible by p^2 we are done. $\square$

Math 422/501: Problem set 5 (due 14/10/09)

Ideals in Rings

Let R be a ring. Recall that an *ideal* $I \lhd R$ is an additive subgroup $I \subset R$ so that $rI \subset I$ for all $r \in R$.

1. (Working with ideals)
   (a) Let $\mathcal{I}$ be a set of ideals in R. Show that $\bigcap \mathcal{I}$ is an ideal.
   (b) Given a non-empty $S \subset R$ show that $(S) \stackrel{\text{def}}{=} \bigcap \{I \mid S \subset I \lhd R\}$ is the smallest ideal of R containing S.
   (c) Show that $(S) = \{\sum_{i=1}^{n} r_i s_i \mid n \geq 0, r_i \in R, s_i \in S\}$.
   (d) Let $a \in R^{\times}$. Show that a is not contained in any proper ideal.
   Hint: Show that $a \in I$ implies $1 \in I$.

2. (Prime and maximal ideals) Call $I \lhd R$ *prime* if whenever $a, b \in R$ satisfy $ab \in I$, we have $a \in I$ or $b \in I$. Call I *maximal* if it is not contained in any proper ideal of R.
   (a) Show that R is an integral domain iff $(0) = \{0\} \lhd R$ is prime.
   (b) Show that $I \lhd R$ is prime iff R/I is an integral domain.
   (c) Show that R is a field iff (0) is its unique ideal (equivalently, a maximal ideal).
   (d) Use the correspondence theorem to show that I is maximal iff R/I is a field.
   (e) Show that every maximal ideal is prime.
   Hint: Every field is an integral domain.

3. (Polynomials and maps of fields) Let $\varphi\colon F \to K$ be a map of fields, and let $\alpha \in K$.
   (a) Show that φ is injective.
   Hint: consider the kernel of the map.
   (b) Show that there is a unique homomorphism of rings ("evaluation at α") $\tilde{\varphi}_\alpha\colon F[x] \to K$ compatible with the embeddings $F \hookrightarrow F[x]$ and $F \to K$ so that $\tilde{\varphi}_\alpha(x) = \alpha$. For $f \in F[x]$ we usually write $f(\alpha)$ for $\tilde{\varphi}_\alpha(f)$.
   Hint: Write $\tilde{\varphi}_\alpha$ as the composition of a map $F[x] \to K[x]$ and a map $K[x] \to K$.
   (c) Show that $\tilde{\varphi}_\alpha$ is not injective iff there exists $f \in F[x]$ (or $f \in K[x]$ with coefficients in the image of φ) so that $f(\alpha) = 0$.
   OPTIONAL If $\tilde{\varphi}$ is not injective, show that its kernel is of the form (f) for an irreducible polynomial $f \in F[x]$ and its image is a subfield of K.

4. (The field of rational functions) Let F be a field.
   (a) For $f, g, h, k \in F[x]$ with $g, k \neq 0$ say $\frac{f}{g} \sim \frac{h}{k}$ if $fk = gh$. Show that $\sim$ is an equivalence relation.
   (b) Show that $F(x) = \left\{ \frac{f}{g} \mid f, g \in F[x], g \neq 0 \right\} / \sim$ is a field, and that the natural map $\iota\colon F[x] \to F(x)$ given by $f \mapsto \frac{f}{1}$ is an embedding.
   (c) $\varphi\colon F \to K$ be an embedding of fields, and let $\alpha \in K$. Assume that $f(\alpha) \neq 0$ for all non-zero $f \in F[x]$, and show that φ extends uniquely to a map $\tilde{\varphi}_\alpha\colon F(x) \to K$ so that $\tilde{\varphi}_\alpha(x) = \alpha$.

DEFINITION. Call $\alpha \in K$ *algebraic over* F if the situation of 3(c) holds, *transcendental over* F if the situation of 4(c) holds.

Irreducible polynomials and zeroes

5. Let $f \in \mathbb{Z}[x]$ be non-zero and let $\frac{a}{b} \in \mathbb{Q}$ be a zero of f with $(a,b) = 1$. Show that constant coefficient of f is divisible by a and that the leading coefficient is divisible by b. Conclude that if f is monic then any rational zero of f is in fact an integer.

6. Decide while the following polynomials are irreducible:
   (a) $t^4 + 1$ over $\mathbb{R}$.
   (b) $t^4 + 1$ over $\mathbb{Q}$.
   (c) $t^3 - 7t^2 + 3t + 3$ over $\mathbb{Q}$.

7. Show that $t^4 + 15t^3 + 7$ is reducible in $\mathbb{Z}/3\mathbb{Z}$ but irreducible in $\mathbb{Z}/5\mathbb{Z}$. Conclude that it is irreducible in $\mathbb{Q}[x]$.

8. Let $\mathbb{R}$ be the field of real numbers. Let $\mathbb{C} = \{a + bi \mid a,b \in \mathbb{R}\}$ where i is a formal symbol, and define $(a+bi)+(c+di) \stackrel{\text{def}}{=} (a+b)+(c+d)i$, $(a+bi)(c+di) \stackrel{\text{def}}{=} (ac-bd)+(ad+bc)i$.
   (a) Show that the definition makes $\mathbb{C}$ into a ring.
   (b) Show that $\{a+0i \mid a \in \mathbb{R}\}$ is a subfield of $\mathbb{C}$ isomorphic to $\mathbb{R}$.
   (c) Show that the *complex conjugation* map $\tau(a+bi) = a-bi$ is a ring isomorphism $\tau\colon \mathbb{C} \to \mathbb{C}$ which restricts to the identity map on the image of $\mathbb{R}$ from part (b).
   (d) Show that for $z \in \mathbb{C}$ the condition $z \in \mathbb{R}$ and $\tau z = z$ are equivalent. Conclude that $Nz = N_{\mathbb{R}}^{\mathbb{C}} z \stackrel{\text{def}}{=} z \cdot \tau z$ is a multiplicative map $\mathbb{C} \to \mathbb{R}$.
   (e) Show that $\mathbb{C}$ is a field.
   Hint: Show first that if $z \in \mathbb{C}$ is non-zero then Nz is non-zero.

9. (Quadratic equations in $\mathbb{C}$).
   (a) Let $d \in \mathbb{C}$. Show that there exist $z \in \mathbb{C}$ such that $z^2 = d$.
   (b) Let $a,b,c \in \mathbb{C}$ with $a \neq 0$, and let $d = b^2 - 4ac$. Show that the equation $az^2 + bz + c = 0$ has two solutions in $\mathbb{C}$ when $d \neq 0$, and one solution when $d = 0$.

Optional - A split $\mathbb{R}$-algebra

8'. Let $\mathbb{R}$ be the field of real numbers. Let $A = \{a + bi \mid a,b \in \mathbb{R}\}$ where i is a formal symbol, and define $(a+bi)+(c+di) \stackrel{\text{def}}{=} (a+b)+(c+d)i$, $(a+bi)(c+di) \stackrel{\text{def}}{=} (ac+2bd)+(ad+bc)i$.
   (a) Show that the definition makes A into a ring.
   (b) Show that $\{a+0i \mid a \in \mathbb{R}\}$ is a subfield of A isomorphic to $\mathbb{R}$.
   (c) Show that the *complex conjugation* map $\tau(a+bi) = a-bi$ is a ring isomorphism $\tau\colon A \to A$ which restricts to the identity map on the image of $\mathbb{R}$ from part (b).
   (d) Show that for $z \in A$ the condition $z \in \mathbb{R}$ and $\tau z = z$ are equivalent. Conclude that $Nz = N_{\mathbb{R}}^{A} z \stackrel{\text{def}}{=} z \cdot \tau z$ is a multiplicative map $A \to \mathbb{R}$.
   (e) Show that $A \simeq \mathbb{R} \oplus \mathbb{R}$, and in particular that it is not a field.
   (f) Assume that multiplication is defined by $(a+bi)(c+di) \stackrel{\text{def}}{=} (ac+tbd)+(ad+bc)i$ for some fixed $t \in \mathbb{R}$. For which t is the algebra a field? Find the isomorphism class of the algebra, depending on t.

Optional - The field of Laurent series

DEFINITION. Let R be a ring. A *formal Laurent series* over R is a formal sum $f(x) = \sum_{i \geq i_0} a_i x^i$, in other words a function $a\colon \mathbb{Z} \to R$ for which there exists $i_0 \in \mathbb{Z}$ so that $a_i = 0$ for all $i \leq i_0$. We define addition and multiplication in the obvious way and write $R((x))$ for the set of Laurent series. For non-zero $f \in R((x))$ let $v(f) = \min\{i \mid a_i \neq 0\}$ ("order of vanishing at 0"; also set $v(0) = \infty$). Then set $|f| = q^{-v(f)}$ ($|0| = 0$) where $q > 1$ is a fixed real number.

A. Show that $R((x))$ is a ring, and that $R[[x]]$ is a subring.

B. (Invertibility)
   (a) Show that $1 - x$ is invertible in $R[[x]]$.
   Hint: Find a candidate series for $\frac{1}{1-x}$ and calculate the product.
   (b) Show that $R[[x]]^\times = \{a + xf \mid a \in R^\times,\ f \in R[[x]]\}$.
   (c) Show that $f \in R((x))$ is invertible iff it is non-zero and $a_{v(f)} \in R^\times$.
   (d) Show that $F((x))$ is a field for any field F.

C. (Locality) Let F be a field.
   (a) Let $I \lhd F[[x]]$ be a non-zero ideal. Show that $I = x^n F[[x]]$ for some $n \geq 1$.
   Hint: Show that $f \in F[[x]]$ can be written in the form $x^{v(f)} g(x)$ where $g \in F[[x]]^\times$.
   (b) Show that the natural map $F[x]/x^n F[x] \to F[[x]]/x^n F[[x]]$ is an isomorphism.

D. (Completeness)
   (a) Show that $v(fg) = v(f) + v(g)$, equivalently that $|fg| = |f|\,|g|$ for all $f, g \in R((x))$.
   (b) Prove the *ultrametric inequality* $v(f+g) \geq \min\{v(f), v(g)\} \iff |f+g| \leq \max\{|f|, |g|\}$ and conclude that $d(f,g) = |f-g|$ defines a metric on f.
   (c) Show that $\{f_n\}_{n=1}^\infty \subset R((x))$ is a Cauchy sequence iff there exists i_0 such that $v(f_n) \geq i_0$ for all n, and if for each i there exists $N = N(i)$ and $r \in R$ so that for $n \geq N$ the coefficient of x^i in f_n is r.
   (d) Show that $(R((x)), d)$ is complete metric space.
   (e) Show that $R[[x]]$ is closed in $R((x))$.
   (f) Show that $R[[x]]$ is compact iff R is finite.

E. (Ultrametric Analysis) Let $\{a_n\}_{n=1}^\infty \subset R((x))$. Show that $\sum_{n=1}^\infty a_n$ converges in $R((x))$ iff $\lim_{n\to\infty} a_n = 0$.
   Hint: Assume first that $a_n \in R[[x]]$ for all n, and for each k consider the projection of $\sum_{n=1}^N a_n$ to $R[[x]]/x^k R[[x]]$.

F. (The degree valuation) Let F be a field.
   (a) For $f \in F[x]$ set $v_\infty(f) = -\deg(f)$ (and set $v_\infty(0) = \infty$). Show that $v_\infty(fg) = v_\infty(f) + v_\infty(g)$. Show that $v_\infty(f+g) \geq \min\{v_\infty(f), v_\infty(g)\}$.
   (b) Extend v_∞ to the field $F(x)$ of rational functions and show that it retains the properties above. For a rational function f you can think of $v_\infty(f)$ as "the order of f at ∞", just like $v(f)$ measures the order of f at zero.
   (c) Show that the completion of $F(x)$ w.r.t. the metric coming from v_∞ is exactly $R((\frac{1}{x}))$.

3.2. Field extensions

DEFINITION 113. A *field extension* is a homomorphism of fields.If $\iota\colon K \to L$ is an inclusion one may identify K with $\iota(K)$. In that case write $L : K$.

If K is a subfield of L and $S \subset L$ we write $K(S)$ for the intersection of all subfields of L containing K and S.

Say $\iota : K \to L$ and $\iota'\colon K' \to L'$ are *isomorphic* if there exist isomorphisms $\lambda\colon K \to K'$ and $\eta : L \to L'$ intertwining the two.

EXAMPLE 114. $\mathbb{Q}(i)$. $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(i,-i,\sqrt{5},-\sqrt{5})$.

DEFINITION 115. Let $K \hookrightarrow L$ be an extension. Call $\alpha \in L$ *algebraic over* K if there exists $p \in K[x]$ such that $p(\alpha) = 0$, *transcendental* otherwise. Call $K \hookrightarrow L$ *algebraic* if every $\alpha \in L$ is algebraic over K.

LEMMA 116. *Let $\alpha \in L$ be transcendental over K. Then $K(\alpha) \simeq K(t)$ via the map $\frac{f(t)}{g(t)} \mapsto \frac{f(\alpha)}{g(\alpha)}$.*

COROLLARY 117. *If α is transcendental over K then $\dim_K K(\alpha) = \infty$.*

Consider the map $\varphi\colon K[x] \to L$ given by evaluation at α. It is a ring homomorphism, and its image is an integral domain contained in $K(\alpha)$. Its kernel is a prime ideal I of $K[x]$, consisting of all polynomials in $K[x]$ which vanish at α. Since $K[x]$ is a PID it follows that $I = (m)$ for some irreducible m, and that the image of the map is a field which must then be equal to $K(\alpha)$. . We have obtained:

LEMMA 118. *Let $\alpha \in L$ be algebraic over K. Then*

1. *Every element of $K(\alpha)$ is of the form $p(\alpha)$ for some $p \in f$*
2. *There is a unique monic irreducible polynomial $m \in K[x]$ such that $m(\alpha) = 0$, called the* minimal polynomial *of α over K.*
3. *If $p \in K[x]$ satisfies $p(\alpha) = 0$ then $m|p$.*

DEFINITION 119. Call $L : K$ *simple* if $L = K(\alpha)$ for some α.

PROPOSITION 120. *Let $m \in K[x]$ be irreducible. Then there exists a simple extension $L = K(\alpha)$ with $m(\alpha) = 0$, and this extension unique up to isomorphism, which can be taken to map the images of α.*

PROOF. $K \hookrightarrow K[x]/(m)$ is such an extension, which we have already seen to be isomorphic to any such $K(\alpha)$. □

COROLLARY 121. $\dim_K K(\alpha) = \deg m$.

PROOF. The polynomials of degree less than m are mapped injectively into $K[x]/(m)$ (the difference of two of them cannot be divisible by m unless zero). They are mapped surjectively by division with remainder. □

THEOREM 122. *α is algebraic over K iff $\dim_K K(\alpha) < \infty$.*

COROLLARY 123. *Let α be algebraic over K. Then $K(\alpha)$ is algebraic over K.*

PROOF. Let $\beta \in K(\alpha)$. Then $K(\beta) \subset K(\alpha)$ so $\dim_K K(\beta) \leq \dim_K K(\alpha) < \infty$. □

DEFINITION 124. Let $K \hookrightarrow L$ be an extension of fields. Call $\dim_K L$ the *degree* of the extension and denote it $[L : K]$.

PROPOSITION 125. *(Multiplicativity) Let $K \hookrightarrow L \hookrightarrow M$. Then $[M:K] = [M:L] \cdot [L:M]$.*

PROOF. Let $\{\lambda_i\}_{i\in I}$ be a basis for L over K. Let $\{\mu_j\}_{j\in J}$ be a basis for M over L. We will see that $\{\lambda_i\mu_j\}_{(i,j)\in I\times J}$ is a basis for M over K. First, assume that $\sum_{i,j} a_{ij}\lambda_i\mu_j = 0$ with $a\colon I\times J \to K$ finitely supported. Then $\sum_j \left(\sum_i a_{ij}\lambda_i\right)\mu_j = 0$. Since the μ_j are independent over L, $\sum_i a_{ij}\lambda_i = 0$ for each j. Now get $a_{ij} = 0$ for all i, j. Next, let $m \in M$. Then there exists $b\colon J \to L$ of finite support such that $\sum_j b_j\mu_j = m$. Next, for each j there exists $a_j\colon I \to K$ of finite support such that $\sum_i a_{ij}\lambda_i = b_j$. It follows that $m = \sum_{i,j} \alpha_{ij}\lambda_i\mu_j$. □

COROLLARY 126. *Let $\alpha, \beta \in L$ be algebraic over K. Then so are $\alpha+\beta$, $-\alpha$, $\alpha\beta$, and α^{-1}.*

PROOF. β is algebraic over K, hence over $K(\alpha)$, and $[K(\alpha,\beta):K] = [K(\alpha,\beta):K(\alpha)][K(\alpha):K] < \infty$. □

DEFINITION 127. Let $K \hookrightarrow L$. The *algebraic closure of K in L* is the set $\{\alpha \in L \mid [K(\alpha):K] < \infty\}$. It is a subfield of L containing every algebraic extension of K contained in L

The algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ is called the field of *algebraic numbers*.

Math 422/501: Problem set 6 (due 21/10/09)

$\mathbb{Q}(\sqrt[3]{2})$

1. Let $K = \mathbb{Q}(\alpha)$ where $\alpha^3 = 2$. By Eisenstein's criterion ($p = 2$), $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible. Without using the tools from abstract algebra:
   (a) Show by hand that $\{1, \alpha, \alpha^2\} \subset K$ is linearly independent over $\mathbb{Q}$.
   Hint: You may use the irreducibility of $x^3 - 2$.
   (b) Show by hand that $\{1, \alpha, \alpha^2\}$ is a basis for K.
   Hint: It is enough to show that $\{a + b\alpha + c\alpha^2\} \subset K$ is closed under addition and multiplication, and that each element has an inverse.
   – Conclude that $[K : \mathbb{Q}] = 3$.

2. (The hard way) Let $\beta \in K$ satisfy $\beta^3 = 2$.
   (a) Write $\beta = a + b\alpha + c\alpha^2$, and convert the equation $\beta^3 = 2 = 2 + 0\alpha + 0\alpha^2$ to a system of three non-linear equations in the three variables a, b, c.
   Hint: You need to use the fact that $\{1, \alpha, \alpha^2\}$ is a basis at some point.
   (b) Taking a clever linear combination of two of the equations, show that $a = 0$.
   (c) Now show that $b = 1$, $c = 0$, that is that $\beta = \alpha$.

3. (The easy way) Let $\beta \in K$ satisfy $\beta^3 = 2$ and assume that $\beta \neq \alpha$.
   (a) Let $\gamma = \beta/\alpha$ and show that $\gamma^3 = 1$.
   (b) Let $m(x) \in \mathbb{Q}[x]$ be the minimal polynomial of γ over $\mathbb{Q}$. Show that $\deg m = 2$.
   Hint: Start by showing that m is an irreducible factor of $x^3 - 1$.
   (c) Consider the field $\mathbb{Q}(\gamma) \subset K$. Show that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2$ and obtain a contradiction.
   Hint: $[K : \mathbb{Q}] = [K : \mathbb{Q}(\gamma)] \cdot [\mathbb{Q}(\gamma) : \mathbb{Q}]$.

Prime fields and the characteristic

4. Let K be a field.
   (a) Show that there is a unique ring homomorphism $\varphi\colon \mathbb{Z} \to K$.
   (b) Let $p \geq 0$ be such that $\mathrm{Ker}(\varphi) = (p)$. Show that either $p = 0$ or p is prime.

   DEFINITION. We call p the *characteristic* of K.

   (c) Let K be a field of characteristic $p > 0$. Show that the image of φ is the intersection of all subfields of K, and that it isomorphic to the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
   (d) Let K be a field of characteristic zero. Show that there is a unique homomorphism $\mathbb{Q} \hookrightarrow K$ and conclude that the minimal subfield of K is isomorphic to $\mathbb{Q}$.

5. (Finite fields)
   (a) Let K be a finite field. Show that there exists a prime p and a natural number n so $|K| = p^n$.
   (b) Show that there exists a field of order 4.
   Hint: Construct an irreducible quadratic polynomial in $\mathbb{F}_2[x]$.
   (c) Show that there is a unique field of order 4.

REMARK. We will see that for each prime power there is a field of that order, unique up to isomorphism.

Quadratic fields

Let K be a field of characteristic not equal to 2. Write $K^\times$ for the multiplicative group of K, $(K^\times)^2$ for its subgroup of squares.

6. (Reduction to squares) Let $L : K$ be an extension of degree 2.
   (a) Show that there exists $\alpha \in L$ such that $K(\alpha) = L$. What is the degree of the minimal polynomial of α?
   (b) Show that there exist $d \in K^\times$ such that $L : K$ is isomorphic to $K(\sqrt{d}) : K$.
   Hint: Complete the square.

7. (Classifying the extensions)
   (a) Assume that $d \in K^\times$ is not a square. Using the representation $K(\sqrt{d}) = \left\{ a + b\sqrt{d} \mid a, b \in K \right\}$ show that $e \in K$ is a square in $K(\sqrt{d})$ iff $e = df^2$ for some $f \in K$. Where did you use the assumption about the characteristic?
   (b) Show that the extensions $K(\sqrt{d})$ and $K(\sqrt{e})$ are isomorphic iff $\frac{d}{e} \in (K^\times)^2$ (in general, the isomorphism will not send $\sqrt{d}$ to $\sqrt{e}$).
   Hint: Construct a K-homomorphism $K(\sqrt{e}) \to K(\sqrt{d})$. Why is it surjective? Injective?
   (c) Show that quadratic extensions of K are in bijection with non-trivial elements of the group $K^\times / (K^\times)^2$.

8. (Applications)
   (a) Show that $\mathbb{R}$ has a unique quadratic extension.
   (b) Show that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
   Hint: Show that $\sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ but that $\sqrt{2} + \sqrt{3} \neq a + b\sqrt{6}$ for any $a, b \in \mathbb{Q}$.

Simple extensions

9. Let $K(\alpha) : K$ be a simple extension.
   (a) If α is algebraic, show that there are finitely many subfields L of $K(\alpha)$ containing K.
   Hint: consider the minimal polynomial of α over L.
   (b) If α is transcendental, show that there are infinitely many intermediate fields L.

10. Let $L : K$ be an extension of fields with finitely many intermediate subfields.
    (a) Show that the extension is algebraic.
    (b) Show that the extension is *finitely generated*: there exists a finite subset $S \subset L$ so that $L = K(S)$.
    (c) Show that $L : K$ is finite.

11. Let $L : K$ be an extension of infinite fields with finitely many intermediate fields.
    (a) Given $\alpha, \beta \in L$ find $\gamma \in L$ so that $K(\alpha, \beta) = K(\gamma)$.
    Hint: Consider elements of the form $\gamma = \alpha + k\beta$ where $k \in K$.
    (b) Show that $L : K$ is a simple algebraic extension.

Algebraicity

12. Let $M : L$ and $L : K$ be algebraic extensions of fields. Show that $M : K$ is algebraic.

3.3. Straightedge and compass

Math 422/501: Problem set 7 (due 28/10/09) [extended till 30/10/09]

Splitting fields and normal closures

1. Construct subfields of $\mathbb{C}$ which are splitting fields over $\mathbb{Q}$ for the following polynomials:
   (a) $t^3 - 1$;
   (b) $t^4 + 5t^2 + 6$;
   (c) $t^4 + 7t^2 + 6$;
   (d) $t^6 - 8$.
   Find the degrees of the splitting fields as extensions of $\mathbb{Q}$.

2. Construct a splitting field for the following polynomials over $\mathbb{F}_3$:
   (a) $t^3 + 2t + 1$;
   (b) $t^3 + t^2 + t + 2$.
   (c) Are the two fields isomorphic?

3. Let $f \in K[x]$ and let $\Sigma : K$ be a splitting field for f over K. Let $K \subset M \subset \Sigma$ be an intermediate field. Show that Σ is a splitting field for f over M.

4. Let $f \in K[x]$ have degree n and let $\Sigma : K$ be a splitting field for f over K. Show that $[\Sigma : K] \leq n!$.

Algebraic closures

DEFINITION. A field extension $K \hookrightarrow \bar{K}$ is called an *algebraic closure* if it is algebraic, and if polynomial in $K[x]$ splits in $\bar{K}[x]$. We also say informally that $\bar{K}$ is an *algebraic closure of* K.

5. Let $K \hookrightarrow L$ be an algebraic extension.
   (a) If K is finite, show that $|L| \leq \aleph_0$.
   (b) If K is infinite, show that $|L| = |K|$.

6. Let $K \hookrightarrow \bar{K}$ be an algebraic closure. Show that every algebraic extension of $\bar{K}$ is isomorphic to $\bar{K}$.

7. (Existence of algebraic closures) Let K be a field, X an infinite set containing K with $|X| > |K|$. Let $0, 1$ denote these elements of $K \subset X$. Let

   $$\mathcal{F} = \{(L, +, \cdot) \mid K \subset L \subset X, (L, 0, 1, +, \cdot) \text{ is a field with } K \subset L \text{ an algebraic extension}\} .$$

   Note that we are assuming that restricting $+, \cdot$ to K gives the field operations of K.

   (OPT) Show that $\mathcal{F}$ is a set. Note that $\{(\varphi, L) \mid L \text{ is a field and } \varphi \colon K \to L \text{ is an algebraic extension}\}$ is not a set.
   (a) Show that every algebraic extension of K is isomorphic to an element of $\mathcal{F}$.
   (b) Given $(L, +, \cdot)$ and $(L', +', \cdot') \in \mathcal{F}$ say that $(L, +, \cdot) \leq (L', +', \cdot')$ if $L \subseteq L'$, $+ \subseteq +'$, $\cdot \subseteq \cdot'$. Show that this is a transitive relation.
   (c) Let $\bar{K} \in \mathcal{F}$ be maximal with respect to this order. Show that $\bar{K}$ is an algebraic closure of K.
   (d) Show that K has algebraic closures.

8. (Uniqueness of algebraic closures) Let $K \hookrightarrow \bar{K}$ and $K \hookrightarrow L$ be two algebraic closures of K. Show that the two extensions are isomorphic.
Hint: Let $\mathcal{G}$ be the set of K-embeddings intermediate subfields $K \subset M \subset L$ into $\bar{K}$, ordered by inclusion.

Symmetric polynomials

Let R be a ring. Then S_n acts on the polynomial ring $R[x_1,\dots,x_n]$ by permuting the variables, and we write $R[\underline{x}]^{S_n}$ for the set of fixed points.

9. (Basic structure)
   (a) Show that $R[\underline{x}]^{S_n}$ is a subring of $R[\underline{x}]$, *the ring of symmetric polynomials*.
   (b) For $\alpha \subset [n]$ write $\underline{x}^\alpha$ for the monomial $\prod_{i\in\alpha} x_i$. For $1 \le r \le n$ let
   $$s_r(\underline{x}) = \sum_{\alpha \in \binom{[n]}{r}} \underline{x}^\alpha \in R[\underline{x}]\,.$$
   Show that $s_r(\underline{x}) \in R[\underline{x}]^{S_n}$. These are called the *elementary symmetric polynomials*.

10. (Generation) Define the *height* of a monomial $\prod_{i=1}^n x_i^{\alpha_i}$ to be $\sum_{i=1}^n i\alpha_i$. Define the *height* of $p \in R[\underline{x}]$ to be the maximal height of a monomial appearing in p.
    (a) Given $p \in R[\underline{x}]^{S_n}$ find $\underline{\beta} \in \mathbb{Z}^n_{\ge 0}$ and $r \in R$ so that the highest term of $q = r\prod_{r=1}^n s_r^{\beta_r}$ occurs in p.
    (b) Show that $p - q$ either fewer highest terms than p or smaller height than p.
    (c) Show that every symmetric polynomial can be written as a polynomial of equal or smaller degree in the elementary symmetric polynomials.

Derivatives, derivations and separability

11. The *formal derivative* of the Laurent series $f = \sum_{i\ge i_0} a_i x^i \in R((x))$ over the ring R is the Laurent series $Df \stackrel{\text{def}}{=} \sum_{i\ge i_0} i a_i x^{i-1}$.
    (a) Show that $D\colon R((x)) \to R((x))$ is R-linear: that $D(\alpha f + \beta g) = \alpha Df + \beta Dg$ for $\alpha,\beta \in R$ and $f,g \in R((x))$.
    (b) Show that D is a *derivation*: that $D(fg) = Df\cdot g + f\cdot Dg$ (this is called the *Leibniz rule*).
    (c) Show that $D(f^k) = k\cdot f^{k-1}\cdot Df$ for all $k \ge 0$.
    (d) Show that if f is a polynomial then Df is a polynomial as well, that is that D restricts to a map $R[x] \to R[x]$.

12. (Derivative criterion for separability) Let K be a field.
    (a) Let $\alpha \in K$ be a zero of $f \in K[x]$. Show that $(x-\alpha)^2 | f$ iff $Df(\alpha) = 0$ iff $(x-\alpha)|Df$.
    (b) Let $\varphi\colon K \to L$ be an extension of fields, and let $f,g \in K[x]$. Let $(f,g) = (h)$ as ideals of $K[x]$, $(\varphi(f),\varphi(g)) = (h')$ as ideals of $L[x]$. Taking h,h' monic show that $h' = \varphi(h)$.
    (c) Show that $f \in K[x]$ is has no repeated roots in any extension (is *separable)* iff $(f,Df) = 1$.
    (d) Show that an irreducible $f \in K[x]$ is separable iff $Df \ne 0$.

Optional problems

A. Construct an embedding $K(x) \hookrightarrow K((x))$ and show that D restricts to a map $K(x) \to K(x)$.

For the rest fix a ring R.

B. Let A be an R-algebra, and consider the map $A \times A \to A$ given by the *commutator bracket* $[a,b] = ab - ba$, .
   (a) Show $(A, [\cdot,\cdot])$ is a *Lie algebra,* that is that the commutator is R-bi-linear and anti-symmetric, and satisfies the *Jacobi identity* $[a,[b,c]] + [b,[c,a]] + [c,[a,b]] = 0$.
   (c) Show that for a fixed $a \in A$ the map $b \mapsto [a,b]$ is an element $\mathrm{ad}(a) \in \mathrm{End}_R(A)$.
   (d) Show that $\mathrm{ad}(a)$ is a derivation: $(\mathrm{ad}(a))(bc) = [(\mathrm{ad}(a))(b)]c + b[(\mathrm{ad}(a))(c)]$.

C. Let A be an R-algebra. Let $\mathrm{Der}_R(A) = \{D \in \mathrm{End}_R(A) \mid D \text{ is a derivation}\}$.
   (a) Show that $\mathrm{Der}_R(A) \subset \mathrm{End}_R(A)$ is an R-submodule.
   (b) Give an example showing that $\mathrm{Der}_R(A)$ need not be an R-subalgebra (that is, closed under multiplication=composition).
   (c) Show that $\mathrm{Der}_R(A)$ is closed under the commutator bracket of $\mathrm{End}_R(A)$.

D. Let A an R-algebra. Show that the map $\mathrm{ad}\colon A \to \mathrm{Der}_R(A)$ is a map of Lie algebras, that is a map of R-modules respecting the brackets.

CHAPTER 4

Monomorphisms, Automorphisms and Galois Theory

4.1. Splitting fields and normal extensions

DEFINITION 128. Let $L:K$ be an extension of fields. Say $f \in K[x]$ *splits* in L if its image in $L[x]$ is a product of linear factors there. Say that L is a *splitting field* for f over K if f splits in L be not in any intermediate field $K \subset M \subsetneq L$.

THEOREM 129. *(Splitting fields)*

(1) *For every field K and $f \in K[x]$ there exists a splitting field L/K, in fact one with $[L:K] \leq (\deg(f))!$.*
(2) *Splitting fields are unique up to isomorphism of extensions: if $\kappa\colon K \to K'$ is an isomorphism of fields, $f \in K[x]$, and $\iota\colon K \to L$, $\iota'\colon K' \to L'$ are splitting fields for f and $\kappa(f)$ respectively, then there exists an isomorphism $\lambda : L \to L'$ so that (κ,λ) is an isomorphism of the extensions ι and ι'.*

PROOF. First, if $f \in K[x]$ splits in L, say $f = c\prod_i (x-\alpha_i)$, then $M = K(\{\alpha_i\})$ is a splitting field: f splits there, and any sub-extension of M where f splits contains the $\{\alpha_i\}$ hence is equal to M. It is thus enough to construct an extension where f splits (with the given bound of the degree). We prove this by induction on the degree of f. If $\deg(f) \leq 1$ there's nothing to prove. Otherwise let g be an irreducible factor of f and let $M = K(\alpha)$ where α is a root of g. By induction $\frac{f}{x-\alpha} \in M[x]$ has a splitting field. It is clear that f splits there as well. The degree bound is an exercise.

We prove the second part by a similar induction. Let $g \in K[x]$ be an irreducible factor of f and let $\alpha \in L$ be a root of g, $\alpha' \in L'$ a root of $\kappa(g)$ which is also irreducible. Then $K(\alpha):K$ and $K'(\alpha'):K'$ are isomorphic extensions, say by (κ,κ'). Then $L:K(\alpha)$ and $K':K'(\alpha')$ are splitting fields for $\frac{f}{x-\alpha}$ and $\kappa'\left(\frac{f}{x-\alpha}\right) = \frac{\kappa(f)}{x-\alpha'}$ respectively so by induction there is $\lambda : L \to L'$ so that (κ',λ) is an isomorphism of the extensions. It follows that (κ,λ) is an isomorphism of extensions. □

DEFINITION 130. Call $L:K$ *normal* if every irreducible $f \in K[x]$ which has a root in L splits in L.

PROPOSITION 131. *If $L:K$ is normal and M is an intermediate field then $L:M$ is normal.*

PROOF. (Exercise). □

THEOREM 132. *L/K is normal and finite iff it is a splitting field.*

PROOF. If L/K is finite it is finitely generated, say $L = K(\alpha_1,\ldots,\alpha_r)$. Let $g_i \in K[x]$ be the minimal polynomial of α_i. Then $f = \prod_i g_i$ splits in L (each g_i does by normality), while every subfield of L where f splits contains all the α_i and hence is L. For the converse let $L:K$ be the splitting field of $f \in K[x]$ and let $\alpha \in L$ have minimal polynomial g. In the splitting field M of fg (which contains a unique copy of L) let α' be another root of g. Then $K(\alpha):K$ and $K(\alpha'):K$

are isomorphic extensions, hence of the same degree. Next, $L(\alpha):K(\alpha)$ and $L(\alpha'):K(\alpha')$ are splitting fields for the same polynomial f (the isomorphism of $K(\alpha)$ and $K'(\alpha)$ fixes K). Thus they are isomorphic extensions and also have the same degree. It follows that $[L(\alpha):K]=[L(\alpha'):K]$. Dividing by $[L:K]$ shows $[L(\alpha'):L]=[L(\alpha):L]=1$ so $\alpha'\in L$ as well so $M=L$ and g splits in L. □

DEFINITION 133. A *normal closure* of an extension of fields $L:K$ is an extension $N:L$ so that $N:K$ is normal while every proper intermediate extension of $N:L$ is not.

PROPOSITION 134. *Normal closures exist and are unique up to isomorphism of fields.*

PROOF. Assume $[L:K]<\infty$, say $L=K(\alpha_1,\ldots,\alpha_r)$. Let $g_i\in K[x]$ be a minimal polynomial of α_i. Then N is a normal closure iff it is a splitting field for $\prod_i g_i$. The infinite case is left as an exercise (one way is to construct it in an algebraic closure). □

EXAMPLE 135. Every quadratic extension is normal.

4.2. Separability

DEFINITION 136. Let $L:K$ be an extension. Call $f\in K[x]$ *separable* if every irreducible factor of f has distinct roots in the splitting field. Call $\alpha\in L$ *separable over* K if its minimal polynomial in $K[x]$ is separable. Call $L:K$ *separable* if every $\alpha\in L$ is separable over K, *purely inseparable* if every $\alpha\in L$ separable over K belongs to K.

PROPOSITION 137. *If $L:K$ is separable and M is an intermediate field then $L:M$ and $M:K$ are separable.*

PROOF. (Exercise). □

PROPOSITION 138. *(Construction of monomorphisms) Let L/K be finite. Then there are at most $[L:K]$ K-monomorphisms of L into a normal closure N/K. If L is generated over K by separable elements then the number of monomorphisms is precisely $[L:K]$, and conversely if the number if $[L:K]$ then the extension is separable.*

PROOF. Induction on the degree. Assuming that $n=[L:K]>1$ let $\alpha\in L\setminus K$ have minimal polynomial $f\in K[x]$ and let $\{\alpha_i\}_{i=1}^{e}$ be the roots of f in N (including $\alpha_1=\alpha$), and note that $e\le d=\deg(f)$. Then $K(\alpha)$ has precisely e embeddings into N. By induction L has at most $\frac{n}{d}=[L:K(\alpha)]$ $K(\alpha)$-embeddings into N with α mapping to α_i. Since every embedding maps α to one of the α_i it follows that the total number of embedding is at most $e\cdot\frac{n}{d}\le d\cdot\frac{n}{d}=n$. If we can choose $\alpha\in L$ which is not separable then we'd have $e<d$ and so the number of embedding would be strictly less than n. If L/K is generated by separable elements then we take α to be one of them so $e=d$; since $L/K(\alpha)$ is also generated by separable elements it has precisely $\frac{n}{d}$ embeddings and we are done. □

We obtain several corollaries:

THEOREM 139. *(Separability) A finite extension L/K is separable iff it is generated by separable elements. Thus:*

1. *An extension generated by separable elements is separable.*
2. *Let $K\hookrightarrow L\hookrightarrow M$ with L/K separable and let $\alpha\in M$ be separable over L. Then α is separable over K. In particular, M/K is separable iff M/L and L/K are.*

(3) *If M/K is an extension then the subset $L \subset M$ of elements which are separably algebraic over K is a subfield, the separable closure of K in M. If M/K is algebraic the extension M/L is purely inseparable.*

PROOF. The initial claim is immediate.

(1) let $L = K(S)$ with $S \subset L$ separable algebraic over K. For each $\alpha \in L$ there is a finite subset $T \subset S$ so that $\alpha \in K(T)$ and we may apply the Proposition to the extension $K(T) : K$.
(2) Let $f \in L[x]$ be the minimal polynomial of α and let $R = K(f)$ be the subfield generated by its coefficients. Let N/K be a normal closure of M/K. Then R has $[R : K]$ embeddings into N and each can be extended in $[R(\alpha) : R] = \deg(f)$ ways to embeddings of $R(\alpha)$. It follows that $R(\alpha)$ has $[R(\alpha) : K]$ K-embeddings into N so $R(\alpha)$ is separable and so is α.
(3) The field extension generated by the separable elements is separable, hence is equal to that set. Any element of the extension separable over the separable closure is separable over the base field.

□

EXAMPLE 140. Let $\mathrm{char}(K_0) = p$ and let $K = K_0(t)$ be the function field in one variable over K_0. Then $x^p - t \in K[x]$ is irreducible and inseparable. Indeed if L/K is a field and $s \in L$ is a root then $(x-s)^p = x^p - s^p = x^p - t$ so s is the unique root of $x^p - t$ in L. Also, any monic divisor of $x^p - t$ in $L[x]$ has the form $(x-s)^r$ for some $0 \leq r \leq p$. If $1 \leq r < p$ then the constant coefficient of this divisor is $s^{r/p} \notin K$ (this elements generates $K(s)$ as well) so the divisor is not in $K[x]$. One can also see that $x^p - t$ is irreducible using Eisenstein's criterion in $K_0[t][x]$.

4.3. Automorphism Groups

DEFINITION 141. Let L be a field. $\mathrm{Aut}(L)$ will be the group of automorphisms of L. If $L : K$ is an extension of fields we write $\mathrm{Aut}_K(L)$ for the group of automorphisms fixing K element-wise.

EXAMPLE 142. Quadratic extensions in characteristic different from 2, $\mathbb{Q}(\sqrt[3]{2})$ and its normal closure, the inseparable extension.

LEMMA 143. *(Dedekind) Let K, L be fields. Then $\mathrm{Hom}(K, L)$ is linearly independent over L (as a subset of L^K).*

PROOF. Let $0 = \sum_{i=1}^{r} a_i f_i$ be a minimal linear combination. Then the f_i distinct and all the a_i are non-zero. We have $r \geq 2$ since $0 \notin \mathrm{Hom}(K, L)$. Let $y \in K$ be such that $f_1(y) \neq f_r(y)$ (then $y \neq 0$ as are $f_1(y)$, $f_r(y)$), and see that for all $x \in K$ we have:

$$\begin{aligned}
\sum_{i=1}^{r-1} \left(a_i \left(f_i(y) - a_i f_n(y)\right)\right) f_i(x) &= \sum_{i=1}^{r} a_i f_i(y) f_i(x) - f_n(y) \sum_{i=1}^{r} a_i f_i(x) \\
&\left(\sum_{i=1}^{r} a_i f_i\right)(yx) - f_n(y) \left(\sum_{i=1}^{r} a_i f_i\right)(x) \\
&= 0 .
\end{aligned}$$

□

REMARK 144. In fact, we have shown that if H is a group then $\mathrm{Hom}(H, L^\times)$ is linearly independent (take $H = K^\times$).

COROLLARY 145. *Let* $[L:K]=n$. *Then* $\#\mathrm{Aut}_K(L)\leq n^2$.

PROOF. $\mathrm{Aut}_K(L)$ is a linearly independent subset of the space of linear maps on an n-dimensional K-vector space. □

PROPOSITION 146. *Let* $[L:K]=n$. *Then* $\#\mathrm{Aut}_K(L)\leq n$.

PROOF. Let $\{\omega_i\}_{i=1}^n$ be a basis for L over K. Each $\sigma\in\mathrm{Aut}_K(L)$ is determined by the vector $(\sigma(\omega_i))_{i=1}^n\in L^n$, and these vectors are linearly independent over L: if $a_\sigma\in L$ are such that $\sum_\sigma a_\sigma\sigma(\omega_i)=0$ for each i, then $\sum_\sigma a_\sigma\sigma$ is a K-linear map $L\to L$ which vanishes on a basis, hence vanishes identically, which forces all the a_σ to vanish by the Lemma. Since $\dim_L L^n=n$ we are done. □

DEFINITION 147. For $\sigma\in\mathrm{Aut}(L)$ write $\mathrm{Fix}(\sigma)=\{x\in L\mid\sigma(x)=x\}$, a subfield of L. For $S\subset\mathrm{Aut}(L)$ write $\mathrm{Fix}(S)=\cap_{\sigma\in S}\mathrm{Fix}(\sigma)$. Note that $\mathrm{Fix}(S)=\mathrm{Fix}(\langle S\rangle)$.

PROPOSITION 148. *Let* L *be a field,* $G\subset\mathrm{Aut}(L)$ *a finite subgroup of order* n, *and let* $K=\mathrm{Fix}(G)$. *Then* $[L:K]=n$.

PROOF. To each $\omega\in L$ associate the vector $\omega^G=(\sigma(\omega))_{\sigma\in G}\in L^G$. Let $\Omega\subset L$ be a basis over K and let $\sum_{i=1}^r a_i\omega_i^G=0$ be a minimal linear dependence in L^G over L. Then for each $\sigma\in G$ we have $\sum_i a_i\sigma(\omega_i)=0$ with $a_i\in L^\times$. For $\tau\in G$ note that we have $\sum_i\tau(a_i)(\tau\sigma)(\omega_i)=0$ for all σ, so $\sum_i\tau(a_i)\omega_i^G=0$ as well. Since minimal combinations are unique up to scalar, there is $b\in L^\times$ so that $\tau(a_i)=ba_i$ for all i. Then $\tau\left(a_1^{-1}a_i\right)=a_1^{-1}a_i$ for all i. Since τ was arbitrary it follows that there are $c_i\in K^\times$ so that $a_i=a_1c_i$. Dividing by a_1 it follows that $\sum_{i=1}^r c_i\omega_i^G=0$. In particular the co-ordinate of the identity gives $\sum_{i=1}^r c_i\omega_i=0$, which is impossible. It follows that $\left\{\omega^G\right\}_{\omega\in\Omega}\subset L^G$ are linearly independent over L, and hence that $|\Omega|\leq|G|$, that is $[L:K]\leq|G|$. In particular ,$[L:K]$ is finite, and we then have $|G|\leq[L:K]$ as well. □

Math 422/501: Problem set 8 (due 4/11/09)

Monomorphisms of fields

1. (From class)
   (a) Let L/K be a finite extension and $\sigma \in \mathrm{Hom}_K(L,L)$. Show that σ is an automorphism.
   (b) Let L/K be an algebraic extension and $\sigma \in \mathrm{Hom}_K(L,L)$. Show that σ is an automorphism.
   (c) Give an example showing there exist extensions with endomorphisms which are not automorphisms.

2. Let $\varphi : \mathbb{R} \to \mathbb{R}$ be a homomorphism of rings. Show that φ is the identity map.

3. (The Frobenius map) Let K be a field of characteristic $p > 0$
   (a) Show that the map $x \mapsto x^p$ defines a monomorphism $K \to K$.
   (b) Conclude by induction that the same holds for the map $x \mapsto x^{p^r}$ for any $r \geq 1$.
   (c) When K is finite show that the Frobenius map is an automorphism.
   OPT When $K = \bar{\mathbb{F}}_p$ show that the Frobenius map is again an automorphism, and obtain a group homomorphism $\mathbb{Z} \mapsto \mathrm{Gal}(\bar{\mathbb{F}}_p : \mathbb{F}_p)$.
   FACT The image of this homomorphism is dense.

4. (The Galois correspondence for $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$).
   (a) Find all $\mathbb{Q}$-automorphisms of K and give their group structure.
   (b) Find all subfields of K.
   (c) Show that the map $H \mapsto \mathrm{Fix}(H)$ gives a bijection between subgroups of the automorphism group and subfields of K.

Finite fields

5. (Multiplicative groups)
   (a) Let G be a finite p-group such that for every d, $\left|\left\{g \in G \mid g^d = e\right\}\right| \leq d$. Show that G is cyclic.
   (b) Let G be a finite group such that for every d, $\left|\left\{g \in G \mid g^d = e\right\}\right| \leq d$. Show that G is cyclic.
   (c) Let F be a field, $G \subset F^\times$ a finite group. Show that G is cyclic.

6. (Uniqueness of finite fields) Fix a prime p and let $q = p^r$ for some $r \geq 1$.
   (a) Show that the polynomial $x^q - x \in \mathbb{F}_p[x]$ is separable.
   (b) Let F be a finite field with q elements. Show that F is a splitting field for $x^q - x$ over $\mathbb{F}_p$.
   (c) Conclude that for each q there is at most one isomorphism class of fields of order q. If such a field exists it is denoted $\mathbb{F}_q$.

7. (Existence of finite fields) Fix a prime p and let $q = p^r$ for some $r \geq 1$.
   (a) Let $F/\mathbb{F}_p$ be a splitting field for $x^q - x$, and let $\sigma\colon F \to F$ be the map $\sigma(x) = x^q$. Show that the fixed field of σ is also a splitting field.
   (b) Conclude that the field F has order q.

8. Let F be a finite field, K/F a finite extension.
   (a) Show that the extension K/F is normal and separable.
   Hint: 7(a).
   (b) Show that there exists $\alpha \in K$ so that $K = F(\alpha)$.
   Hint: Consider the group $K^\times$.

Optional – Finite fields

A. (Galois correspondence for finite fields) Fix a prime p.
   (a) Assume that $\mathbb{F}_{p^r}$ embeds in $\mathbb{F}_{p^k}$. Show that $r|k$.
   (b) Let $r|k$. Show that $\mathbb{F}_{p^k}$ has a unique subfield isomorphic to $\mathbb{F}_{p^r}$, consisting of the fixed points of the map $x \mapsto x^{p^r}$.
   (c) Show that $\mathrm{Gal}(\mathbb{F}_{p^k} : \mathbb{F}_{p^r})$ is cyclic and generated by the Frobenius map $x \mapsto x^{p^r}$.
   (d) Obtain the Galois correspondence for extensions of finite fields.

4.4. The group action

If L/K is an extension of fields, then $\mathrm{Aut}_K(L)$ acts on L. We now investigate the orbits of this action. For this note that if L,M are extensions of K and $\sigma \in \mathrm{Hom}_K(L,M)$, and if $f \in K[x]$, $\alpha \in L$ then $\sigma(f(\alpha)) = f(\sigma(\alpha))$. In particular, α is root of f iff $\sigma(\alpha)$ is.

COROLLARY 149. *Let L/K be an algebraic extension, let N/K be a normal extension and let M/N be a further extension. Assume we have a K-monomorphism $\sigma\colon L \to N$. Then every K-monomorphism $\tau \in \mathrm{Hom}_K(L,M)$ has its image in N.*

PROOF. For every $\alpha \in L$, $\tau(\alpha) \in M$ is a root of the minimal polynomial of α, and this polynomial already has the root $\sigma(\alpha) \in N$. □

and $\sigma \in \mathrm{Aut}_K(L)$ then $\sigma(f(\alpha)) = f(\sigma(\alpha))$. It follows that if α is algebraic over K then its orbit is contained in the set of roots of its minimal polynomial.

LEMMA 150. *Let $f \in K[x]$ be irreducible and let N/K be a finite normal extension. If f splits in N then $\mathrm{Aut}_K(N)$ acts transitively on the roots of f.*

PROOF. Let α, β be roots of f in N. By Theorem 132 there exist $g \in K[x]$ be such that N is the splitting field of g over K, hence also over $K(\alpha)$ and $K(\beta)$. By Theorem 129 the K-isomorphism of $K(\alpha)$ and $K(\beta)$ carrying α to β extends to an isomorphism of N to itself. □

We can generalize this:

PROPOSITION 151. *(Construction of monomorphisms) Let L/K be a finite algebraic extension, let N/K be a finite normal extension and let $\sigma, \tau \in \mathrm{Hom}_K(L,N)$. Then there exists $\rho \in \mathrm{Aut}_K(N)$ so that $\tau = \rho\sigma$.*

PROOF. Again let $g \in K[x]$ be such that N is the splitting field of g. Then $\sigma, \tau\colon L \to N$ are both splitting fields for g, and are therefore isomorphic. □

We can rephrase this by saying that $\mathrm{Aut}_K(N)$ acts transitively on $\mathrm{Hom}_K(L,N)$.

THEOREM 152. *Let L/K be an algebraic extension, let N/K be a normal algebraic extension, and let $\sigma, \tau \in \mathrm{Hom}_K(L,N)$. Then there exists $\rho \in \mathrm{Aut}_K(N)$ so that $\tau = \rho\sigma$.*

PROOF. Identifying L with $\sigma(L)$ we may assume $\sigma = \mathrm{id}$. Consider the set of functions μ whose domain is a subfield of N containing L, whose range is contained in N, and which are field monomorphisms extending τ, ordered by inclusion. Let ρ be a maximal element of the set (this exists by Zorn's Lemma). If the domain of ρ is a proper subfield M of N let $\alpha \in N \setminus M$. □

4.5. Galois groups and the Galois correspondence (2/11/09)

DEFINITION 153. If L/K is normal and separable we say that it is a *Galois extension,* call $\mathrm{Aut}_K(L)$ the *Galois group,* and denote it $\mathrm{Gal}(L:K)$.

THEOREM 154. *Let $[L:K] = n$. Then the following are equivalent:*

(1) *L/K is a Galois extension.*
(2) *$\mathrm{Aut}_K(L)$ has order n.*
(3) *The fixed field of $\mathrm{Aut}_K(L)$ is precisely K.*

PROOF. By Proposition 138 if L/K is normal and separable there are $n = [L:K]$ K-automorphisms of L. By Proposition 148, K is the fixed field of $\mathrm{Aut}_K(L)$ iff $\#\mathrm{Aut}_K(L) = [L:K]$. If the fixed is indeed K let N be a normal closure of L/K. Then $\#\mathrm{Aut}_K(L)$ consists of $[L:K]$ K-monomorphisms from L to N. By Proposition 138 we see that L/K is separable. Also, every K-monomorphism of L into N has its image in L. Let $f \in K[x]$ be irreducible and have a zero $\alpha \in L$. Then f splits in N, and for every other root $\beta \in N$ there is a K-monomorphism of L into N mapping α to β (otherwise there would not be $n = [L:K]$ monomorphisms in total). It follows that $\beta \in L$, that is that L is normal. □

THEOREM 155. *(Galois Correspondence) Let $L:K$ be a finite Galois extension. Then the inclusion-reversing maps $H \mapsto \mathrm{Fix}(H)$, $M \mapsto \mathrm{Gal}(L:M)$ between subgroups $H < \mathrm{Gal}(L:K)$ and intermediate fields $K \subset M \subset L$ are inverse to each other. Further:*

(1) *$M:K$ is normal iff $\mathrm{Gal}(L:M)$ is normal in $\mathrm{Gal}(L:K)$.*
(2) *If $M:K$ is normal then $\mathrm{Gal}(M:K) \simeq \mathrm{Gal}(L:K)/\mathrm{Gal}(L:M)$.*

PROOF. Clearly if $M \subset M' \subset L$ then $\mathrm{Aut}_{M'}(L) \subset \mathrm{Aut}_M(L)$: every M'-automorphism of L is an M-automorphism. Similarly, if $H \subset H'$ then every $\alpha \in L$ fixed by H' is fixed by H. Also, for any intermediate field M, $L:M$ is normal and separable hence Galois. Now for $H < \mathrm{Gal}(L:K)$ we have $H \subset \mathrm{Gal}(L:\mathrm{Fix}(H))$. By Proposition 148 $[L:\mathrm{Fix}(H)] = \#H$ and by the previous Theorem $[L:\mathrm{Fix}(H)] = \#\mathrm{Gal}(L:\mathrm{Fix}(H))$. It follows that $H = \mathrm{Gal}(L:\mathrm{Fix}(H))$. Similarly for an intermediate field M, the index of $\mathrm{Fix}(\mathrm{Gal}(L:M))$ in L is the same as the index of M. Since the two are contained in each other they are equal.

Finally, let $\sigma \in \mathrm{Gal}(L:K)$ and let $H < \mathrm{Gal}(L:K)$. Then the fixed field of $\sigma H \sigma^{-1}$ is exactly $\sigma\,\mathrm{Fix}(H)$. If $\mathrm{Fix}(H)$ is normal than any K-automorphism of L must leave $\mathrm{Fix}(H)$ invariant since it maps roots of polynomials to roots of polynomials, so $\sigma H \sigma^{-1}$ has the same fixed field as H and hence is equal. Conversely, if H is normal then $\mathrm{Fix}(H)$ is an invariant set for the action of $\mathrm{Gal}(L:K)$; since the orbits of the action are precisely the sets of roots of irreducible polynomials, it follows that $M = \mathrm{Fix}(H)$ is normal over K. Restricting the action of the Galois group to M we obtain a map $\mathrm{Gal}(L:K) \to \mathrm{Gal}(M:K)$. By definition, the kernel of this map is $\mathrm{Gal}(L:M)$. It is surjective since by Proposition 151 every K-automorphism of M extends to a K-automorphism of L. □

PROPOSITION 156. *Let L/K Galois extension, and let $\alpha \in L$. Let $O \subset L$ be the orbit of α under $\mathrm{Gal}(L:K)$. Then O is finite and $f = \prod_{\beta \in O}(x-\beta)$ is the minimal polynomial of α over K.*

PROOF. Since O is contained in the roots of the minimal polynomial, it is finite, and we may then take L finite. From now on we only assume that $G = \mathrm{Aut}_K(L)$ has order $n = [K:L]$, this giving an alternative proof of the converse part of Theorem 154. First, for $\sigma \in G$ we have $\sigma(f) = \prod_{\beta \in O}(x - \sigma(\beta)) = f$ so f belongs to the fixed field of G, that is K. Note that f has distinct roots by construction, so α is separable. f is also irreducible, since a product of the form $\prod_{\beta \in S}(x-\beta)$ is G-fixed if an only if S is G-invariant set, and it follows that every irreducible in $K[x]$ which has a root in L splits in L, so L is normal. □

4.6. Examples and applications

4.6.1. The primitive element Theorem.

THEOREM 157. *Let L/K be a finite, separable extension. Then $L = K(\theta)$ for some $\theta \in K$.*

PROOF. Assume first that K is infinite, and let N/K be a normal closure of L/K. Then N/K is finite by Proposition 134 and separable since the Proposition shows it is generated by separable elements. Since $\mathrm{Gal}(N/K)$ is finite it has finitely many subgroups, and by the Galois correspondence it follows that there are finitely many intermediate fields between N and K, hence also between L and K. The claim now follows from problem 11 of problem set 6. When K is finite L is finite as well and the claim is problem 8 of problem set 8. □

4.6.2. Symmetric combination and Galois's outlook. Let $f \in K[x]$ split in $L[x]$ with roots $\{\alpha_1, \ldots, \alpha_r\}$. Let $s \in K[\underline{y}]^{S_r}$. Then $s(\underline{\alpha}) \in K$.

4.6.3. Cyclotomic fields. See Problem Set 9.

4.6.4. The polynomial $t^4 - 2$. See [**2**, Ch. 12]

Math 422/501: Problem set 9 (due 13/11/09)

Galois theory

1. Let L/K be a finite Galois extension. Let $K \subset M_1, M_2 \subset L$ be two intermediate fields. Show that the following are equivalent:
   (1) M_1/K and M_2/K are isomorphic extensions.
   (2) There exists $\sigma \in \mathrm{Gal}(L:K)$ such that $\sigma(M_1) = M_2$.
   (3) $\mathrm{Gal}(L:M_i)$ are conjugate subgroups of $\mathrm{Gal}(L:K)$.

2. (V-extensions) Let K have characteristic different from 2.
   (a) Suppose L/K is normal, separable, with Galois group $C_2 \times C_2$. Show that $L = K(\alpha, \beta)$ with $\alpha^2, \beta^2 \in K$.
   (b) Suppose $a, b \in K$ are such that none of a, b, ab is a square in K. Show that $\mathrm{Gal}(K(\sqrt{a}, \sqrt{b}) : K) \simeq C_2 \times C_2$.

The fundamental theorem of algebra

3. (Preliminaries)
   (a) Show that every simple extension of $\mathbb{R}$ has even order.
   (b) Show that every quadratic extension of $\mathbb{R}$ is isomorphic to $\mathbb{C}$.

4. (Punch-line)
   (a) Let $F : \mathbb{R}$ be a finite extension. Show that $[F : \mathbb{R}]$ is a power of 2.
   Hint: Consider the 2-Sylow subgroup of the Galois group of the normal closure.
   (b) Show that every proper algebraic extension of $\mathbb{R}$ contains $\mathbb{C}$.
   (c) Show that every proper extension of $\mathbb{C}$ contains a quadratic extension of $\mathbb{C}$.
   (d) Show that $\mathbb{C} : \mathbb{R}$ is an algebraic closure.

Example: Cyclotomic fields

$\mu_n \subset \mathbb{C}^\times$ will denote the group of nth roots of unity, $S_n \subset \mu_n$ the primitive nth roots of unity.

5. (prime order) Let p be an odd prime, and recall the proof from class that $\Phi_p(x) = \frac{x^p - 1}{x - 1}$ is irreducible in $\mathbb{Q}[x]$.
   (a) Let ζ_p be a root of Φ_p. Show that $\mathbb{Q}(\zeta_p)$ is a splitting field for Φ_p. What is its degree?
   (b) Show that $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ is cyclic.
   (c) Show that $\mathbb{Q}(\zeta_p)$ has a unique subfield K so that $[K : \mathbb{Q}] = 2$.
   (d) Show that there is a unique non-trivial homomorphism $\chi : G \to \{\pm 1\}$.
   (e) Let $g = \sum_{\sigma \in G} \chi(\sigma)\sigma(\zeta)$ ("Gauss sum"). Show that $g \in K$ and that $g^2 \in \mathbb{Q}$.
   OPT Show that $g^2 = (-1)^{\frac{p-1}{2}} p$, hence that $K = \mathbb{Q}(g)$.

6. Let $\zeta_n \in \mathbb{C}$ be a primitive nth root of unity.
   (a) Show that $\mathbb{Q}(\zeta_n)$ is normal over $\mathbb{Q}$.
   Hint: Show that every embedding of $\mathbb{Q}(\zeta_n)$ in $\mathbb{C}$ is an automorphism.
   (b) Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$. Show for every $\sigma \in G$ there is $j \in (\mathbb{Z}/n\mathbb{Z})^\times$ so that $\sigma(\zeta_n) = \zeta_n^{j(\sigma)}$ and that $j\colon G \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an injective homomorphism.
   (c) Let $\Phi_n(x) = \prod_{\zeta \in S_n}(x - \zeta)$. Show that $\Phi_n(x) \in \mathbb{Q}[x]$ (in fact, $\Phi_n(x) \in \mathbb{Z}[x]$). Show that the degree of Φ_n is exactly $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.
   (d) Show that the definitions of $\Phi_p(x)$ in problems 5 and 6(c) agree.

7. (prime power order) Let p be prime, $r \geq 1$ and let $n = p^r$.
   (a) Show that $\Phi_n(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1}$.
   (b) Show that Φ_n is irreducible.
   Hint: Change variables to $\Phi_n(1+y)$ and reduce mod p.
   (c) Conclude that $\mathrm{Gal}(\Phi_{p^r}) \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times$.

8. (general order) Let $n = \prod_{i=1}^s p_i^{r_i}$ with p_i distinct primes. Let G, j be as in 6(b).
   (a) Show that $\mathbb{Q}(\zeta_n) = \mathbb{Q}\left(\zeta_{p_1^{r_1}}, \ldots, \zeta_{p_s^{r_s}}\right)$.
   (b) For each i let $\pi_i\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \left(\mathbb{Z}/p_i^{r_i}\mathbb{Z}\right)^\times$ be the natural quotient map. Show that the maps $\pi_i \circ j\colon G \to \left(\mathbb{Z}/p_i^{r_i}\mathbb{Z}\right)^\times$ are surjective.
   (c) [deferred]

Example: Cubic extensions

9. Let K be a field, $f \in K[x]$ of degree n, and let $\{\alpha_i\}_{i=1}^n \subset \Sigma$ be the roots of f in a splitting field Σ, counted with multiplicity.
   (a) Let $\{s_r\}_{r=1}^n$ be the elementary symmetric polynomials in n variables, thought of as elements of $K[y_1, \ldots, y_n]$. Show that $s_r(\alpha_1, \ldots, \alpha_n) \in K$.
   Hint: Consider the factorization of f in Σ.
   (b) Let $t \in K[\underline{y}]^{S_n}$ be any symmetric polynomial. Show that $t(\alpha_1, \ldots, \alpha_n) \in K$.

10. Let K be a field of characteristic zero, and let $f \in K[x]$ be an irreducible cubic. Let Σ be a splitting field for f, and let $\{\alpha_i\}_{i=1}^3$ be the roots.
   (a) Show that $[\Sigma : K] \in \{3, 6\}$ and that $\mathrm{Gal}(\Sigma : K)$ is isomorphic to C_3 or S_3.
   Hint: The Galois group acts transitively on the roots.
   (b) Let $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$, and let $\Delta = \delta^2$. Show that $\Delta \in K^\times$.
   (c) Let $M = K(\delta)$. Show that $[\Sigma : M] = 3$ and hence that $[\Sigma : K] = 3$ iff $\delta \in K$. Conclude that f is still irreducible in $M[x]$.
   (d) Assume that $K \subset \mathbb{R}$ and that $\Sigma \subset \mathbb{C}$. Show that $\Sigma \subset \mathbb{R}$ iff $M \subset \mathbb{R}$ iff $\delta \in \mathbb{R}$ iff $\Delta > 0$.
   — We now adjoin ω so that $\omega^3 = 1$.
   (e) Show that $[\Sigma(\omega) : M(\omega)] \in \{1, 3\}$, and in the first case that Σ is contained in a radical extension.
   (f) Assuming $[\Sigma(\omega) : M(\omega)] = 3$ show that this extension is still normal.
   (g) Let $y = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \in \Sigma(\omega)$. Show that for any $\sigma \in \mathrm{Gal}(\Sigma(\omega) : M(\omega))$ there is j so that $\sigma y = \omega^j y$. Conclude that $y^3 \in M(\omega)$.

4.7. Solubility by radicals

In this section all fields have characteristic zero.

DEFINITION 158. $f \in K[x]$ separable. Then $\mathrm{Gal}(f) \stackrel{\text{def}}{=} \mathrm{Gal}(\Sigma(f) : K)$ where $\Sigma(f)$ is the splitting field.

Call L/K radical *if* $L = K(\alpha_1, \ldots, \alpha_s)$ *and for each* i *there is* r_i *so that* $\alpha_i^{r_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$. *Call* $f \in K[x]$ soluble by radicals *if there exists a radical extension containing* $\Sigma(f)$. *If* f *is irreducible enough to show* $K[x]/(f)$ *is contained in a radical extension.*

THEOREM 159. $f \in K[x]$ *is soluble by radicals iff* $\mathrm{Gal}(f)$ *is a solvable group.*

4.7.1. Radical extensions are solvable (4-9/11/09).

LEMMA 160. L/K *contained in a radical then normal closure* N/K *contained in a radical.*

PROOF. Enough to show that the normal closure of a radical extension is radical. Indeed, let $L = K(\alpha_1, \ldots, \alpha_s)$ be radical, let N be the normal closure, $G = \mathrm{Gal}(N : K)$. Then $N = K(\{\sigma(\alpha_i) \mid \sigma \in G, 1 \leq i \leq s\}$ Ordering this lexicographically with i most significant than σ exhibits this as a radical extension.

In the alternative let $r = \mathrm{lcm}\{r_1, \ldots, r_s\}$ and let $N = L(\mu_r)$. Then N is normal (contains all conjugates of the α_i) and radical. □

LEMMA 161. $\mathrm{Gal}(\Sigma(t^p - 1) : K)$ *is Abelian.*

PROOF. Automorphisms raise generator to a power. □

LEMMA 162. *If* $\mu_n \subset K$ *then* $\Sigma(t^n - a) : K$ *is abelian.*

PROOF. Galois group maps the root α to the root $\zeta\alpha$ where ζ is a root of unity. □

PROPOSITION 163. L/K *normal and radical implies* $\mathrm{Gal}(L : K)$ *solvable.*

PROOF. Induction on number of roots. Can assume r_i are all prime. Say $\alpha^p \in K$ but $\alpha \notin K$. Let $M \subset L$ be splitting field for $t^p - 1$. Then $M : K$, $M(\alpha) : M$ are normal and abelian. $L : M(\alpha)$ solvable by induction. □

THEOREM 164. L/K *contained in radical extension. Then* $\mathrm{Aut}_K(L)$ *is solvable.*

PROOF. $K \subset L \subset R \subset N$ where R/K is radical, N/K its normal closure. Then N/K is radical so $\mathrm{Gal}(N/K)$ is solvable. Let $H = \{\sigma \in \mathrm{Gal}(N/K) \mid \sigma(L) \subset L\}$; restriction gives a map $H \to \mathrm{Aut}_K(L)$ with kernel $\mathrm{Gal}(N : L)$. This map is surjective since every K-automorphism of L is extends to an automorphism of N since N is a splitting field of some $f \in K[x]$. Now H is solvable as a subgroup of a solvable group, and $\mathrm{Aut}_K(L)$ is solvable as a quotient of a solvable group. □

4.7.2. Insoluble polynomials (9/11/09).

PROPOSITION 165. *Let* p *be prime,* $f \in \mathbb{Q}[x]$ *irreducible of degree* p *with precisely two complex roots. Then* $\mathrm{Gal}(f) \simeq S_p$.

PROOF. Let $A \subset \mathbb{C}$ be the roots of f, $\Sigma = \mathbb{Q}(A)$ the splitting field, $G = \mathrm{Gal}(\Sigma : \mathbb{Q})$. Then G acts transitively on a set of size p, giving an embedding $G \hookrightarrow S_p$. If $\alpha \in A$ is any root then $[\mathbb{Q}(\alpha) : \mathbb{Q})] = p$ so $p | [\Sigma : \mathbb{Q}] = \#G$ so the image of the map contains an element of order p, which is hence a p-cycle $\sigma \in S_p$. Let $\tau \in G$ be the restriction of complex conjugation to Σ. Then τ is a 2-cycle, say $\tau = (12)$. Any non-identity power of σ is also a p-cycle, and by transitivity there is one of the form $(12 \ldots p)$. These two together generated S_p. □

EXAMPLE 166. $t^5 - 6t + 3 \in \mathbb{Q}[x]$ is irreducible by Eisenstein. Its derivative is $5t^4 - 6$ which is positive if $|t| > \left(\frac{6}{5}\right)^{1/4} = u$ and negative in $|t| < \left(\frac{6}{5}\right)^{1/4}$. Since $f(-u) = -\frac{6}{5}u + 6u + 3 > 0$ and $f(u) = \frac{6}{5}u - 6u + 3 = 3 - 4.8u < 0$ since $u > 1$, it follows that f has three real roots (one in $(-\infty, -u)$, one in $(-u, u)$ and one in (u, ∞)).

4.7.3. Solvable extensions are radical (9/11/09).

DEFINITION 167. Let L/K be a finite extension and let $\alpha \in L$. If L/K is Galois set $\mathrm{Tr}_K^L(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha$, $N_K^L(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha$. In general let $\mathrm{Tr}_K^L(\alpha)$ and $N_K^L(\alpha)$ be, respectively, the trace and determinant of multiplication by α, thought of as a K-linear map $L \to L$.

EXERCISE 168. (PS10 problem 3) The two definitions coincide when they intersect.

(PS10 problem 2) Let $1 < [L : K] < \infty$ be prime to $\mathrm{char}(K)$. Then $L = L_0 \oplus K$ as K-vector spaces. In particular, there exist $\alpha \in L \setminus K$ with trace zero.

The key step in our induction will be the following:

PROPOSITION 169. *Let L/K be a Galois extension of prime index p, and assume $\mu_p \subset K$. Then L is radical over K.*

PROOF. Let σ generate $G = \mathrm{Gal}(L/K)$ (a group of order p hence cyclic). For $\alpha \in L$ and $\zeta \in \mu_p$ consider the *Lagrange Resolvent*

$$\Theta(\alpha, \zeta) = \sum_{b(p)} \zeta^b \sigma^b(\alpha).$$

Then:

$$\sigma(\Theta(\alpha, \zeta)) \quad = \quad \zeta^{-1}\Theta(\alpha, \zeta).$$

If $\Theta \neq 0$ and $\zeta \neq 1$ this would show $\Theta(\alpha, \zeta) \notin K$ but $(\Theta(\alpha, \zeta))^p \in K$, finishing the proof. For α fixed let $\Theta(\alpha)$ be the vector $\left(\Theta(\alpha, \zeta_p^a)\right)_{a \in \mathbb{Z}/p\mathbb{Z}} = Z \cdot \alpha^G$ where $Z \in M_n(K)$ is the Vandermonde matrix $Z_{ab} = \zeta_p^{ab}$ and $\alpha^G = \left(\sigma^b(\alpha)\right)_b$. Note that $(Z\alpha)_0 = \mathrm{Tr}\,\alpha$ and choose $\alpha \in L \setminus K$ so that $\mathrm{Tr}(\alpha) = 0$. Then $\alpha^G \neq 0$ so $Z\alpha^G \neq 0$ and it follows that there is $a \neq 0$ so that $(Z\alpha)_a \neq 0$. □

PROPOSITION 170. *("Base change") Let $T : K$ be an extension of fields, and let $L, M \subset T$ be intermediate extensions with L/K is a finite Galois extension. Let $LM \subset T$ be the field generated by L, M. Then $LM : M$ is a finite Galois extension, and restriction to L is an injective map* $\mathrm{Gal}(LM : M) \to \mathrm{Gal}(L : K)$ *(in particular, $[LM : M] \leq [L : K]$). Moreover, if L/K is cyclic, abelian or solvable then so is LM/M.*

PROOF. Assume that L is the splitting field of the separable polynomial $f \in K[x]$. Then LM is the splitting field of f over M. It follows that $LM : M$ is a finite Galois extension. Since L is normal every $\sigma \in \mathrm{Aut}_K(LM)$ maps L to L, so restriction to L gives a map $\mathrm{Aut}_M(LM) \to \mathrm{Aut}_K(L)$. If σ belongs to the kernel of this map then $\sigma \in \mathrm{Aut}(LM)$ fixes M (assumption on the domain) and L (assumption on the image). It follows that σ is trivial. □

THEOREM 171. *Let L/K be a finite solvable Galois extension. Then there exists a radical extension M of K containing L.*

PROOF. Let $[L:K] = n$. We will show that $L(\mu_{n!}) : K$ is radical. It is clearly enough to show that $L(\mu_{n!}) : K(\mu_{n!})$ is radical, and by the base change proposition this is a solvable extension of degree at most n. We now prove by induction on N that if L/K is solvable, and K contains $\mu_{n!}$ then L/K is radical. For this let $G = \mathrm{Gal}(L/K)$, and let $H < G$ be normal of prime index p. Let $M = \mathrm{Fix}(H)$.Then $M : K$ is Galois, with Galois group $G/H \simeq C_p$. Since $p \leq n$, we may apply the first Proposition to see that M/K is radical. Also, $L : M$ is solvable and $[L:M]! \mid [L:K]!$ so M contains all the requisite roots of unity to apply the induction hypothesis. $\square$

Math 422/501: Problem set 10 (due 18/11/09)

The trace

When L/K is a finite Galois extension and $\alpha \in L$ we used in class the combination ("trace") $\mathrm{Tr}_K^L(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha$, which we needed to be non-zero. We will study this construction when L/K is a finite separable extension, fixed for the purpose of the problems 1-3.

1. Let N/K be a normal extension containing L.
   (a) For $\alpha \in L$ we provisionally set $\mathrm{Tr}_K^L(\alpha) = \sum_{\mu\,:\,L\to N} \mu\alpha$ ("trace of α"), $N_K^L(\alpha) = \prod_{\mu\,:\,L\to N} \mu\alpha$ ("norm of α"). Show that the definition is independent of the choice of N.
   (b) Making a judicious choice of N show that the trace and norm defined in part (a) are elements of K.
   (c) Show that when L/K is a Galois extension the definition from part (a) reduces to the combination used in class.

2. (Elements of zero trace) In class we had the occasion to need elements $\alpha \in L$ with trace zero. For this, let $L_0 = \left\{\alpha \in L \mid \mathrm{Tr}_K^L(\alpha) = 0\right\}$.
   (a) Show that Tr_K^L is a K-linear functional on L, so that L_0 is a K-subspace of L.
   (b) When $\mathrm{char}(K) = 0$, show that $L = K \oplus L_0$ as vector spaces over K (direct sum of vector spaces; the analogue of direct product of groups). Conclude that when $[L:K] \geq 2$ the set $L_0 \setminus K$ is non-empty.
   (c) Show that Tr_K^L is a non-zero linear functional in all characteristics.
   (d) Show that L_0 is not contained in K unless $[L:K] = \mathrm{char}(K) = 2$, in which case $L_0 = K$, or $[L:K] = 1$ in which case $L_0 = \{0\}$.

3. (Yet another definition) We continue with the separable extension L/K of degree n.
   (a) Let $f \in K[x]$ be the (monic) minimal polynomial of $\alpha \in L$, say that $f = \sum_{i=0}^d a_i x^i$ with $a_d = 1$. Show that $\mathrm{Tr}_K^{K(\alpha)}(\alpha) = -a_{d-1}$ and that $N_K^{K(\alpha)}(\alpha) = (-1)^d a_0$.
   (b) Show that $\mathrm{Tr}_K^L(\alpha) = -\frac{n}{d} a_{d-1}$ and that $N_K^L(\alpha) = (-1)^n a_0^{n/d}$.
   Hint: Recall the proof that $[L:K]$ has n embeddings into a normal closure.
   (c) Show that $\mathrm{Tr}_K^L(\alpha)$ and $N_K^L(\alpha)$ are, respectively, the trace and determinant of multiplication by α, thought of as a K-linear map $L \to L$.
   Hint: Show that we have $L \simeq (K(\alpha))^{n/d}$ as $K(\alpha)$-vector spaces,.

REMARK. From now on we define the trace and norm of α as in 3(c). Note that this definition makes sense even if L/K is not separable.

4. (Transitivity) Let $K \subset L \subset M$ be a tower of finite extensions. Show that
   (a) $\mathrm{Tr}_K^M = \mathrm{Tr}_K^L \circ \mathrm{Tr}_L^M$.
   (b) $N_K^M = N_K^L \circ N_L^M$.

Purely inseparable extensions

5. Let L/K be an purely inseparable algebraic extension of fields of characteristic p.
   (a) For every $\alpha \in L$ show that there exists $r \geq 0$ so that $\alpha^{p^r} \in K$. In fact, show that the minimal polynomial of α is of the form $x^{p^r} - \alpha^{p^r}$.
   Hint: Consider the minimal polynomials of α and α^p
   (b) Conclude that when $[L:K]$ is finite it is a power of p.
   (c) When $[L:K]$ is finite show that Tr_K^L is identically zero.

Some examples

6. Solve the equation $t^6 + 2t^5 - 5t^4 + 9t^3 - 5t^2 + 2t + 1 = 0$ by radicals.
   Hint: Try $u = t + \frac{1}{t}$.

7. Let K have characteristic zero and consider the system of equations over the field $K(t)$:

$$\begin{cases} x^2 = y + t \\ y^2 = z + t \\ z^2 = x + t \end{cases}.$$

   (a) Let (x,y,z) be a solution in a field extension of $K(t)$. Show that x satisfies either $x^2 = x + t$ or a certain sextic equation over $K(t)$.
   OPT Use a computer algebra system to verify that the sextic is relatively prime both to $x^2 - x - t$ and to its own formal derivative.
   (b) Show that the Galois group of the splitting field of the sextic preserves an equivalence relation among its six roots.
   Hint: Find an permutation of order 3 acting on the roots. This is visible in the original system.
   (c) Let $\{\alpha, \beta, \gamma\}$ be an equivalence class of roots, and let $s(a,b,c)$ be a symmetric polynomial in three variables. Show that $s(\alpha,\beta,\gamma)$ belongs to an extension of $K(t)$ of degree 2 at most.
   Hint: If $s(\alpha,\beta,\gamma)$ is a root of a quadratic, what should the other root be? Show that the coefficients of the putative quadratic are indeed invariant by the Galois group.
   (d) Show that the system of equations can be solved by radicals.
   Hint: For each equivalence class construct a cubic whose roots are the equivalence class and whose coefficients lie in a radical extension.
   OPT Show that knowing $[K(t, x+y+z) : K(t)] = 2$ where x, y, z are roots of the original system would have been enough.

OPTIONAL Let $L = \mathbb{C}(x)$ (the field of rational functions in variable) and for $f \in L$ let $(\sigma(f))(x) = f(\frac{1}{x})$, $(\tau(f))(x) = f(1-x)$.
   (a) Show that $\sigma, \tau \in \mathrm{Aut}(L)$ and that $\sigma^2 = \tau^2 = 1$.
   (b) Show that $G = \langle \sigma, \tau \rangle$ is a subgroup of order 6 of $\mathrm{Aut}(L)$ and find its isomorphism class.
   (c) Let $K = \mathrm{Fix}(G)$. Find this field explicitly.

4.8. The group action and Grothendieck's Galois Correspondence

[to be added later]

CHAPTER 5

Algebraic Number Theory

5.1. Intro (16-18/11/09)

PROPOSITION 172. *TFAE for $\alpha \in \mathbb{C}$:*

(1) *There exists a monic $f \in \mathbb{Q}[x]$ with $f(\alpha) = 0$.*
(2) *$\mathbb{Q}(\alpha)$ is finite-dimensional.*
(3) *There exists a finite-dimensional Q-subspace $W \subset \mathbb{C}$ so that $\alpha W \subset W$.*

PROOF. We have seen $(1) \Rightarrow (2)$, $(2) \Rightarrow (3)$ and clear and $(3) \Rightarrow (1)$ is Cayley-Hamilton. □

DEFINITION 173. $\alpha \in \mathbb{C}$ is an *algebraic number if it satisfies any of these properties.*

PROPOSITION 174. *TFAE for $\alpha \in \mathbb{C}$:*

(1) *There exists a monic $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$.*
(2) *$\mathbb{Z}[\alpha]$ is finite-dimensional.*
(3) *There exists a finite-dimensional $\mathbb{Z}$-submodule $W \subset \mathbb{C}$ so that $\alpha W \subset W$.*

PROOF. Same (see xxx below) □

DEFINITION 175. $\alpha \in \mathbb{C}$ is an *algebraic number if it satisfies any of these properties.*

Math 422/501: Problem set 11 (due 25/11/09)

The discriminant

Let L/K be a separable extension, and let N/K be its normal closure. Let $n = [L:K] = \#\mathrm{Hom}_K(L,N)$, with an enumeration $\mathrm{Hom}_K(L,N) = \{\mu_i\}_{i=1}^n$. Given $\{\omega_j\}_{j=1}^n \subset L$ let $\Omega \in M_n(L)$ be the matrix with $\Omega_{i,j} = \mu_i(\omega_j)$ and set:

$$d_{L/K}(\omega_1,\ldots,\omega_n) = (\det\Omega)^2 .$$

In particular, write $d_{L/K}(\alpha) = d_{L/K}\left(1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\right)$.

1. Let $\{\omega_j\}_{j=1}^n \subset L$.
   (a) Show that $d_{L/K}(\omega_1,\ldots,\omega_n) \in K$.
   (b) Show that $d_{L/K}(\omega_1,\ldots,\omega_n) \neq 0$ iff $\{\omega_j\}_{j=1}^n$ is a basis for L over K.
   (c) Show that $d_{L/K}(\alpha) \neq 0$ iff $L = K(\alpha)$.
   (d) Show that if $d_{L/K}(\alpha) \neq 0$ then it is the discriminant of the minimal polynomial of α.

2. (The case $K = \mathbb{Q}$) Let L be a number field of degree n over $\mathbb{Q}$. Let $\{\omega_i\}_{i=1}^n, \left\{\omega'_j\right\}_{j=1}^n \subset L$ be Q-bases of L so that the abelian groups $M = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$ and $N = \mathbb{Z}\omega'_1 \oplus \cdots \oplus \mathbb{Z}\omega'_n$ satisfy $N \subset M$.
   (a) Show that the sum $\oplus_{i=1}^n (\mathbb{Z}\omega_i)$ is indeed direct.
   (b) Show that $d_{L/\mathbb{Q}}(\omega'_1,\ldots,\omega'_n) = D d_{L/\mathbb{Q}}(\omega_1,\ldots,\omega_n)$ for some positive integer D.
   Hint: Relate the matrices Ω and Ω'.
   (c) Show that when $M = N$ we have $d_{L/\mathbb{Q}}(\omega_1,\ldots,\omega_n) = d_{L/\mathbb{Q}}(\omega'_1,\ldots,\omega'_n)$, in other words that the discriminant of a basis is really a function of the $\mathbb{Z}$-module generated by that basis.
   (d) Say $\omega'_j = a_j\omega_j$ for some $a_j \in \mathbb{Z}$. Show that $D = [M:N]^2$.

   REMARK (c),(d) are special cases of the general identity $d_{L/\mathbb{Q}}(N) = [M:N]^2 d_{L/\mathbb{Q}}(M)$.

Rings of integers

FACT. *(Integral basis Theorem) Let K be a number field of degree n (that is, $[K:\mathbb{Q}] = n$), and let $\mathcal{O}_K \subset K$ be the set of algebraic integers in K. Then there exists a basis $\{\alpha_i\}_{i=1}^n$ of K over $\mathbb{Q}$ so that $\mathcal{O}_K = \oplus_{i=1}^n \mathbb{Z}\alpha_i$. Moreover, $d_K \stackrel{def}{=} d_{K/\mathbb{Q}}(\alpha_1,\ldots,\alpha_n)$ is an integer.*

3. Let D be a square-free integer (this means a product of distinct primes up to sign) and let $K = \mathbb{Q}(\sqrt{D})$.
   (a) Let $\alpha \in K$. Show that α is an algebraic integer iff $\mathrm{Tr}\,\alpha, N\alpha \in \mathbb{Z}$ (trace and norm from K to $\mathbb{Q}$).
   (b) Show that $\frac{1+\sqrt{D}}{2}$ is an algebraic integer iff $D \equiv 1\,(4)$.
   (c) Show that $\mathbb{Z}[\sqrt{D}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{D} \subset \mathcal{O}_K \subset \mathbb{Z}\frac{1}{2} \oplus \mathbb{Z}\frac{\sqrt{D}}{2}$.
   Hint: write $\alpha \in K$ in the form $a + b\sqrt{D}$ for $a,b \in \mathbb{Q}$.
   (d) By considering the equation $x^2 - y^2 D \equiv 0\,(4)$ in $\mathbb{Z}/4\mathbb{Z}$, show that if $D \equiv 2,3\,(4)$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}] = \left\{a + b\sqrt{D} \mid a,b \in \mathbb{Z}\right\}$.

(e) Show that when $D \equiv 1\,(4)$ $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{\frac{a+b\sqrt{D}}{2} \mid a,b \in \mathbb{Z}, a \equiv b\,(2)\right\}$.

— What about $D \equiv 0\,(4)$?

4. (Dedekind) Let $K = \mathbb{Q}(\theta)$ where θ is a root of $f(x) = x^3 - x^2 - 2x - 8$.
   (a) Show that f is irreducible over $\mathbb{Q}$ and find its Galois group.
   (b) Show that $1, \theta, \theta^2$ are all algebraic integers.
   (c) Let $\eta = \frac{\theta^2+\theta}{2}$. Show that $\eta^3 - 3\eta^2 - 10\eta - 8 = 0$ and conclude that is an algebraic integer a well.
   (d) Show that $1, \theta, \eta$ are linearly independent over $\mathbb{Q}$.
   (e) Let $M = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\eta$ and let $N = \mathbb{Z}[\theta] = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta^2$. Show that $N \subset M$.
   (f) Show that $d_{K/\mathbb{Q}}(\theta) = \Delta(f) = -4 \cdot 503$.
   (g) Find $d_{K/\mathbb{Q}}(1, \theta, \eta)$.
   Hint: You can be confident in your answer by consulting 2(a).
   (h) Show that $\{1, \theta, \eta\}$ is an integral basis.
   Hint: Let $\{\alpha, \beta, \gamma\}$ be an integral basis and consider $\frac{d_{K/\mathbb{Q}}(1,\theta,\eta)}{d_{K/\mathbb{Q}}(\alpha,\beta,\gamma)}$.
   (i) Let $\delta = A + B\theta + C\eta$ with $A, B, C \in \mathbb{Z}$. Show that $2 | d_{K/\mathbb{Q}}(\delta)$. Conclude that the set of algebraic integers of K is not of the form $\mathbb{Z}[\delta]$.

5.2. Integrality and Integral basis (23-25/11/09)

Let K be an algebraic extension of $\mathbb{Q}$, $\mathcal{O}_K \subset K$ be the set of algebraic integers.

PROPOSITION 176. *$\alpha \in \mathcal{O}_K$ iff $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module iff there is a non-zero finitely generated $\mathbb{Z}$-module $M \subset K$ so that $\alpha M = M$.*

PROOF. Say α is integral of degree d. Then $\mathbb{Z}[\alpha] = \oplus_{i=0}^{d-1} \mathbb{Z}\alpha^i$ and $\alpha\alpha^i \in \mathbb{Z}[\alpha]$ for all i. The third part implies the first by Cayley-Hamilton. □

COROLLARY 177. *$\mathcal{O}_K$ is a subring of K. If $\alpha \in \mathcal{O}_K$ then:*

(1) *Every conjugate of α is integral over $\mathbb{Q}$;*
(2) *The minimal polynomial of α over $\mathbb{Q}$ is monic and belongs to $\mathbb{Z}[x]$;*
(3) *If K is finite over $\mathbb{Q}$ then $\mathrm{Tr}_{\mathbb{Q}}^K(\alpha), N_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}$ and,*
(4) *$\alpha \in \mathcal{O}_K^\times$ iff $N_{\mathbb{Q}}^K \alpha \in \{\pm 1\}$.*

PROOF. Given $\alpha, \beta \in \mathcal{O}_K$ say $\alpha M \subset M$ and $\alpha N \subset N$ then MN is finitely generated and $\mathbb{Z}[\alpha,\beta]MN \subset MN$. Also, every conjugate of α satisfies the same polynomials that α does. The minimal polynomial of α is $\prod_{\mu \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \bar{\mathbb{Q}})} (x - \mu\alpha) \in \mathcal{O}_{\bar{\mathbb{Q}}}[x] \cap \mathbb{Q}[x]$ since $\mathcal{O}_{\bar{\mathbb{Q}}}$ is a ring. Since $\mathcal{O}_{\bar{\mathbb{Q}}} \cap \mathbb{Q} = \mathbb{Z}$ we have claim (2). Claim (3) now follows by taking specific coefficients. For (4) note that for $\alpha \in OK$, $\frac{N\alpha}{\alpha} = \prod_{\mu \neq 1} \mu\alpha \in \mathcal{O}_{\bar{\mathbb{Q}}} \cap K = OK$. Thus $\alpha | N\alpha$ in OK, so if $N\alpha$ is invertible so is α. Conversely, if $\alpha\beta = 1$ then $N\alpha N\beta = 1$. □

LEMMA 178. *Let $\alpha \in K$. Then there is $m \in \mathbb{Z}$ so that $m\alpha \in \mathcal{O}_K$.*

PROOF. Let $f = \sum_{i=0}^d a_i x^i \in \mathbb{Q}[x]$ be the (monic) minimal polynomial of α. Then $\sum_{i=0}^d m^{d-i} a_i (m\alpha)^i = 0$. If m is large enough then $m^{d-i} a_i \in \mathbb{Z}$ for all $0 \leq i < d$. □

COROLLARY 179. *There exists a basis of K consisting of elements of $\mathcal{O}_K$.*

From now on assume that K is a *number field*, that is a finite extension of $\mathbb{Q}$. We write $n = [K : \mathbb{Q}]$.

LEMMA 180. *The quadratic form $(x,y) \mapsto \mathrm{Tr}(xy)$ is non-degenerate.*

PROOF. $\mathrm{Tr}(x \cdot x^{-1}) = n$. □

PROPOSITION 181. *There exist a basis $\{\omega_i^*\}_{i=1}^n \subset K$ so that $\mathcal{O}_K \subset \oplus_i \mathbb{Z}\omega_i^*$.*

PROOF. Take $\{\omega_i^*\}$ be the basis dual to a basis contained in $\mathcal{O}_K$ w.r.t. the trace form. □

CONCLUSION 182. The $\mathbb{Z}$-module $\mathcal{O}_K$ embeds in $\mathbb{Z}^n$ and contains a copy of $\mathbb{Z}^n$.

The structure theorem of finitely generated abelian groups now immediately shows that $\mathcal{O}_K =\simeq \mathbb{Z}^n$ as Z-modules. We give a self-contained proof of this fact.

LEMMA 183. *Let $f \colon \mathbb{Z}^r \to \mathbb{Z}^s$ be an isomorphism of Z-modules. Then $r = s$.*

PROOF. In short: $f \otimes_{\mathbb{Z}} 1 \colon \mathbb{Z}^r \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Z}^s \otimes_{\mathbb{Z}} \mathbb{Q}$ is an isomorphism of vector spaces. In detail, define $\tilde{f} \colon \mathbb{Q}^r \to \mathbb{Q}^s$ by setting $\tilde{f}(\underline{v}) = \frac{1}{m} f(m\underline{v})$ for any $\underline{v} \in \mathbb{Q}^r$ and $m \in \mathbb{Z} \setminus \{0\}$ so that $m\underline{v} \in \mathbb{Z}^r$. This is easily seen to be a well-defined isomorphism of vector spaces. □

DEFINITION 184. A $\mathbb{Z}$-module M is called *free* if $M \simeq \mathbb{Z}^r$ for some r. In that case we call r the *rank* of M.

PROPOSITION 185. *Let A be a free Z-module of finite rank, $B < A$ a Z-submodule. Then B is free and* $\operatorname{rank}(B) \leq \operatorname{rank}(A)$.

PROOF. By induction on $r = \operatorname{rank}(A)$. If $r = 1$ then $A \simeq \mathbb{Z}$ and this is problem 1(a) of Problem Set 1. Assume then that $A = \oplus_{i=1}^{r+1} \mathbb{Z} x_i$ and let $A' = \oplus_{i=1}^{r} \mathbb{Z} x_i$, $B' = B \cap A'$. By induction, B' is free of rank at most r. Also, B/B' embeds in $A/A' \simeq \mathbb{Z}$ so by the case of rank 1, B/B' is free of rank 0 or 1. In the first case $B \simeq B'$ and we are done. Otherwise, let $y \in B$ project to a generator of B/B'. Then the sum $B' + \mathbb{Z}y$ is direct and equal to B, finishing the proof. □

THEOREM 186. *(Integral Basis Theorem) Let $[K : \mathbb{Q}] = n$. Then is $\mathcal{O}_K$ a free $\mathbb{Z}$-module of rank n.*

PROOF. Applying Proposition 185 to the inclusion of Proposition 181 we see that $\mathcal{O}_K$ is free of rank at most n. Applying Proposition 185 to the inclusion of Corollary 179 show that $\mathcal{O}_K$ has rank at least n. □

5.3. Unique factorization (30/11/09)

Fix a number field K of degree n.

PROPOSITION 187. *(Ideals of $\mathcal{O}_K$) Fix a non-zero proper ideal $\mathfrak{a} \lhd \mathcal{O}_K$.*

1. *$\mathfrak{a} \cap \mathbb{Z}$ is a non-zero proper ideal of $\mathbb{Z}$.*
2. *$[\mathcal{O}_K : \mathfrak{a}] < \infty$.*
3. *$\mathfrak{a}$ is finitely generated. In fact,* $\operatorname{rank}_{\mathbb{Z}} \mathfrak{a} = n$.
4. *If $\mathfrak{a}$ is prime then it is maximal, and $\mathfrak{a} \cap \mathbb{Z} = (p)$ for a prime number p.*

PROOF. $\mathfrak{a} \cap \mathbb{Z}$ is certainly an ideal. It does not contain 1 since $\mathfrak{a}$ doesn't, and is not zero since it contains $N\alpha$ for all $\alpha \in \mathfrak{a}$. Setting $a \cap \mathbb{Z} = (m)$ we have $m\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$. This shows that $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank n, and that $[\mathcal{O}_K : \mathfrak{a}] \leq [\mathcal{O}_K : m\mathcal{O}_K] = m^n$.

If $\mathfrak{a}$ is prime then $\mathcal{O}_K/\mathfrak{a}$ is a finite integral domain, hence a field, so $\mathfrak{a}$ is maximal. $\mathbb{Z}/(\mathbb{Z} \cap \mathfrak{a})$ is also an integral domain since it embeds in $\mathcal{O}_K/\mathfrak{a}$. □

DEFINITION 188. An $\mathcal{O}_K$-submodule $\mathfrak{a} \subset K$ is a *fractional ideal* if there is $\alpha \in K^\times$ so that $\alpha\mathfrak{a} \subset \mathcal{O}_K$.

Given fractional ideals $\mathfrak{a}, \mathfrak{b}$ let $\mathfrak{ab}$ be the module generated by all products xy, $x \in \mathfrak{a}$, $y \in \mathfrak{b}$. Multiplication of fractional ideals is commutative and associative, and has the unit $(1) = \mathcal{O}_K$. We call a fractional ideal *invertible* if it is invertible in this commutative semigroup.

LEMMA 189. *Every proper ideal of $\mathcal{O}_K$ contains a product of primes.*

PROOF. Let $\mathfrak{a}$ be a maximal counterexample. It is not prime so there are $x, y \in \mathcal{O}_K \setminus \mathfrak{a}$ with $xy \in \mathfrak{a}$. Then $(\mathfrak{a}, x)(\mathfrak{a}, y) = \mathfrak{a}$, a contradiction. □

PROPOSITION 190. *Let $\mathfrak{p} \lhd \mathcal{O}_K$ be prime. Then $\mathfrak{p}^{-1} \stackrel{def}{=} \{x \in K \mid x\mathfrak{p} \subset \mathcal{O}_K\}$ is a fractional ideal properly containing $\mathcal{O}_K$. In particular, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.*

PROOF. Let $p \in \mathbb{Z}$ be the prime lying below $\mathfrak{p}$. Let $x, y \in \mathfrak{p}^{-1}$ and $\alpha \in \mathcal{O}_K$. First, $(\alpha x + y)\mathfrak{p} \subset x\mathfrak{p} + y\mathfrak{p} \subset \mathcal{O}_K + \mathcal{O}_K = \mathcal{O}_K$. Second, $(px)\mathfrak{p} = \subset p\mathcal{O}_K \subset \mathfrak{p}$. Since $\mathfrak{p}$ is a finitely generated $\mathbb{Z}$-module, it follows that px is integral over $\mathbb{Z}$, and hence that $p \cdot \mathfrak{p}^{-1} \subset \mathcal{O}_K$. To see that $\mathfrak{p}^{-1} \supsetneq \mathcal{O}_K$ fix a non-zero $x \in \mathfrak{p}$. Then $x\mathcal{O}_K \subset \mathfrak{p}$ and hence contains a product of prime ideals. Let $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ be a

minimal such product. Since $\mathfrak{p}$ contains this product, it contains one factor, and hence equal to it (all primes are maximal). Let $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus x\mathcal{O}_K$ (this exists by minimality of r). Then $b\mathfrak{p} \subset x\mathcal{O}_K$ so $\frac{b}{x}\mathfrak{p} \subset OK$ but $\frac{b}{x} \notin \mathcal{O}_K$. Finally, $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathcal{O}_K$. Since $\mathfrak{p}\mathfrak{p}^{-1}$ is an $\mathcal{O}_K$-submodule of $\mathcal{O}_K$ and $\mathfrak{p}$ is a maximal ideal one side must be an equality. If $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ held then every $y \in \mathfrak{p}^{-1}$ would be integral, a contradiction. □

THEOREM 191. *All ideals of $\mathcal{O}_K$ are invertible; every ideal can be uniquely written in the form $\prod_{i=1}^r \mathfrak{p}_i^{e_i}$ with $\mathfrak{p}_i$ prime and $e_i \in \mathbb{Z}_{>0}$. $\mathfrak{a}|\mathfrak{b}$ in the monoid of ideals iff $\mathfrak{b} \subset \mathfrak{a}$.*

PROOF. First, let $\mathfrak{a} \lhd \mathcal{O}_K$ be a proper ideal and let $\mathfrak{a} \subset \mathfrak{p} \lhd \mathcal{O}_K$ be a maximal ideal. Then $\mathfrak{p}^{-1}\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$ and $\mathfrak{p}^{-1}\mathfrak{a} \neq \mathfrak{a}$ since $\mathfrak{p}^{-1} \not\subset \mathcal{O}_K$.

Now let $\mathfrak{a} \lhd \mathcal{O}_K$ be maximal among the non-invertible non-zero ideals. Then $\mathfrak{p}^{-1}\mathfrak{a}$ is invertible, and hence so is $\mathfrak{a}$. Similarly, let $\mathfrak{a}$ be maximal ideal without representation as a product of primes. Then $\mathfrak{p}^{-1}\mathfrak{a}$ can be written as such a product, and hence so can $\mathfrak{a}$. Finally, let $\prod_{i=1}^r \mathfrak{p}_i = \prod_{j=1}^t \mathfrak{q}_j$. Then $\mathfrak{p}_r$ contains the product on the left, hence the product on the right, hence equal to one of the factors. Multiplying by $\mathfrak{p}_r^{-1}$ the claim follows by induction on r.

If $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ then certainly $\mathfrak{b} \subset \mathfrak{a}$. Conversely, if $\mathfrak{b} \subset \mathfrak{a}$ then $\mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}_K$. □

COROLLARY 192. *Every fractional ideal is invertible, so that the fractional ideals form a group. Every element of this group has a unique representation in the form $\prod_{i=1}^r \mathfrak{p}_i^{e_i}$ with $e_i \in \mathbb{Z} \setminus \{0\}$.*

DEFINITION 193. Call a fractional ideal *principal* if it is of the form $\alpha\mathcal{O}_K$ for some $\alpha \in K^\times$. Say that two fractional ideals $\mathfrak{a}, \mathfrak{b}$ are *in the same class* if $\mathfrak{a}\mathfrak{b}^{-1}$ is principal (note that every fractional ideal is in the same class as an ideal by definition). The principal fractional ideals form a subgroup of the group of fractional ideals. The *class group* of K is the quotient $\mathrm{Cl}(K)$ of the group of ideals by the group of principal ideals. It measures the failure of unique factorization.

THEOREM 194. *(Dedekind) $\mathrm{Cl}(K)$ is a finite group.*

PROPOSITION 195. *(Kummer) Let $\alpha, \beta \in \mathcal{O}_K$ be relatively prime and let their product be a pth power, where $p \nmid \#\mathrm{Cl}(K)$. Then α, β are pth powers up to units.*

PROOF. Say that $\alpha\beta = \gamma^p$. Then $(\alpha)(\beta) = (\gamma)^p$ and so $(\alpha), (\beta)$ are pth powers in the monoid of ideals, say $(\alpha) = \mathfrak{a}^p$, $(\beta) = \mathfrak{b}^p$. But then the classes of $\mathfrak{a}$, $\mathfrak{b}$ are trivial in the class group. □

DEFINITION 196. (Kummer) Call the odd prime p *regular* if $p \nmid \mathrm{Cl}(\mathbb{Q}(\zeta_p))$.

THEOREM 197. *(Kummer) Let p be a regular prime. Then $x^p + y^p + z^p = 0$ has only the trivial solution $x = y = z = 0$.*

PROOF. We consider the equation $x^p - y^p = z^p$ in $\mathbb{Z}[\zeta_p]$. We have there $\prod_{j=0}^{p-1}(x - \zeta_p^j y) = z^p$. □

5.4. Splitting of primes (2/12/09)

DEFINITION 198. If $\mathfrak{p} \lhd \mathcal{O}_K$ is a non-zero prime ideal and $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ we say that $\mathfrak{p}$ *divides* p or *lies above it*, and write $\mathfrak{p} \mid p$.

We have seen that every prime of $\mathcal{O}_K$ lies above a unique prime of $\mathbb{Z}$. There is a partial converse.

LEMMA 199. *Let $p\mathbb{Z}$ be a prime of $\mathbb{Z}$. Then there exist primes $\mathfrak{p}$ of $\mathcal{O}_K$ lying above (p).*

PROOF. let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ containing the ideal $p\mathcal{O}_K$. Then $\mathfrak{p} \cap \mathbb{Z}$ is a proper ideal containing the maximal ideal (p) hence equal to it. □

Next, let $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$ for $g = g(\mathfrak{p})$. Then $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}_i$ is a finite extension of $\mathbb{Z}/p\mathbb{Z}$, say of degree f_i. By the CRT, we have

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \prod_{i=1}^{g} \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

Now $\dim_{k_\mathfrak{p}} \mathfrak{p}^r/\mathfrak{p}^{r+1} = 1$ so $\dim_{k_p} \mathcal{O}_K/\mathfrak{p}^e = e$ and $\dim_{\mathbb{F}_p} \mathcal{O}_K/\mathfrak{p}_i^{e_i} = e_i f_i$. It follows that

$$n = \sum_{i=1}^{g} e_i f_i.$$

DEFINITION 200. Say *p ramifies* in K if $e_i \geq 2$ for some i.

THEOREM 201. *p ramifies iff $p|d_K$. In particular, there are only finitely many ramified primes.*

When $K/\mathbb{Q}$ is Galois, we have more structure. Note that if $\sigma \in G = \mathrm{Gal}(K:\mathbb{Q})$ and $\mathfrak{p}$ is a prime ideal then so is $\sigma(\mathfrak{p})$ and both have the same intersection with $\mathbb{Z}$.

THEOREM 202. $\mathrm{Gal}(K/\mathbb{Q})$ *acts transitively on the set of primes lying above p.*

In particular, f_i, e_i are constant and we have $n = e(p)f(p)g(p)$.

DEFINITION 203. $D_\mathfrak{p} = \{\sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$. This group acts on $\mathcal{O}_K$ fixing $\mathfrak{p}$ setwise hence on $k_\mathfrak{p}$ fixing $\mathbb{Z}/p\mathbb{Z}$ element-wise, giving a homomorphism $D_\mathfrak{p} \to \mathrm{Gal}(k_\mathfrak{p}:\mathbb{F}_p)$. Write $I_\mathfrak{p}$ for the kernel of this map.

THEOREM 204. $D_\mathfrak{p}$ *surjects onto the Galois group of the residue field.*

COROLLARY 205. $[G:D_\mathfrak{p}] = g(p)$ *by transitivity,* $[D_\mathfrak{p}:I_\mathfrak{p}] = f(p)$ *by surjectivity. It then follows that* $\#I_\mathfrak{p} = e(p)$ *since* $efg = n$.

If p is unramified then $e = 1$ so for each $\mathfrak{p}$ lying above p there is a unique element mapping to the Frobenius element of $k_\mathfrak{p}$. Write Frob_p for the resulting conjugacy class.

THEOREM 206. *(Chebotarev density theorem) Let $C \subset G$ be a conjugacy class. Then*

$$\frac{\#\left\{p \leq x \mid p \text{ unramified and } \mathrm{Frob}_p = C\right\}}{\#\{p \leq x\}} \xrightarrow[x\to\infty]{} \frac{\#C}{\#G}.$$

Bibliography

[1] Arthur Cayley. Desiderate and suggestions: No. 1. the theory of groups. *Amer. J. Math.*, 1(1):50–52, 1878.

[2] Ian Stewart. *Galois Theory*. Chapman & Hall/CRC Mathematics. Chapman & Hall/CRC, Boca Raton, FL, third edition, 2004.