Math 251 - Algebra 1

Lectures by Dan Abramovich
Notes by Zev Chonoles

Brown University, Fall 2008

Introduction

Math 251 is one of the courses offered for mathematics graduate students at Brown University. It is the first of two courses in the year-long algebra sequence. I took these notes while auditing the course as a freshman.

The notes are handwritten because this was before I started live-TeXing. I may eventually get around to typing these notes properly.

I am responsible for all faults in this document, mathematical or otherwise; any merits of the material here should be credited to the lecturer, not to me.

Please email any corrections or suggestions to `chonoles@math.uchicago.edu`.

Lecture 1 (2008-09-05)

9/5/08

Sources for groups: $\mathrm{Aut}(X)$ for a set X, $GL(V)$ for a vector space V

Kernel of $\det : GL_n(k) \to k^\times$ is $SL_n(k)$, a group since kernel of a homomorphism is always a subgroup

Let $A \in M_{n\times n}(\mathbb{R})$; when does A preserve lengths? $|v| = (v\cdot v)^{\frac{1}{2}}$
i.e. when is $|Av| = |v|$ $\forall v \in \mathbb{R}^n$? If it does then since A preserves the length of all $v, w \in \mathbb{R}^n$, it must also preserve $|v+w|$ and $|v-w|$, so

$$|A(v+w)| = |v+w|, \quad |A(v-w)| = |v-w) \quad \Rightarrow$$
$$|A(v+w)|^2 = (v+w)\cdot(v+w) = |v|^2 + 2(v\cdot w) + |w|^2, \quad |A(v-w)|^2 = (v-w)\cdot(v-w) = |v|^2 - 2(v\cdot w) + |w|^2 \Rightarrow$$

also preserves the difference of these two quantities, $4(v\cdot w)$ and thus $v\cdot w$.

So $Av \cdot Aw = v\cdot w$ $\forall v, w \in \mathbb{R}^n$. $Av\cdot Aw = (Av)^T \overset{\curvearrowleft}{Aw}$, thinking as a column vector, and thus $Av\cdot Aw = v^T A^T A w$, but if $Av \cdot Aw = v\cdot w$, $v^T A^T A w = v^T w$ so

$$\text{matrix preserves length} \Leftrightarrow A^T A = I$$

set of such Matrices is $O_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) : A^T A = I\}$, clearly a group since composition of length preserving transformations is length-preserving

If we look at $\det : O_n(\mathbb{R}) \to \mathbb{R}^\times$, $\det(A^T)\det(A) = 1$, but $\det(A) = \det(A^T)$, so $\det(A) = \pm 1$. We define $SO_n(\mathbb{R}) = SL_n(\mathbb{R}) \cap O_n(\mathbb{R})$, which is also a group since the intersection of subgroups is a subgroup, and also because $SO_n(\mathbb{R}) = \mathrm{Ker}(\det : O_n(\mathbb{R}) \to \mathbb{R}^\times)$, and Kernel of a homomorphism is always a subgroup.

An action of G on X is $G\times X \Rightarrow X$ with $(g_1 g_2)x = g_1(g_2 x)$ and $ex = x$.

Observation:

$$\begin{tikzcd} \text{action of } G \text{ on } X \quad G\times X \xrightarrow{a} X \arrow[d, leftrightarrow, "\text{bijection}"] \\ \text{group homomorphism} \quad p : G \to \mathrm{Aut}(x) \end{tikzcd}$$

- Given a homomorphism $p : G \to \mathrm{Aut}(X)$, define $a_p : G\times X \Rightarrow X$ to be $a_p(g,x) = p(g)x$. This is an action (exercise).
- Given an action $a : G\times X \to X$, define $p_a : G \to \mathrm{Aut}(X)$ to be $g \mapsto (x \mapsto \overbrace{gx}^{g \text{ acting on } x \text{ by } a})$ This is a homomorphism (exercise)
- $p_{(a_p)} = p$, $a_{(p_a)} = a$ (exercise)

Lecture 2 (2008-09-08)

Let $a: G \times X \to X$ be an action. 9/8/08

trivial action: $gx = x \quad \forall g \in G, x \in X$ (or equivalently, $\rho_a: G \to \mathrm{Aut}(X)$, $g \mapsto id$)

effective action: $\forall g \in G, g \neq e, \exists x \in X: gx \neq x$ (or equivalently, $\rho_a: G \to \mathrm{Aut}(X)$, $\mathrm{Ker}(\rho_a) = \{e\}$)

transitive action: $\forall x, y \in X, \exists g \in G: gx = y$

Note: simply transitive $\Rightarrow$ effective

simply transitive: $\forall x, y \in X, \exists! g \in G: gx = y$

$\forall$ groups G, $\exists$ a set X which is simply transitively acted on by G (trivial example: G acting on itself by left multiplication)

Choose an action $G \times X \to X$. The set X^g = the fixed points of g under the action and X^G = the fixed points of the entire action

$\mathrm{Stab}(x) = \{g \in G : gx = x\}$ (stabilizer)

$Gx = \{gx : g \in G\}$ (orbit)

Lemma: $\forall x, y \in X$, either $Gx = Gy$ or $Gx \cap Gy = \phi$

Proof: It suffices to prove $Gx \cap Gy \neq \phi \Rightarrow Gx = Gy$. To do this we prove that if $z \in Gx$, $Gz = Gx$ (so that if $z \in Gx, Gy$, then $Gx = Gz = Gy$). $z \in Gx \Rightarrow \exists g \in G: z = gx$, and suppose $y \in Gz$; then $y = hz$ for some $h \in G$, so $y = h(gx) = (hg)x$ by the action axioms, so $Gz \subset Gx$ (and the reverse inclusion by symmetry). We are done.

Thus $X = \bigsqcup Gx_i$, x_i's being representatives of distinct orbits.

We can also have right actions $X \times G \to X$, with $xe = x$, $x(gh) = (xg)h$.

Right actions may be transformed into left actions by G^{op}, which has the same elements, identity, and inverses, but in G^{op}, $g * h = hg$.

$X \times G \to X$ is a right action $\Rightarrow$ $G^{op} \times X \to X$ is a left action

$x, g \mapsto xg \longrightarrow g, x \mapsto g * x = xg$

Also, $\underset{g \mapsto g^{-1}}{G \cong G^{op}}$ (which is the identity map if G is abelian)

We can also have $G \times G \to G$ with $g, h \mapsto ghg^{-1}$, written ${}^g h$ so that ${}^g(hk) = g(hk)g^{-1} = ghg^{-1}gkg^{-1} = {}^g h \, {}^g k$.

The quotient (or orbit) space $G\backslash X$ is the set of orbits $\{Gx : x \in X\}$. We can restate orbit decomposition as $X = \bigsqcup_{\bar{x} \in G\backslash X} \bar{x}$

Lecture 3 (2008-09-10)

If $G \times X \to X$, we can map $X \to {}_G\backslash^X$ by $x \mapsto Gx$. 9/10/08

For $H < G$ (that is, H a subgroup of G), ${}_H\backslash^G = \{Hg : g \in G\}$, the set of right cosets, and $G/H = \{gH : g \in G\}$, the set of left cosets.

Clearly $|{}_H\backslash^G| = |G/H|$ (since we can bbiject $\begin{array}{l} G/H \to {}_H\backslash^G \\ gH \mapsto Hg^{-1} \end{array}$, because $k \in gH \Rightarrow k^{-1} \in Hg^{-1}$, because $k \in gH \Rightarrow k = gh$ for some $h \in H \Rightarrow k^{-1} = h^{-1}g^{-1}$, but $h^{-1} \in H$ since $H < G$, so $k^{-1} \in Hg^{-1}$)

Furthermore, $|G| = |H| \cdot |G/H|$, since we can biject $G/H \times H \to G$ (letting $G/H = \{g_\alpha H : \alpha \in G/H\}$, with g_α a representative group element, $(g_\alpha H, h) \mapsto g_\alpha h$.

Corollary. For $H < G$, $|H| \,\big|\, |G|$ and thus $\operatorname{ord}(g) = |\langle g \rangle| \,\big|\, |G|$.

$\begin{array}{l} G \times G/H \to G/H \\ (g', gH) \mapsto (g'g)H \end{array}$ is a transitive action

A G-set is a set X which is acted on by G. Let X_1, X_2 be G-sets. We say $f : X_1 \to X_2$ is a G-set homomorphism if $\forall g \in G, x \in X_1$, $f(gx) = g f(x)$

Theorem. Let $G \circlearrowright X$ be a transitive action, and let $x \in X$. Then $X \simeq G/\mathrm{Stab}(x)$ is an isomorphism of G-sets.

Proof. (separate page)

Proposition. If X is a transitive G-set, letting $y = gx$, then $\mathrm{Stab}(y) = g\,\mathrm{Stab}(x) g^{-1}$

Proof. We need $g\,\mathrm{Stab}(x) = \mathrm{Stab}(y) g$. Let $h \in \mathrm{Stab}(x)$. Then $hx = x$, and thus $(hg^{-1})(gx) = x$, $(ghg^{-1})(gx) = gx$, and $(ghg^{-1})y = y$, so $\forall h \in \mathrm{Stab}(x)$, $ghg^{-1} \in \mathrm{Stab}(y)$, so $g\,\mathrm{Stab}(x) g^{-1} \subset \mathrm{Stab}(y)$ and we can prove the reverse inclusion similarly.

Transitive action: $\forall x, y \in X, \exists g \in G : gx = y$ 9/10/08

For $H < G$, $G/H = \{gH : g \in G\}$ (left cosets)

A G-set is a set X which is acted upon by a group G.

For G-sets X_1, X_2, $f : X_1 \to X_2$ is a G-set homomorphism iff

$\forall g \in G, x \in X_1, f(gx) = gf(x)$

For a G-set X, $x \in X$, $Stab(x) = \{g \in G : gx = x\}$

Theorem. Let $G \times X \to X$ be a transitive action, and $x \in X$.

$X \simeq G/Stab(x)$, as an isomorphism of G-sets.

Proof. Let $S = Stab(x)$ for our chosen $x \in X$. We want a mapping $f : G/S \to X$, $gS \mapsto gx$, which is a) well-defined, b) a G-set homomorphism, and c) an isomorphism.

a) Let $g \in G$, $s \in S$. Then $gS = (gs)S$, that is, they are different representatives of the same element of G/S. We want to show $gx = (gs)x$; since $s \in S$, $sx = x$, and thus $(gs)x = g(sx)$, by action axioms, which $= gx$.

b) To be a G-set homomorphism, we need $\forall g_1, g_2 \in G$, $s \in S$, $f((g_1g_2)S) = g_1 f(g_2S)$. $f(g_1g_2)S) = (g_1g_2)x = g_1(g_2x)$, by action axioms, which $= g_1 f(g_2S)$.

c) Lemma: A G-set homomorphism $f : X_1 \to X_2$ is an isomorphism iff it is a bijection between X_1 and X_2 as sets.

Proof: If $f : X_1 \to X_2$ is an isomorphism, $\exists \phi : X_2 \to X_1$ such that $\phi \circ f = f \circ \phi = id$. Immediately we have that f is bijective. However, if $f : X_1 \to X_2$ is a bijection between X_1 and X_2 only as sets, we know $\exists \phi : X_2 \to X_1$ such that $\phi \circ f = f \circ \phi = id$ as sets, but we still need to show ϕ is also a G-set homomorphism, that is, $\forall g \in G$, $x \in X_2$, $\phi(gx) = g\phi(x)$. Noting that $gx = f(\phi(gx))$, and $gx = gf(\phi(x)) = f(g\phi(x))$, we have $f(\phi(gx)) = f(g\phi(x))$ and therefore $\phi(gx) = g\phi(x)$, our desired result.

With this Lemma, all we need to do is prove $f : X_1 \to X_2$ is bijective. Let $y \in X$; by hypothesis, f is a transitive action, so $\exists g \in G : y = gx$, or equivalently, $y = f(gS)$, so that all $y \in X$ are mapped to by a $gS \in G/S$. Thus f is surjective. To prove injectivity, suppose $g_1x = g_2x$; we want $g_1S = g_2S$. We have $g_2^{-1}g_1x = x$, so $g_2^{-1}g_1 \in S$; thus, $\forall s_1 \in S$, $g_2^{-1}g_1s_1 = s_2 \in S$, or equivalently, $\forall s_1 \in S$, $g_1s_1 = g_2s_2$ for some $s_2 \in S$. Thus $g_1S = g_2S$.

Lecture 4 (2008-09-12)

9/12/08

previous class:

X is a transitive G-set, $x \in X$

$$G/\mathrm{Stab}(x) \simeq X$$

$$gS \longmapsto gx$$

If $x, y \in X$, $y = gx$,

$$\mathrm{Stab}(y) = g\,\mathrm{Stab}(x)\,g^{-1}$$

If $H < G$, and G/H is finite, $[G:H] = |G/H|$ (called the index of H in G)

Let X be a transitive G-set. $|X| = [G : \mathrm{Stab}(x)]$ for any $x \in X$

(Corollary to)

Prop: If X is a finite G-set, then

$$|X| = \sum_{\overline{x} \in X/G} [G : \mathrm{Stab}(x)]$$

{distinct orbits}

Proof. $X = \bigsqcup_{\overline{x} \in X/G} \overline{x}$, with $\overline{x} = Gx$ for some representative $x \in G$

$$|X| = \sum |\overline{x}| = \sum [G : \mathrm{Stab}(x)]$$

Ex. If $X = G$, $G \times X \to X$

$$g, x \mapsto gxg^{-1}$$

Orbit(x) = conjugacy class of x, written (x), set of conjugacy classes written $Cl(G)$

Stab(x) = centralizer of x, since $gxg^{-1} = x \Rightarrow gx = xg$, written $C(x)$

Theorem. $|G| = |Z(G)| + \sum_{\substack{(g) \in Cl(G) \\ \text{with } g \notin Z(G)}} [G : C(g)]$

$G = X$ $\qquad$ X/G becomes $Cl(G)$

$$|G| = \sum_{\overline{x} \in X/G} [G : \mathrm{Stab}(x)] = \sum_{g \in Z(G)} [G : C(g)] + \sum_{\substack{(g) \in Cl(G) \\ g \notin Z(G)}} [G : C(g)]$$

Since each $z \in Z(G)$ is a representative of a distinct orbit, i.e., itself, since $gzg^{-1} = gg^{-1}z = z$ $\forall g \in G$, so z only ever gets set to itself. But equivalently, z's centralizer $C(g) = G$, so $[G : C(g)] = 1$ for each $g \in Z(G)$, and

$$|G| = |Z(G)| + \sum_{\substack{(g) \in Cl(g) \\ g \notin Z(g)}} [G : Cl(g)]$$

Theorem. Suppose p is prime, $|G| = p^n$. Then $|Z(G)| > 1$.

Proof. $|G| = p^n = |Z(G)| + \sum_{\substack{(g)\in Cl(G) \\ g \notin Z(G)}} [G : C(g)]$

But since $[G : C(g)] = |G|/|C(g)|$, and $|C(g)| \neq 1$ since the sum is over $g \notin Z(G)$, so $p \mid [G : C(g)]$ for each term in the sum, so $p \mid |Z(G)|$. But $Z(G) \neq \phi$, since $e \in Z(G)$, so $|Z(G)|$ is a multiple of p.

Def. Let $G \circlearrowright X$. The inertia set of X, $IX = \{(g,x) : gx = x\}$ (so that $IX \subset G \times X$)

To count elements of a product, in general we do "double summation", fix an x, count each element associated with it, then let x vary. Changing the order of summation can lead to interesting results.

$$\sum_{x\in X} \#\{g \in G : gx = x\} = \sum_{x \in X} |Stab(x)|$$

$$\sum_{g\in G} \#\{x \in X : gx = x\} = \sum_{g\in G} |X^g|$$, where X^g is the set of fixed points under left-multiplication by g.

so $\sum_{x\in X} |Stab(x)| = \sum_{g \in G} |X^g|$

But we can break up the left sum into distinct orbits,

$\sum_{\bar{x} \in G\backslash X} \sum_{x \in \bar{x}} |Stab(x)|$, and for each $x \in \bar{x}$, $|Stab(x)|$ is the same, so we have

$\sum_{\bar{x} \in G\backslash X} |\bar{x}| \cdot |Stab(x)|$; but we also know $|\bar{x}| = |G|/|Stab(x)|$ for any $x \in \bar{x}$,

so it's really equivalent to $\sum_{\bar{x} \in G\backslash X} \frac{|G|}{|Stab(x)|} |Stab(x)| = |G| \sum_{x \in G\backslash X} 1 = |G\backslash X| \cdot |G|$

Substituting back in,

$|G\backslash X|$, number of orbits, $= \frac{1}{|G|} \cdot \sum_{g\in G} |X^g|$

9/12/08

Let $F = \{\text{faces of cube}\}$, $|F| = 6$

$G =$ group of rigid motions of cube (oriented)

$\tilde{G} =$ group of all symmetries (i.e., allowing reflections)

$G \times F \to F$ is transitive, since any face can be sent to any other

$|F| = [G : \mathrm{Stab}(f)]$ for any $f \in F$

$= |G| / |\mathrm{Stab}(f)|$ $\quad \mathrm{Stab}(f) = 4$

$|G| = 24$, similarly $|\tilde{G}| = 48$

Let $k \in \mathbb{N}$, $\bar{k} = \{1, \dots, k\}$ be colors

$X =$ set of k-colorings of $F = \bar{k}^F$

so $|X| = k^6$ $\quad c : F \to \bar{k}$ is a coloring $c \in X$

$f \mapsto c(f)$

for $g \in G$, $cg = f \mapsto c(gf)$

but this is a right action since for $g, g' \in G$,

$(cg)g' = c(gg')$ so $((cg)g')(x) = (cg)(g'x) =$

$c(gg'x) = c(gg')(x)$

but we can turn this into a left action by $gc = cg^{-1}$

When we want # of distinct colorings up to motion by G, we really want # of orbits, so we use $\left|X/G\right| = \frac{1}{|G|} \sum_{g \in G} |X^g|$

Lecture 5 (2008-09-15)

9/15/08

A subgroup $K < G$ is normal if $\forall g \in G$, $gKg^{-1} = K$ (i.e. $gK = Kg$). We write $K \trianglelefteq G$.

Examples. $G \trianglelefteq G$, $\{e\} \trianglelefteq G$, $Z(G) \trianglelefteq G$, and if $\phi : G \to H$ is a homomorphism, $Ker(\phi) \trianglelefteq G$

Remark. If $K \trianglelefteq G$, G/K has a group structure by $(g_1K)(g_2K) = (g_1g_2)K$.

<u>FIRST ISO</u>. If $\phi : G \to H$ is a homomorphism, $G/Ker(\phi) \simeq Im(\phi)$
$gKer(\phi) \mapsto \phi(g)$

$$\begin{tikzcd}
g \arrow[d] & G \arrow[r, "\phi"] \arrow[d] & H \\
gKer(\phi) & G/Ker(\phi) \arrow[ur, dashed] &
\end{tikzcd}$$

$\}\exists!$ homomorphism here, namely $gKer(\phi) \mapsto \phi(g)$

Definition. $HK = \{hk : h \in H, k \in K\}$ for $H, K < G$. Not always a subgroup.

Definition. For $K < G$, $N_G(K) = \{g \in G : gKg^{-1} = K\}$

Lemma. $N_G(K) < G$, and $K \trianglelefteq N_G(K)$

Proof. Second part, trivial. First part, letting $G \circlearrowright S(G)$, the set of all subgroups of G, with $(g, H) \mapsto gHg^{-1}$, then $N_G(K) = Stab(K)$ (thinking of $K \in S(G)$), and $Stab < G$ always.

Lemma. If $H < N_G(K)$, $HK < G$

Proof. Let $h_1k_1, h_2k_2 \in HK$. Then we want $(h_1k_1)(h_2k_2) \in HK$; since $H < N_G(K)$, $h_2K = Kh_2$, so $h_1\underbrace{k_1h_2}_{\in Kh_2}k_2 = \underbrace{(h_1h_3)}_{\in H}\underbrace{(k_1k_3)}_{\in K}$ for whatever $h_3k_3 = k_1h_2$.

<u>SECOND ISO</u>. If $H, K < G$, and $H < N_G(K)$, then

a) $K \trianglelefteq HK$, b) $H \cap K \trianglelefteq H$, and c) $HK/K \simeq H/H\cap K$

<u>THIRD ISO</u>. If $H, K \trianglelefteq G$, with $H < K$, then

a) $H \trianglelefteq K$, b) $K/H \trianglelefteq G/H$, and c) $(G/H)/(K/H) \simeq G/K$

Theorem. If $N \trianglelefteq G$, then there is a bijection between $\{$subgroups of $G/N\}$ and $\{$subgroups of G containing $N\}$ with $N < H < G \quad \overline{H} < G/N$
q, the quotient map
, and H ends up being $q^{-1}(\overline{H})$, the preimage of $\overline{H}$

Theorem (Cauchy). For G abelian, p a prime, if $p \mid |G|$, the $\exists g \in G$ with $ord(g) = p$.

Lemma. Theorem holds if G is cyclic.
Proof. If $G = \langle g \rangle$, and $|G| = p \cdot k$ for some k, $ord(g^k) = p$.

Proof. Let $h \in G$, $h \neq e$, $H = \langle h \rangle$. If $p \mid |H|$, we're done by the Lemma. If $p \nmid |H|$, then $p \mid |G/H|$ since $p \mid |G| = |H| \cdot |G/H|$. Thus by the Lemma, $\exists \overline{g} \in G/H$ with $ord(\overline{g}) = p$. If $G \xrightarrow{q} G/H$ is the quotient map, and letting $g \in q^{-1}(\overline{g})$, then $ord(g)$ is divisible by p and we are done by the Lemma

Lecture 6 (2008-09-17)

9/17/08

Sylow's Theorem: G finite, $p^u \| |G|$, $n_p = |Syl_p(G)|$

1) $Syl_p(G) = \phi$

2) $P \in Syl_p(G)$

$H < G$, $|H| = p^e$ for some $\ell \Rightarrow$

$\exists g \in G : H < gPg^{-1}$

equivalently,

2(i) $\exists P' \in Syl_p(G) : H < P'$

2(ii) $\forall P, P' \in Syl_p(G)$

$\exists g : gPg^{-1} = P'$

3) $n_p \equiv 1 \mod p$

$n_p \mid \frac{|G|}{p^u}$

\# of fixed points under H

Lemma. Let H be a p-group, $H \curvearrowright X$, then $|X^H| \equiv |X| \mod p$

Proof. $|X| = \sum_{\bar{x} \in X/H} |\bar{x}| = \sum_{\bar{x} \in X/H} [H : Stab(x)] =$

x a rep. of $\bar{x}$

$$\sum_{x \in X^H} 1 + \sum_{\substack{\bar{x} \in X/H \\ x \notin X^H}} [H : Stab(x)]$$

each an orbit, thus size divisible by p since H is a p-group

$$|X| \equiv |X^H| \mod p$$

Lemma. $H < G$, $|H| = p^e$, $H < N_G(P)$ for $P \in Syl_p(G)$

$\Rightarrow H < P$

Proof. $HP < G$, and $P \trianglelefteq HP < N_G(P)$. By 3rd Iso, $[HP:P] = [H : H \cap P]$,

since we're already working inside $N_G(P)$

But since H is a Sylow p-group, $[H : H \cap P] = p^r$, so $[HP : P] = p^r$ and thus $|HP| = p^{r+u}$ for some u, but it contains P, so $P < HP$ and thus $H < P$.

$S \subset Syl_p(G)$

$S = \{gPg^{-1} \mid g \in G\}$

$$\left.\begin{array}{l} G \times S \to S \\ (g, P) \mapsto gPg^{-1} \end{array}\right\} \underline{\text{transitive}}$$

$P \in S$,

$Stab_G(P) = N_G(P) < G$

$|S| = [G : N_G(P)] \not\equiv 0 \bmod p$

Now let $H \times S \to S$ be the action restricted to H

$|S| \equiv |S^H| \bmod p$ by Lemma 1

so $S^H \neq \phi$ since $|S| \not\equiv 0$

$\exists p' \in S : hP'h^{-1} = P' \;\forall h \in H$, i.e. there is a sylow p-group fixed by all elements of H

$\Rightarrow H < N_G(P')$

$\Rightarrow H < P'$ by Lemma 2

$\Rightarrow$ if $P, P'' \in Syl_p(G)$, $\exists g : P'' \subset gPg^{-1}$, so

$P'' = gPg^{-1}$ since they have the same size.

thus 2 holds

Sylow's Theorems.

Def. Suppose $p^k \| |G|$. A subgroup $P < G$ of order p^k is called a Sylow p-subgroup of G

Def. $Syl_p(G) = \{ P < G : |P| = p^k \}$ (set of Sylow p subgroups)

$n_p(G) = |Syl_p(G)|$

Theorem. Let be a finite group.

1) $n_p(G) \neq 0$ (there is a Sylow p subgroup)

2) If $P \in Syl_p(G)$, and $|H| = p^\ell$, $\ell \geq 0$,
$\exists g \in G : gHg^{-1} < P$ (or equivalently, $H < gPg^{-1}$)

3) $n_p(G) \equiv 1 \bmod p$
$n_p(G) \mid |G|/p^k$

Remark: (2) is equivalent to (2') and (2'')

(2'): $H < P' \in Syl_p(G)$

(2''): If $P, P' \in Syl_p(G)$, $\exists g \in G : P = gP'g^{-1}$

Remark: $n_p(G) = [G : N_G(P)]$ since all Sylow p-subgroups are conjugate so [illegible] is is the number of conjugates proof of (1). Induct on $|G|$.

Assume $\exists H < G, H \neq G : p \nmid [G:H]$,

then $Syl_p(H) \subset Syl_p(G)$

induction $\Rightarrow$ $(\exists P \in Syl_p(H) \Rightarrow \exists P \in Syl_p(G))$

Now suppose $p \mid [G:H]$.

conjugacy classes

$$|G| = |Z(G)| + \sum_i [G : C_G(g_i)]$$

$\Rightarrow p \mid |Z(G)|$, and we know $Z(G)$ is abelian

$\Rightarrow \exists H = \langle g \rangle < Z(G)$ of order p

$H \lhd G$

Lecture 7 (2008-09-19)

9/19/08.

G is solvable if $\exists$ abelian tower ending with $\{e\}$

Prop. G finite,

a) Every abelian tower has a cyclic refinement

b) G is solvable iff it has a cyclic tower ending in $\{e\}$

a) of course $\Rightarrow$ b), prove of (a) last class

If G is a p-group, G is solvable.

Proof. Induction on $|G|$

Let R be a commutative ring. Then $B_n(R) \subset GL_n(R)$, ← matrices with determinant invertible in R

$B_n(R)$ = upper triangular matrices, is a solvable subgroup of $GL_n(R)$, and if R is a field, $B_n(R)$ is maximal in $GL_n(R)$.

$U_n(R) \subset B_n(R)$ = unipotent UT matrix, subgroup $\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$B_n(R) / U_n(R) \simeq D_n$ diagonal matrices $\simeq (R^\times)^n$ commutative

exercise: $U_n(R) \triangleleft B_n(R)$

$$\underset{\overset{\uparrow}{U_{n-1}}}{\left\{ \begin{pmatrix} 1 & 0 & & * \\ & 1 & 0 & \\ & & \ddots & 0 \\ 0 & & & 1 \end{pmatrix} \right\}} \triangleleft \underset{\overset{\uparrow}{U_n}}{\left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}},$$

$U_n / U_{n-1} \simeq R^{n-1}$, additively, since for example $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$

describe $\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \right\}$!

Prop. $H \triangleleft G$, then G is solvable $\Longleftrightarrow$ H is solvable and G/H is solvable

Proof. $\Rightarrow$ G solvable, then $G > G_1 \cdots > G_k = \{e\}$ is an abelian tower.

restrict to H to get tower for H ending in $\{e\}$

Look at $G_1 H \triangleleft G$, let Q_1 = image of G_1 in G/H.

then $Q_1 \triangleleft G/H$ (3rd Iso). $(G/H)/Q_1 \cong G/G_1H$, abelian

$Q \triangleleft G/H$

Now replace G by G_1H and G/H by Q_1.

$$\vdots$$

$g, h \in G$, $[g,h] = ghg^{-1}h^{-1}$.

$[g,h] = e$ iff $gh = hg$.

$G' = [G,G]$ = subgroup generated by all commutators

the conjugate of a commutator is a commutator.

$${}^{k}[g,h] = [{}^{k}g, {}^{k}h]$$

Prop. $G' \triangleleft G$.

Proof. Need $kG'k^{-1} = G'$, but $k[g,h]k^{-1}$, and $\{[g,h]\}$ generates G', so we're good.

Thm $H \triangleleft G$, G/H abelian, iff $G' < H$.

Thm. G is solvable iff $G > G' > G'' \cdots$ ends with $\{e\}$.

Proof. $\Leftarrow$: G_i/G_{i+1} abelian, so G is solvable

$\Rightarrow$: assume $G > G_1 > \cdots > G_k = \{e\}$ is abelian tower, then $G_1 \subset G'$

so $G > G' > G_2 \cap G' > \cdots > G_k \cap G' = \{e\}$

Proof of 3. $S = Syl_p(G) \Rightarrow n_p = [G : N_G(P)]$, which $\mid |G|/p^k$

$$n_p = |S| \equiv |S^P| = \#\{P' : \underbrace{P < N_G(P')\} = \# \{P' : P}_{\text{by lem 2}} < P'\} =$$

$\#\{P\} \equiv 1 \mod p$

$\uparrow$ has one elmt

A_n, $n \geq 5$

$PSL_2(k)$, $|k| \geq 4$, k a field $\Big\}$ simple

A tower of subgroups is $G = G_0 > G_1 > \cdots > G_n$

A normal tower is where $G_{i+1} \triangleright G_i$

An abelian tower is a $\overset{\text{normal}}{\text{tower}}$ where G_{i+1}/G_i is abelian

A cyclic tower is when $G_{i+1} \triangleright G_i$, G_{i+1}/G_i is cyclic

Inducing a Tower

Let $\overbrace{G' = G_0' > \cdots > G_n'}^{*}$ be a tower

If $f : G \to G'$ is a group hom,

$$\underbrace{G > f^{-1}(G_1') > \cdots > f^{-1}(G_n')}_{**}$$

$**$ is a tower, and if $*$ is normal, so is $**$
abelian
cyclic

Proof. $f^{-1}(G_i') < G$ always

$$G_i \longrightarrow G_i' \longrightarrow G_i'/G_{i+1}'$$

G_{i+1} = kernel, so it is normal

$$G_i/G_{i+1} \hookrightarrow G_i'/G_{i+1}'$$

a subgroup of abelian/cyclic is abelian/cyclic

A refinement is a tower

$$G = G_0 > H_1 > \cdots H_k > \cdots > H_m \cdots$$
$$H_k = G_1, \quad H_m = G_n$$

G is solvable if $\exists$ abelian tower: $G_n = \{e\}$

Thm. every abelian tower has a cyclic refinement, and G is solvable iff $\exists$ a cyclic tower with $G_n = \{e\}$

Lecture 8 (2008-09-22)

9/22/08

Theorem (Schreier's)

Let $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = \{e\}$ $\quad (G_\bullet)$

$G = H_1 \triangleright H_2 \triangleright \cdots \triangleright H_s = \{e\}$ $\quad (H_\bullet)$

be two normal towers ending in the trivial subgroup. Then they have a common refinement (here, a refinement of $G_\bullet$ is a normal tower $G_\bullet'$, where

$$G_\bullet' = G_{i_1}' \triangleright \cdots \triangleright G_{i_k}' \quad \text{for some } i_1 < \cdots < i_k$$

Proof

Set $G_{i,j} = G_{i+1}(G_i \cap H_j)$. We claim this is a normal tower refining $G_\bullet$. (with $1 \le i \le r-1$, $1 \le j \le s$)

$$G \simeq G_{1,1} \triangleright G_{1,2} \triangleright \cdots \triangleright G_{1,s-1} \triangleright G_{1,s} \simeq$$

$$G_2 \simeq G_{2,1} \triangleright G_{2,2} \triangleright \cdots G_{r-1,s} = \{1\})$$

We want
$$\begin{array}{ccc} G_{1,2} & & G_{1,1} \\ \parallel & \triangleleft & \parallel \\ G_2(G_1 \cap H_2) & & G_2(G_1 \cap H_1) \end{array}$$

We know $G_1 \cap H_2 \triangleleft G_1 \cap H_1$ since $H_2 \triangleleft H_1$ and $G_1 \triangleleft G_2$ (using facts 1 and 2)

and so on, by induction

Similarly, $H_{i,j} = H_{i+1}(H_i \cap G_j)$ defines a normal tower refining $H_\bullet$

Now we want $\dfrac{G_{i,j}}{G_{i,j+1}} \simeq \dfrac{H_{j,i}}{H_{j,i+1}}$ or equivalently

$$\frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})} \simeq \frac{H_{j+1}(H_j \cap G_i)}{H_{j+1}(H_j \cap G_{i+1})}$$, and use Butterfly lemma with $u = G_{i+1}$, $v = H_{j+1}$, $U = G_i$, $V = H_j$

normal tower $G_\bullet$ is simple if G_i/G_{i+1} are all simple

Jordan-Holder

$$G = G_1 \rhd \cdots \rhd G_r = \{e\}$$
$$G = H_1 \rhd \cdots \rhd H_s = \{e\}$$

Pf: Trivial by Schrier: they have an equivalent common refinement, but a refinement of a simple tower is always trivial.

Exercise: upper triangular matrices in $GL(n,k)$ has an abelian tower ending in $\{e\}$

$$\begin{tikzcd}
u(U\cap V) \arrow[dd, dash, "\triangledown"'] \arrow[dr, dash] & & (U\cap V)v \arrow[dl, dash] \arrow[dd, dash, "\triangledown"] \\
& (U\cap V) \arrow[dd, dash, "\triangledown"'] & \\
u(U\cap v) \arrow[dr, dash] & & (u\cap V)v \arrow[dl, dash] \\
& (u\cap V)(U\cap v) &
\end{tikzcd}$$

By symmetry it suffices to check $\dfrac{u(U\cap V)}{u(U\cap v)} \simeq \dfrac{U\cap V}{(u\cap V)(U\cap v)}$

(we could exchange u's and v's

but first we check that $u(U\cap v) \triangleleft u(U\cap V)$

by fact 1, $v \triangleleft V \Rightarrow U\cap v \triangleleft U\cap V$

(view these as subgroups of U) then fact 2 gives the result since $u \triangleleft U$

Claim: $[u(U\cap v)] \cap [(U\cap V)] = (u\cap V)(U\cap v)$

Exercise

Claim: $[u(U\cap v)](U\cap V) = u(U\cap V)$

Easy

Now Iso theorem $\dfrac{NH}{N} \simeq \dfrac{H}{N\cap H}$, with $H = U\cap V$

$N = u(U\cap v)$

9/22/08

a (normal) tower is a decreasing sequence of subgroups of G

$G = G_1 > G_2 > \cdots$ (or equivalently $G = G_1 \rhd G_2 \rhd \cdots$)

two normal towers

$G = G_1 \rhd G_2 \rhd \cdots G_r$

$G = H_1 \rhd H_2 \rhd \cdots H_s$

are equivalent if $r = s$ and the factor groups are the same up to reordering

$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 \rhd \mathbb{Z}_2 \oplus 0 \rhd 0$

$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \rhd 0 \oplus \mathbb{Z}_3 \rhd 0$

For $A, B < \cancel{G}$, $AB = \{a_1 b_1 \cdots a_n b_n : a_i \in A, b_i \in B\} = BA$

Facts ① if $A, B < G$, and $A \lhd B$, and $C < G$, then

$$A \cap C \lhd B \cap C$$

$a \in A \cap C$

$b \in B \cap C$ $\qquad bab^{-1} \in A \cap C$ ✓

② if A, B are as in 1, and $C \lhd G$, $AC \lhd BC$

Suffices to check that for $a \in A$, $c \in C$, and $b \in B$, $c' \in C$, we have $(bc')ac(bc')^{-1} \in AC$

$$\underbrace{bc' \cdot b^{-1}}_{\in C} \underbrace{b \; a \cdot b^{-1}}_{\in A} \underbrace{b \cdot c \cdot b^{-1}}_{\in C} \underbrace{b \, c^{-1} b^{-1}}_{\in C} \quad ✓$$

Iso: $\dfrac{H}{N \cap H} \simeq \dfrac{NH}{N}$

Butterfly Lemma: Suppose $U, V < G$, $u \lhd U$, $v \lhd V$;

$u(U \cap v) \lhd u(U \cap V)$

$(u \cap V)v \lhd (U \cap V)v$, and the $\quad \dfrac{u(U \cap V)}{u(U \cap v)} \simeq \dfrac{(U \cap V)v}{(u \cap V)v}$

corresponding quotients are isomorphic.

Lecture 9 (2008-09-26)

9/28/08

Def. A category A is the following data:

- a <u>collection</u> of objects, called $Ob(A)$ (could be set or class)
- $\forall X, Y \in Ob(A)$, a <u>set</u> $Hom_A(X,Y)$ of "arrows" or "morphisms" from X to Y

satisfying these axioms:

- $\forall X \in Ob(A)$, $\exists!\ id_X \in Hom_A(X,X)$ with $\forall g \in Hom_A(X,Y)$, $g \circ id_X = id_Y \circ g = g$
- morphisms closed under composition, i.e. $\forall X, Y, Z \in Ob(A)$, and $g \in Hom_A(X,Y)$, and $h \in Hom_A(Y,Z)$, then $h \circ g \in Hom_A(X,Z)$
- composition is associative, i.e. $\forall X, Y, Z, W \in Ob(A)$, $g \in Hom_A(X,Y)$, $h \in Hom_A(Y,Z)$, $k \in Hom_A(Z,W)$, then $k \circ (h \circ g) = (k \circ h) \circ g$
- $\forall X, X', Y, Y' \in Ob(A)$, if $X \neq X'$ or $Y \neq Y'$, $Hom_A(X,Y) \cap Hom_A(X',Y') = \phi$

Ex. $A = Sets$, with $Ob(Sets)$ = all sets, $Hom_{Sets}(X,Y)$ = maps from X to Y, and id_X the identity map from X to X. Composition is associative.

Ex. $A = Grp$, with $Ob(Grp)$ = all groups, mappings are group homomorphisms, etc. Check that the composition of homomorphisms is a homomorphism.

Ex. Ab = abelian groups, also Rings, Fields, Top = topological spaces with mappings being continuous functions, R-Mod = R-modules, Vect = vector spaces

Let G be a group. Define a category $Cat(G)$, with $Ob(Cat(G)) = *$, a set of one element $Hom_{Cat(G)}(*,*) = G$, with $id_* = e_G$, the identity of G, and composition being the group operation, i.e. $g \circ h = gh$

Simplest example: $A = \phi$, with $Ob(A) - \phi$, $Hom_A(,) = id$. Called the <u>final</u> category.

Ex. Let $(X, \leq)$ be a poset. Define $Cat(X, \leq)$ to have $ob(Cat(X,\leq)) = X$, and for $x, y \in X$, $Hom_{cat(X,\leq)}(x,y) = \phi$ if $x \not\leq y$, and $\{x \mapsto y\}$ if $x \leq y$.

$$\begin{tikzcd} \{\} \arrow[loop above, "id"] \end{tikzcd}$$

Ex. Let A, B be categories. A <u>covariant functor</u> $\mathfrak{F}: A \rightarrow B$ is the data

- $\forall X \in Ob(A)$, there is an object $\mathfrak{F}X \in Ob(B)$
- $\forall g \in Hom_A(X,Y)$, $\mathfrak{F}g : \mathfrak{F}X \rightarrow \mathfrak{F}Y \in Hom_B(\mathfrak{F}X, \mathfrak{F}Y)$

satisfying these axioms:

- $\mathfrak{F} id_X = id_{\mathfrak{F}X}$
- $\mathfrak{F}(g \circ h) = \mathfrak{F}g \circ \mathfrak{F}h$
- the following diagram is commutative:

$$\begin{tikzcd} & \mathfrak{F}Y \arrow[dr, "\mathfrak{F}g"] & \\ \mathfrak{F}X \arrow[ur, "\mathfrak{F}h"] \arrow[rr, bend right, "\mathfrak{F}(g \circ h)"'] & \circlearrowleft & \mathfrak{F}Z \end{tikzcd}$$

A contravariant functor reverses arrows, so if $\mathcal{F}: A \to B$ is contravariant, we get

$\forall g \in \mathrm{Hom}_A(X, Y)$, there is an

$\mathcal{F}g \in \mathrm{Hom}_B(\mathcal{F}Y, \mathcal{F}X)$, and

$\mathcal{F}(g \circ h) = \mathcal{F}(h) \circ \mathcal{F}(g)$, and

$$\begin{tikzcd}
 & \mathcal{F}Y \arrow[dl, "\mathcal{F}h"'] & \\
\mathcal{F}X & G & \mathcal{F}Z \arrow[ul, "\mathcal{F}g"'] \arrow[ll, bend left, "\mathcal{F}(g\circ h)"]
\end{tikzcd}$$

commutes.

Lecture 10 (2008-09-29)

9/29/08

Let A be a category.

Def. $X, Y \in Ob(A)$, $f \in Hom_A(X,Y)$. f is an <u>isomorphism</u> if $\exists g \in Hom_A(Y,X)$: $g \circ f = id_X$ and $f \circ g = id_Y$.

Let $X = \mathbb{R}$ with euclidean topology, $Y = \mathbb{R}$ with topology $(\phi, \mathbb{R})$, $f: X \to Y$ being the identity map <u>as sets</u>.

Def. $Aut_A(X) \subset Hom_A(X,X)$ is the set of isomorphisms from X to itself. THIS IS A GROUP.

Exc. Let $f \in Hom_A(X,Y)$. Prove $f \in Iso_A(X,Y)$ <u>iff</u> $\forall T \in Ob(A)$, the composition map $Hom_A(T,X) \to Hom(T,Y)$ is a bijection.
$h \longmapsto f \circ h$

State and prove the analog for $h \in ?$, $h \longmapsto h \circ f$.

Def. Let G be a group. An <u>action</u> of G on $S \in Ob(A)$ is a group homomorphism from $G \to Aut_A(S)$. (Of course, S is not necessarily a set anymore). That is,

$\forall g \in G$, get an element $p(g) \in Aut(S)$, with $p(e) = id_S$, composition associative, etc.

When G acts on an object of A, it is called a representation of G in A.
representation of G in Sets = action of G on set A
representation of G in Fin-Vect = linear map $G \to GL_n(k)$

Exc. $S, T \in Ob(A)$, prove that $Aut_A(T) \times Iso_A(S,T) \longrightarrow Iso_A(S,T)$ is a
$\sigma \quad , \quad h \longmapsto \sigma \circ h$

well-defined group action, and if $Iso_A(S,T) \neq \phi$, is simply transitive.

Stupid category: X is a set, let A be category with $Ob(A) = X$, and $\forall x, y \in X$, $Hom_A(x,y) = \phi$ if $x \neq y$, $\{id_x\}$ if $x = y$

For $S \in Ob(A)$, define A_S to be the <u>objects over S</u>, so $Ob(A_S) = \bigsqcup_{X \in Ob(A)} Hom_A(X,S)$, or intuitively, the set of $\left\{ \begin{smallmatrix} X \\ \downarrow \\ S \end{smallmatrix} \right\}$, and for $f \begin{smallmatrix} X \\ \downarrow \\ S \end{smallmatrix}, g \begin{smallmatrix} Y \\ \downarrow \\ S \end{smallmatrix} \in Ob(A_S)$, $Hom_{A_S}\left(\begin{smallmatrix} X \\ \downarrow \\ S \end{smallmatrix}, \begin{smallmatrix} Y \\ \downarrow \\ S \end{smallmatrix} \right) =$ $\{h \in Hom_A(X,Y) : g \circ h = f\}$, i.e. h such that

$$\begin{tikzcd} X \arrow[rr, "h"] \arrow[dr, "f"'] & & Y \arrow[dl, "g"] \\ & S \arrow[u, phantom, "\circlearrowleft"] & \end{tikzcd}$$

commutes.

Exc. Prove A_S is a category.

Similar concept of <u>objects under S</u>, ${}_SA$, with $ob({}_SA) = \bigsqcup_{X \in Ob(A)} Hom_A(S,X) = \left\{ \begin{smallmatrix} S \\ \downarrow \\ X \end{smallmatrix} \right\}$.

Exc. Prove $(A_S)^{op} = {}_S(A^{op})$, $A_S = ({}_SA^{op})^{op}$, ${}_SA = ((A^{op})_S)^{op}$

A trivial category:

$$\begin{tikzcd} X \arrow[loop above, "id_X"] \arrow[r, bend left, "f"] & Y \arrow[loop above, "id_Y"] \arrow[l, bend left, "g"] \end{tikzcd}$$

Some ways to make new categories: A, B categories, then $A \times B$ has $Ob(A \times B) = Ob(A) \times Ob(B)$

2A has $Ob(2A) = Ob(A) \sqcup Ob(A)$, $Hom((X,i),(Y,i)) = Hom(X,Y)$

Lecture 11 (2008-10-03)

10/3/08

Funct(A, B) is collection of all functors from A to B

If $F, G \in$ Funct(A,B), we can define $\alpha : F \to G$ "natural" transformation

turns Funct(A,B) into a category

Def. natural transformation $\alpha : F \to G$ has

data: $\forall x \in Ob(A)$, $\alpha_x : F(x) \to G(x)$ in $Hom_B(F(x), G(x))$

axiom: $\forall x, y \in Ob(A)$, $f \in Hom_A(x, y)$,

$$\begin{tikzcd}
F(x) \arrow[r, "\alpha_x"] \arrow[d, "F(f)"'] \arrow[dr, phantom, "\circlearrowright"] & G(x) \arrow[d, "G(f)"] \\
F(y) \arrow[r, "\alpha_y"'] & G(y)
\end{tikzcd}$$

If F and G were contravariant, switch arrows

* note: for a functor $F : A \to B$, $id_F : F \to F$ given by $(id_F)_x : F(x) \xrightarrow{id_{F(x)}} F(x)$ satisfies the axiom of natural transformation

So if $\alpha : F \to G$, $\beta : G \to H$ are natural,

$$\begin{tikzcd}
F(x) \arrow[r, "\alpha_x"] \arrow[d, "F(f)"'] \arrow[dr, phantom, "\circlearrowright"] & G(x) \arrow[r, "\beta_x"] \arrow[d, "G(f)"] \arrow[dr, phantom, "\circlearrowright"] & H(x) \arrow[d, "H(f)"] \\
F(y) \arrow[r, "\alpha_y"'] & G(y) \arrow[r, "\beta_y"'] & H(y)
\end{tikzcd}$$

then $\beta \circ \alpha : F \to H$ is natural

Exer. Funct(A, B) forms a category

Def. An isomorphism of functors is an invertible natural transformation, i.e. $\exists \beta : G \to F$, a natural trans. : $\alpha \circ \beta = id_G : G \to G$

$\beta \circ \alpha = id_F : F \to F$, i.e.

$\forall x$, $f : X \to Y$,

$$\begin{tikzcd}
G(x) \arrow[r, "\beta_x"] \arrow[d, "G(f)"'] \arrow[dr, phantom, "\circlearrowright"] & F(x) \arrow[r, "\alpha_x"] \arrow[d, "F(f)"] \arrow[dr, phantom, "\circlearrowright"] & G(x) \arrow[r, "\beta_x"] \arrow[d, "G(f)"] \arrow[dr, phantom, "\circlearrowright"] & F(x) \arrow[d, "F(f)"] \\
G(y) \arrow[r, "\beta_y"] & F(y) \arrow[r, "\alpha_y"'] & G(y) \arrow[r, "\beta_y"'] & F(y)
\end{tikzcd}$$

Lemma. $\alpha : F \to G$ is an isom. of functors $\iff$ $\alpha_x : F(x) \longrightarrow G(x)$ is an isom. $\forall x$

Proof $\Rightarrow$, assume α is an isom. Then $\forall x$, $\beta_x \circ \alpha_x = id_{F(x)}$, $\alpha_x \circ \beta_x = id_{G(x)}$

$\Leftarrow$ assume α_x is invertible $\forall x$, let $\beta_x : G(x) \to F(x)$ be its inverse. This is a natural transformation (we need: $F(f) \circ \beta_x = \beta_y \circ G(f)$

$$\begin{tikzcd} G(x) \arrow[r] & F(Y) \arrow[d, "\alpha_x"] \\ & G(Y) \end{tikzcd}$$

equivalently, $\alpha_y \circ F(f) \circ \beta_x = \underset{id}{\alpha_y \circ \beta_y} \circ G(f)$

$\alpha_y \circ F(f) \circ \beta_x = G(f)$

$\alpha_y \circ F(f) = G(f) \circ \alpha_x$

Def. $F : A \to B$ is an equivalence of categories if F is a functor and $\exists g : B \to A$ and $F \circ G \overset{\beta}{\simeq} id_B$, $G \circ F \overset{\alpha}{\simeq} id_A$

$$\begin{tikzcd} A \arrow[r, bend left, "F"{name=U}] \arrow[r, bend right, "F_1"'{name=D}] & B \arrow[Rightarrow, from=U, to=D, "\alpha"] \end{tikzcd}$$

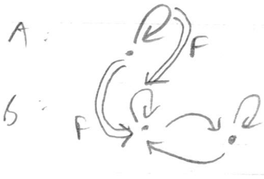
diagrammed like this

$$\begin{tikzcd} & B \arrow[ld, "G"'] \arrow[d, "id_B"] \arrow[ld, phantom, shift right=4, "\overset{\simeq}{\underset{\beta}{\Rightarrow}}"] \\ A \arrow[r, "F"] \arrow[d, "id_A"'] & B \arrow[ld, "G"] \\ A \arrow[ru, phantom, shift left=4, "\overset{\simeq}{\underset{\alpha}{\Leftarrow}}"] & \end{tikzcd}$$

Ex. $id_A : A \to A$ is an equivalence

$id_{(id_A)} : id_A \to id_A$

Ex.



F is an equivalence, since we can take all arrows in B to the single arrow in A, and all objects in B to the single object in A

Let $G : B \to A$ be the unique one in

$$\begin{tikzcd} & B \arrow[ld, "G"'] \arrow[d, "id_B"] \\ A \arrow[r, "F"] \arrow[d, "id_A"'] & B \arrow[ld, "G"] \\ A & \end{tikzcd}$$

, $G \circ F : A \to A$ equals id_A, so $G \circ F \underset{\alpha}{\overset{\sim}{\Rightarrow}} id_A$ by $\alpha = id_{(id_A)}$

$F \circ G\ z = x$
$F \circ G\ f = id_x$

$F \circ G \longrightarrow id_B$
$F \circ G_x \xrightarrow{\beta_x} X$
$\underbrace{F \circ G\ y}_{x} \xrightarrow{\beta_y} Y$

$$\begin{tikzcd} X \arrow[r, "\beta_x"] \arrow[d] \arrow[rd, phantom, "\circlearrowright"] & X \arrow[d] \\ x \arrow[r] & Y \end{tikzcd}$$

$\forall z \in Ob(B)$ $\beta_z : x \to z$ if $f : z_1 \to z_2$

$$\begin{tikzcd} X \arrow[r, "\beta_{z_1}"] \arrow[d, "id_x"'] & z_1 \arrow[d, "f"] \\ X \arrow[r, "\beta_{z_2}"'] & z_2 \end{tikzcd}$$

but $x \to z_1$ unique, so commutative

$\Rightarrow \beta$ is a natural transformation

Lecture 12 (2008-10-06)

10/6/08

$\mathcal{F} : A \to B$ is an equivalence if

(a): $\exists g : B \to A$

(b): $\mathcal{F} \circ g \overset{\beta}{\simeq} id_B$, $g \circ \mathcal{F} \overset{\alpha}{\simeq} id_A$

Def. $\mathcal{F} : A \to B$ be a functor, $\mathcal{F}$ is faithful if for any objects $x, y \in Ob(A)$, the map $Hom_A(x,y) \xrightarrow{*} Hom_B(\mathcal{F}x, \mathcal{F}y)$ is injective and

$\mathcal{F}$ is full if $*$ is surjective

$\mathcal{F}$ is essentially surjective if $\forall w \in Ob(B)$, $\exists x \in Ob(A) : \mathcal{F}x \simeq w$

Thm. $\mathcal{F}$ is an equivalence of categories $\Leftrightarrow$ fully faithful + essentially surjective (depends on axiom of choice)

Let $B =$ finite dimensional vector spaces over $\mathbb{R}$
$A = \{\mathbb{R}^n, n \geq 0\}$
$Hom_A(\mathbb{R}^n, \mathbb{R}^m) = M_{m \times n}(\mathbb{R})$, composition is matrix multiplication, and $id_{\mathbb{R}_n} = I_n$

Let $\mathcal{F} : A \to B$ with $\mathcal{F}\mathbb{R}^n = \mathbb{R}^n$, $\mathcal{F}\phi =$ linear trans. associated to ϕ, $(v \in \mathbb{R}^n \mapsto \phi v \in \mathbb{R}^m)$

Prop. this is an equivalence of categories

Pf. Two matrices are the same linear trans. $\Leftrightarrow \phi_1 = \phi_2$ and any linear trans. has a matrix
Any finite dimensional vector space is isomorphic to some $\mathbb{R}^n$

$\Rightarrow$ easy

$\Leftarrow$ Let $\mathcal{F} : A \to B$ be a fully faithful + essentially surjective.

need $G : B \to A$, $\forall w \in Ob(B)$ <u>Choose</u> an object $Gw \in Ob(A)$ with $\mathcal{F}Gw \simeq w$

If $w, z \in Ob(B)$,

$$\begin{tikzcd} Hom_A(Gw, Gz) \arrow[r, phantom, "\simeq"] & Hom_B(\mathcal{F}Gw, \mathcal{F}Gw) \arrow[d, phantom, "\wr"] \\ & Hom_B(w, z) \arrow[ul] \end{tikzcd}$$

check: compatible with id, composition $\Rightarrow$ G is a functor

Let A be a category. An object P is called a final object if $\forall X \in Ob(A)$ if $\exists ! \ X \to P$

Q is an initial object if $\forall X \in Ob(A)$ $\exists ! \ Q \to X$

$A = $ Sets ; $P = $ any singleton , $Q = \emptyset$

$A = Gr$; $P = \{1\}$, $Q = \{1\}$

$A = $ Ptd. Top. Sets ; $P = \{\{pt\}, pt\}$, $Q = \{\{pt\}, pt\}$

$A = $ Ring , $P = \{0\}$, $Q = \mathbb{Z}$

Lecture 13 (2008-10-08)

10/8/08

initial object } called universal objects
final object }

<u>Products + coproducts</u>

Let A be a category, $S, T \in Ob(A)$, a product of S and T in A is

Data:
$$\begin{tikzcd} & X \arrow[dl, "p_S"'] \arrow[dr, "p_T"] & \\ S & & T \end{tikzcd}$$
$p_{S,T}$ = projection on S, T

Axiom: $\forall C$, $\begin{tikzcd} & C \arrow[dl, "\phi_S"'] \arrow[dr, "\phi_T"] & \\ S & & T \end{tikzcd}$, in A, $\exists! \, C \xrightarrow{h} X$ such that

We say $h = \phi_S \times \phi_T$

This is called a universal property

$$\begin{tikzcd} & C \arrow[dl, "\phi_S"'] \arrow[d, "h"] \arrow[dr, "\phi_T"] & \\ S \arrow[r, phantom, "\circlearrowleft"] & X \arrow[l, "p_S"] \arrow[r, "p_T"'] \arrow[r, phantom, "\circlearrowleft", shift left=3] & T \end{tikzcd}$$

Also think of as product of S_α's for some indexing α,

product is $\underbrace{(X, p_\alpha : X \to S_\alpha)}_{\text{data}}$, $\underbrace{\text{such that}}_{\text{axiom}}$ $\forall C$ with $\phi_\alpha : C \to S_\alpha$,

$\exists! h$:
$$\begin{tikzcd} C \arrow[r] \arrow[dr, "\phi_\alpha"'] & X \arrow[d, "p_\alpha"] \arrow[dl, phantom, "\circlearrowleft"] \\ & S_\alpha \end{tikzcd}$$
commutes

Prop. exists a product in Sets. Let $S, T \in Ob(Sets)$. Let
$X = S \times T = \{(s,t) : s \in S, t \in T\}$. with the maps
$p_S : X \to S$ $\quad$ $p_t : X \to T$
$(s,t) \mapsto s$ $\quad$ $(s,t) \mapsto t$ $\qquad$ Let C be a set and let

$\phi_S : C \to S$, $\phi_T : C \to T$; define $C \xrightarrow{h} X$
$c \mapsto (\phi_S(c), \phi_T(c)) = \phi_S \times \phi_T(c)$

need. $p_S \circ h(c) = p_S(\phi_S(c), \phi_T(c)) = \phi_S(c)$
$p_T \circ h(c)$ ——— $> \phi_T(c)$

Also, if h' satisfies $p_S \circ h'(c) = \phi_S(c)$, $p_T \circ h'(c) = \phi_T(c)$, then $h'(c) = (\phi_S(c), \phi_T(c))$
$= h(c)$, so

Prop: a product in a category is unique up to a unique isomorphism if it exists, i.e., if

$$\begin{tikzcd} & X \arrow[dl, "p_S"'] \arrow[dr, "p_T"] & \\ S & & T \end{tikzcd}, \quad \begin{tikzcd} & X' \arrow[dl, "p_S'"'] \arrow[dr, "p_T'"] & \\ S & & T \end{tikzcd}$$

are products in A,

then $\exists!$ isom. $X' \simeq X$: diagram commutes

Proof. by definition, X is a product, so $\exists! h$:

$$\begin{tikzcd} & X' \arrow[dl, bend right] \arrow[d, "h"] \arrow[dr, bend left] \arrow[dl, phantom, shift left=3, "\circlearrowleft"] \arrow[dr, phantom, shift right=3, "\circlearrowleft"] & \\ S & X \arrow[l] \arrow[r] & T \end{tikzcd} \qquad \begin{tikzcd} & X \arrow[dl, bend right] \arrow[d, "h'"] \arrow[dr, bend left] & \\ S & X' \arrow[l] \arrow[r] & T \end{tikzcd}$$

observing

$$\begin{tikzcd} & X' \arrow[d, "h"] \arrow[dddl, bend right, "p_S'"'] \arrow[dddr, bend left, "p_T'"] & \\ & X \arrow[d, "h'"] \arrow[ddl, bend right, "p_S"'] \arrow[ddr, bend left, "p_T"] & \\ & X' \arrow[d, "h"] \arrow[dl, bend right, "p_S'"'] \arrow[dr, bend left, "p_T'"] & \\ S & X \arrow[l, "p_S"] \arrow[r, "p_T"'] & T \end{tikzcd}$$

we want $h \circ h' = id_X : X \to X$, but both $h \circ h'$ and id

$$\begin{tikzcd} & X \arrow[dl, bend right, "p_S"'] \arrow[d, "h \circ h'"] \arrow[dr, bend left, "p_T"] \arrow[dl, phantom, shift left=3, "\circlearrowleft"] \arrow[dr, phantom, shift right=3, "\circlearrowleft"] & \\ S & X \arrow[l, "p_S"] \arrow[r, "p_T"'] & T \end{tikzcd} \qquad \begin{tikzcd} & X \arrow[dl, bend right, "p_S"'] \arrow[d, "id"] \arrow[dr, bend left, "p_T"] \arrow[dl, phantom, shift left=3, "\circlearrowleft"] \arrow[dr, phantom, shift right=3, "\circlearrowleft"] & \\ S & X \arrow[l, "p_S"] \arrow[r, "p_T"'] & T \end{tikzcd}$$

make this commutative,

and by assumption $h \circ h'$ is unique, any one id, so $h \circ h' = id$

reversing roles / symmetry, $h' \circ h = id_{X'}$ as well, Let $\mathcal{B}$ be a category.

Prop. A final object in $\mathcal{B}$ is unique up to unique isom., if it exists.

Proof.

P, P' are final objects in $\mathcal{B}$. Then $\forall S \in Ob(\mathcal{B})$,

$\exists! S \to P$, $\exists! S \to P'$.

Since P' is final, $\exists! h' : P \to P'$, and since P is final,

$\exists! h : P' \to P$, so we need $id = h \circ h' : P \to P$

$P \xrightarrow{h \circ h'} P$ is a unique isom. in $\mathcal{B}$, but only id works,

etc

Same is true for initial objects, since we can either prove directly, or note that

Q is initial in $A \iff Q$ is final in A^{op}

Products in Top. If X, Y are top spaces, then $X \times Y$, with product top, is a product in Top.

$X \times Y$ topology generated by $\{U \times Y : U \subset X \text{ is open}\}$
$\{X \times V : V \subset Y \text{ is open}\}$

$$\begin{tikzcd}
 & X \times Y \arrow[dl, "p_X"'] \arrow[dr, "p_Y"] & \\
X & & Y
\end{tikzcd}$$

p_X, p_Y are arrows in Top (continuous) since the inverse image of open sets in X and Y are open sets in $X \times Y$

We want

$$\begin{tikzcd}
 & C \arrow[dl, bend right, "\phi_X"'] \arrow[dr, bend left, "\phi_Y"] \arrow[d, "\exists! h"] & \\
X & X \times Y \arrow[l] \arrow[r] & Y
\end{tikzcd}$$

Since top. spaces are already sets, we know the diagram is commutative, and exists unique map as sets, but we need to show h is an arrow in Top (i.e. continuous). So we need

$\phi_X \times \phi_Y : C \to X \times Y$ continuous, i.e. $\phi_X \circ \phi_Y (U \times Y)$ open, $\phi_X \circ \phi_Y (X \times V)$ open, since

It suffices to check on generating sets. But $(\phi_X \circ \phi_Y)^{-1}(U \times Y) = \phi_X^{-1}(U)$ open in C
$(\phi_X \circ \phi_Y)^{-1}(X \times V) = \phi_Y^{-1}(V)$ open in C

Lecture 14 (2008-10-10)

10/10/08

Products in Sets, Top, Grps.

products in Grps exist: G_1, G_2 groups,
$$\begin{tikzcd} & G_1 \times G_2 \arrow[dl] \arrow[dr] & \\ G_1 & & G_2 \end{tikzcd}$$
set product is group product

In Sets^{op}, the product is

$$\begin{tikzcd} & Y & \\ X_1 \arrow[ur] & & X_2 \arrow[ul] \end{tikzcd}$$

(in Sets, since arrows are reversed)

s.t. if $X_1 \xrightarrow[\phi_1]{} C \xleftarrow[\phi_2]{} X_2$,

$$\begin{tikzcd} & C & \\ & Y \arrow[u, "\exists ! h"'] & \\ X_1 \arrow[ur, "p_1"] \arrow[uur, "\phi_1"] & & X_2 \arrow[ul, "p_2"'] \arrow[uul, "\phi_2"'] \end{tikzcd}$$

(in Sets)

$Y = X_1 \sqcup X_2$

Def. Let A be a category, $S, T \in Ob(A)$.

A coproduct of S_α in A, $\bigsqcup_\alpha S_\alpha$, is an object Y with $i_\alpha : S_\alpha \to Y$ such that if C, $\phi_\alpha : S_\alpha \to Y$, then $\exists ! \, h : Y \to C$ and

$$\begin{tikzcd} S_\alpha \arrow[r, "i_\alpha"] \arrow[dr, "\phi_\alpha"'] & Y \arrow[d, "h"] \\ & C \end{tikzcd}$$

The disjoint union is a coproduct in Sets. Proof. given $X_1 \xrightarrow{\phi_1} C$, $X_2 \xrightarrow{\phi_2} C$,

need $h : X_1 \sqcup X_2 \to C$, and show uniqueness

let $x \in X_1 \sqcup X_2$. Case 1. $x \in X_1$, then define $h(x) = \phi_1(x)$
$x \in X_2$, then $h(x) = \phi_2(x)$

If $h \circ i_1 = \phi_1(x)$
then $h(x) = \phi_1(x)$

If $h \circ i_2(x) = \phi_2(x)$
then $h(x) = \phi_2(x)$, so h is unique

Top : $X_1 \sqcup X_2$

Ab : NOT LIKE SETS,
$X_1 \oplus X_2$

$$\begin{tikzcd} A_1 \arrow[dr, "i_1"'] & & A_2 \arrow[dl, "i_2"] \\ & A_1 \oplus A_2 & \end{tikzcd}$$

with $a_1 \overset{i_1}{\longmapsto} (a_1, 0)$
$a_2 \overset{i_2}{\longmapsto} (0, a_2)$

$$\begin{tikzcd} A_1 \arrow[r] \arrow[dr, bend right, "\phi_1"'] & A_1 \oplus A_2 \arrow[d, "\exists ! \, h"] & A_2 \arrow[l] \arrow[dl, bend left, "\phi_2"] \\ & C & \end{tikzcd}$$

Commutative ?

$h(a_1, 0) = h(i_1(a_1)) = \phi_1(a_1)$
$h(0, a_2) = h(i_2(a_2)) = \phi_2(a_2)$
and $(a_1, a_2) \mapsto \phi_1(a_1) + \phi_2(a_2)$, $h((a_1, a_2) + (b_1, b_2)) = h(a_1 + b_1, a_2 + b_2) =$
$\phi_1(a_1 + b_1) + \phi_2(a_2 + b_2) - h(a$

If A_α are abelian groups,

$$A_\alpha \to \bigoplus_\alpha A_\alpha \text{ is a coproduct in } Ab$$

$$\bigoplus_\alpha A_\alpha = \{a_{\alpha_1} + \cdots a_{\alpha_n} : \overset{\text{all but}}{\text{finitely}} \text{ many are } 0\}$$

Note: $i_\alpha : A_\alpha \to \bigoplus_\alpha A_\alpha$

$$a_\alpha \mapsto (0, \ldots 0, a_\alpha, \ldots 0)$$

Need: if $\phi_\alpha : A_\alpha \to C$,

$\exists! \, h : \oplus A_\alpha \to C$

$$h(a_{\alpha_1} + \cdots + a_{\alpha_n}) = \phi_{\alpha_1}(a_{\alpha_1}) + \cdots \phi_{\alpha_n}(a_{\alpha_n})$$

Clearly a gp homomorphism, unique by comm. diagram.
Can't split homomorphism over infinitely many terms?

Coproducts in Gr:

$G_1 * G_2 =$ free group on elements of G_1 and G_2, with presentation of product of two things in G_1 is its answer, etc.

Lecture 15 (2008-10-15)

10/15/08

Exercises If $S, T \in Ob(A)$, show that $S \times T \overset{\uparrow}{\simeq} T \times S$

$S \times (T \times U) \simeq (S \times T) \times U \simeq S \times T \times U$

unique isomorphism compatible with some diagram

A a category, $S \in Ob(A)$, then A_S is a category with $Ob(A_S) = \left\{ \begin{smallmatrix} X \\ \downarrow \\ S \end{smallmatrix} \right\}$

and $Hom\left(\begin{smallmatrix} X \\ \downarrow \\ S \end{smallmatrix}, \begin{smallmatrix} Y \\ \downarrow \\ S \end{smallmatrix} \right) = \left\{ \begin{tikzcd} X \arrow[rr, "f"] \arrow[dr] & & Y \arrow[dl, "g"] \\ & S & \end{tikzcd} \right\}$ (commutative diagrams)

What is product in A_S, in terms of A? A product would be an object of the category, P, :

$$\begin{tikzcd} & P \arrow[dl, "\pi_X"'] \arrow[dr, "\pi_Y"] \arrow[dd, "\exists! h"] & \\ X \arrow[dr, "f"'] & & Y \arrow[dl, "g"] \\ & S & \end{tikzcd}$$

commutes, and any similar C

$$\begin{tikzcd} & C \arrow[dl, "\phi_X"'] \arrow[dr, "\phi_Y"] \arrow[d, "\exists! h"] \arrow[dd, dotted, bend left] & \\ X \arrow[dr, "f"'] & P \arrow[l, "\pi_X"'] \arrow[r, "\pi_Y"] \arrow[d, dotted] & Y \arrow[dl, "g"] \\ & S & \end{tikzcd}$$

This is the fibered product over S

Prop. These exist in SetS.

$$\begin{tikzcd} X \arrow[dr] & & Y \arrow[dl] \\ & S & \end{tikzcd}$$

$$\begin{tikzcd} & P \arrow[dl, "\pi_X"'] \arrow[dr, "\pi_Y"] & \\ X \arrow[dr] & & Y \arrow[dl] \\ & S & \end{tikzcd}$$

Then we can see P must be some subset of $X \times Y$

If $(x,y) \in X \times Y$

$\pi_X(x,y) = x$

$\pi_Y(x,y) = y$

$f(\pi_X(x,y)) = f(x)$

$g(\pi_Y(x,y)) = g(y)$

Condition for (x,y) to be in P is $f(x) = g(y)$ (i.e, diagram be commutative)

Def. $X \times_S Y \subset X \times Y$

$\overset{\shortparallel}{\{(x,y) : f(x) = g(y)\}}$

Claim. $X \times_S Y$ is a fibered product in Set_S

$$\begin{tikzcd} & X \times_S Y \arrow[dl, "\pi_X"'] \arrow[dr, "\pi_Y"] & \\ X \arrow[dr] & & Y \arrow[dl] \\ & S & \end{tikzcd}$$

Proof. (a) this data satisfies the requirement $f \circ \pi_X = g \circ \pi_Y$, by definition of $X \times_S Y$

(b) Say

$$\begin{tikzcd} & C \arrow[dl, "\phi_X"'] \arrow[dr, "\phi_Y"] & \\ X \arrow[dr, "f"'] & & Y \arrow[dl, "g"] \\ & S & \end{tikzcd}$$

, then

$$\begin{tikzcd} & C \arrow[dl, "\phi_X"'] \arrow[dr, "\phi_Y"] \arrow[d, "\exists! h"] & \\ X \arrow[dr, bend right, "f"'] & P \arrow[l, "\pi_X"] \arrow[r, "\pi_Y"'] \arrow[d, "\bar{h}"] & Y \arrow[dl, bend left, "g"] \\ & S & \end{tikzcd}$$

assume $f \circ \phi_X = g \circ \phi_Y$

$f \circ \pi_X \circ \bar{h} = g \circ \pi_Y \circ \bar{h}$

for $c \in C$, $f \circ \pi_X(\bar{h}(c)) = g \circ \pi_Y(\bar{h}(c))$

write $\bar{h}(c) = (x,y)$

then $f(x) = g(y)$ as needed

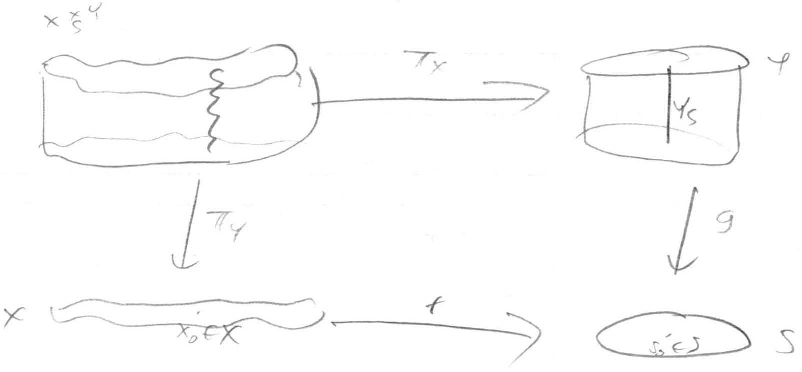
If $X, Y \subset S$, what is $\underset{\underset{S}{\downarrow}}{X \times_S Y}$?

$X \times_S Y = \{(x,y) : f(x) = g(y)\}$, but f and g are inclusions into S, so this is ordered pairs of elements of $X \cap Y$

so $X \times_S Y \simeq X \cap Y$

If $X \subset S$, $Y \to S$,

$X \times_S Y = \{(x,y : f(x) = g(y)\} = \{(s,y) : \begin{matrix} s = g(y) \\ s \in X \end{matrix}\} = g^{-1}(X)$



$g \circ \pi_Y = f \circ \pi_X$

$X \times_S Y = \{(x,y) : f(x) = g(y)\}$

fix $x_0 \in Y$, what is $\pi_X^{-1}(x_0)$?

$\pi^{-1}(x_0) = \{(x_0, y) : f(x_0) = g(y)\} \cong \{y : g(y) = f(x_0)\} = g^{-1}(s_0)$

fibered product is pullback of $Y \to S$ to X

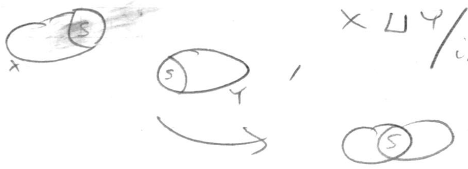
---

fibered coproduct

$$\begin{tikzcd}
S \arrow[r, "f"] \arrow[d, "g"'] \arrow[dr, phantom, "G"] & X \arrow[d, "i_X"] \arrow[ddr, bend left] & \\
Y \arrow[r, "i_Y"'] \arrow[drr, bend right] & P \arrow[dr, "h"] \arrow[dr, phantom, "\exists!"'] & \\
& & C
\end{tikzcd}$$

disjoint union doesn't necessarily work

If



, $X \sqcup Y / i_X \circ f(s) = i_Y \circ g(s)$

Lecture 16 (2008-10-18)

10/18/08

Product: universal property in terms of A, $S, T \in Ob(A)$

$$\begin{tikzcd} & S\times T \arrow[dl] \arrow[dr] & \\ S & & T \end{tikzcd}$$ and is universal, i.e. $$\begin{tikzcd} & C \arrow[dl] \arrow[d, dashed] \arrow[dr] & \\ S & S\times T \arrow[l] \arrow[r] & T \end{tikzcd}$$

Makes category $A_{S,T}$: objects $$\begin{tikzcd} & C \arrow[dl, "\phi_S"'] \arrow[dr, "\phi_T"] & \\ S & & T \end{tikzcd}$$, arrows $$\left(\begin{tikzcd} & C \arrow[dl, "\phi_S"'] \arrow[dr, "\phi_T"] & \\ S & & T \end{tikzcd}\right) \to \left(\begin{tikzcd} & C' \arrow[dl, "\phi_S'"'] \arrow[dr, "\phi_T'"] & \\ S & & T \end{tikzcd}\right)$$

$$\begin{tikzcd} & S\times T \arrow[dl] \arrow[dr] & \\ S & & T \end{tikzcd}$$ is a final object in $A_{S,T}$, so

$$\begin{tikzcd} & C \arrow[d, "h"] \arrow[ddl, "\phi_S"'] \arrow[ddr, "\phi_T"] & \\ & C' \arrow[dl, "\phi_S'"] \arrow[dr, "\phi_T'"'] & \\ S & & T \end{tikzcd}$$

$\phi_S' \circ h = \phi_S$

$\phi_T' \circ h = \phi_T$

If $Y \in Ob(A)$, we have a contravariant functor M_Y from $M_Y : A \to Sets$

$X \mapsto Hom(X, Y)$

$$\begin{tikzcd} X \arrow[r, "\mathcal{F}"] \arrow[dr] & X_1 \arrow[d] \\ & Y \end{tikzcd}$$

$X, X_1 \in Ob(A)$

$Hom(X, Y) \xrightarrow{\circ \mathcal{F}} Hom(X_1, Y)$

Def. A contravariant functor $\mathcal{F}$ from A to Sets is said to be represented by Y if there is an isomorphism $\mathcal{F} \simeq M_Y$

given S, T, consider $\mathcal{F} : A \to Sets$

$X \mapsto Hom(X, S) \times Hom(X, T)$

$\mathcal{F}$ $X \xrightarrow{\mathcal{F}} X_1$,

$$\begin{tikzcd} Hom(X_1, S) \times Hom(X_1, T) \arrow[d, "\phi_S \quad\quad \phi_T"] \\ Hom(X, S) \times Hom(X, T) \end{tikzcd}$$

$$(\phi_{1S} \circ \mathcal{F}, \phi_{1T} \circ \mathcal{F})$$

$$\overset{\shortparallel}{\phi_S} \qquad \overset{\shortparallel}{\phi_T}$$

Claim. $S \times T$ represents $\mathcal{F}$.

$X \mapsto Hom(X, S \times T)$

$X \mapsto Hom(X, S) \times Hom(X, T)$

$$\begin{tikzcd} & X \arrow[d, "\exists!\, h"] \arrow[ddl, bend right, "p_S \circ \mathcal{F} = \phi_S"'] \arrow[ddr, bend left, "p_T \circ \mathcal{F} = \phi_T"] & \\ & S\times T \arrow[dl, "p_S"] \arrow[dr, "p_T"'] & \\ S & & T \end{tikzcd}$$

$A = Sets$

A group is a $G \in Ob(A)$ with

$G \times G \xrightarrow{m} G$ operation

$G \xrightarrow{i} G$ inversion

$P \xrightarrow{e} G$ takes final object P in Sets to identity

Satisfying

$$\begin{tikzcd} P \times G \arrow[r, "e \times id"] \arrow[dr, "proj_G"'] & G \times G \arrow[d, "m"] \arrow[dl, phantom, "\circlearrowleft"] \\ & G \end{tikzcd}$$

$$\begin{tikzcd} G \times P \arrow[r, "id \times e"] \arrow[dr, "proj_G"'] & G \times G \arrow[d, "m"] \arrow[dl, phantom, "\circlearrowleft"] \\ & G \end{tikzcd}$$

e is left + right id,

$$\begin{tikzcd} a & (a, a) \\ G \arrow[r, "\Delta"', "\text{``diagonal'' map}"] \arrow[ddd] & G \times G \arrow[d, "i \times id"] \\ & G \times G \arrow[d, "m"] & (a^{-1}, a) \\ & G \\ P \arrow[r, "e"] & G \end{tikzcd}$$

(and, similar case with (a, a^{-1}))

and

$$\begin{tikzcd} (G \times G) \times G \arrow[r, "m \times id"] \arrow[d, "id \times m"'] & G \times G \arrow[d, "m"] \arrow[dl, phantom, "\circlearrowleft"] \\ G \times G \arrow[r, "m"] & G \end{tikzcd}$$

Ex. If G is a group object in A, then $\forall X \in Ob(A)$, $Hom(X, G)$ is a group and $Hom(X,G) \xrightarrow{\circ f} Hom(X,G)$ is a group homomorphism

Ex. A group object in the category of Groups is an <u>abelian</u> group.

Ex. What is a group object in Top?

It is a group G : $G \times G \xrightarrow{m} G$, $G \xrightarrow{i} G$, and $P \xrightarrow{e} G$ are continuous

$e : P \to G$ is continuous already since P is a single point

$\mathbb{R}, +$ with $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$
$(a,b) \mapsto a+b$ is continuous

10/18/08

If F a field with $|F| \geqslant 4$, then $PSL_2(F) = SL_2(F)/Z$, $Z = \{I, -I\}$ is simple (and for $|F| \geqslant 3$, $PSL_n(F) = SL_n(F)/Z$, $Z = \{\zeta_n I : \zeta_n^n = 1\}$, is simple)

Def. Standard Borel subgroup, B_2 of $SL_2(F) = \{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a, b \in F\}$

Def. Standard unipotent subgroup, U $= \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F\}$ we call $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ "$x(b)$"

Def. torus subgroup, $T_2 = \{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in F\}$ we call $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ "$s(a)$"

Def. $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $y(c) = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$

Lemma. $\{x(b) : b \in F\}$, $\{y(c) : c \in F\}$ generate $SL_2(F)$. We will call $SL_2(F)$ "

Proof. $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \delta & 1 \end{pmatrix} \cdots$, check that you can get anything you want in T_2 ■

Note that $wUw^{-1} = \{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\}$, the lower triangular matrices in $SL_2(F)$, which we will call $\overline{U}$, and $w\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}w^{-1} = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$ and $B = UT = TU$. Note G acts on F^2, and the stabilizer of $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is $U = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\}$.

Note $Be_1 = \{\begin{pmatrix} a \\ 0 \end{pmatrix}\}$ $a \in F^\times$, and $Bwe_1 = B\begin{pmatrix} 0 \\ -1 \end{pmatrix} = \begin{pmatrix} -b \\ -a^{-1} \end{pmatrix}$

so $F^2 - \{0\} = Be_1 \sqcup Bwe_1$

Note that $F^2 - \{0\}$ is a principle homogeneous space for $SL_2(F) = G$, since we can get from any non-zero vector to any other via $SL_2(F)$,

So $F^2 - \{0\} = G/\text{Stab}(\text{anything}) = G/U$, but $Be_1 \sqcup Bwe_1 = B/U \sqcup BwU/U$,

$\parallel$

$Be_1 \sqcup Bwe_1$

so $G = B \sqcup BwU$ (Bruhat decomposition)

Prop. B is a maximal subgroup of G.

Suppose $B \lneqq S < G$. Say $x \in S - B$. $x \in BwU = BwB$, and let $x = bwb^{-1}$, $B \subset S \Rightarrow w \in S$, which $\Rightarrow BwU \subset S$, so $S = G$.

commutator subgroup

If $|F|>4$, then $SL_2(F)'=SL_2(F)$.

Pf. $[s(a), X(b)] = X(z)$, where $z = b(a^2-1)$.

By assumption, $|F|>4$, so $\exists a \in F^\times : a^2 \neq 1$, so $B'=U$, and thus $G' \supset U$,

$G' \triangleleft G$, so $\bar{U} = wUw^{-1} \subset G'$, so $\underset{\overset{\parallel}{G}}{\langle U, \bar{U} \rangle} \subset G' \subset G$, so $G = G'$

Proof of main theorem.

Lemma. $C = \bigcap_{g \in SL_2} gBg^{-1} = Z$

"Pf" Start with $g = id$, w, get $\left\{\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix}\right\} \cap \left\{\begin{pmatrix} a & 0 \\ b & a^{-1}\end{pmatrix}\right\}$, so $C = \left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}\right\}$

Lemma. $H \triangleleft G \Rightarrow$ either $H < Z$ or $G' < H$

"Pf". Two cases: either a) $HB = B$, or b) $HB = G$.

a) $H < B \Rightarrow H \subset Z$ by Lemma.

b) $HB = G \Rightarrow w \in HB$, so $w = hb$ $h \in H$, $b \in B$.

$$\bar{U} = wUw^{-1}$$
$$= hb\underbrace{U}_{U}b^{-1}h^{-1} = hUh^{-1} \subset HU$$

$U \subset HU$, $\bar{U} \subset HU \Rightarrow HU = G$, since $\langle U, \bar{U} \rangle = G$

$G/H = HU/H \simeq U/(H \cap U)$ is abelian, but a modding out can only be abelian if it contains the commutator subgroup, so $H \supset G^{-1}$.

Say $\bar{H} \subset G/Z$ is normal. Let $H \triangleleft G$ be the inverse image group.

either $H < Z \Rightarrow \bar{H} = \{id\}$ or $H > G' = G \Rightarrow \bar{H} = G/Z$

Ex. describe $PSL_2(\mathbb{F}_3)$ and $PSL_2(\mathbb{F}_2)$

Lecture 17 (2008-10-22)

Rings + modules 10/22/08

Def. A ring $(R, +, \cdot)$ is $(R, +)$ an abelian group, $(R, \cdot)$ is monoid with 1. and distributive on both sides.

Def. A ring homomorphism is $f : R \to S$ such that
$$1_R \mapsto 1_S$$
$$f(a+b) = f(a) + f(b)$$
$$f(ab) = f(a)f(b)$$

Category of Rings.

Ex. $\mathbb{Q}, \mathbb{R}, \mathbb{Z}, R[x], \mathbb{Z}/n\mathbb{Z}$, and if M an ab. gp., $\mathrm{Hom}_{Ab}(M, M) = \mathrm{End}(M)$ is a ring

$f, g \in \mathrm{End}(M)$
$$(f+g)(m) = f(m) + g(m)$$
$$(fg)(m) = f(g(m))$$

distributive since $f((g_1+g_2)(m)) = f(g_1(m) + (g_2(m))) = f(g_1(m)) + f(g_2(m)) = ((fg_1) + (fg_2))(m)$

Similarly, $\mathrm{End}_k(V)$ for V a vector space, is a ring

We can have a ring action...

An R-module M is an abelian group
$$R \times M \to M$$
$$(1, m) \mapsto m$$
$$(r+s)m = rm + sm$$
$$r(m+n) = rm + rn$$
$$(rs)m = r(sm)$$

Ex. vector space V over $k \Leftrightarrow k$-module

$$\mathrm{End}(M) \times M \to M$$
$$(f, m) \mapsto f(m)$$
M is an $\mathrm{End}(M)$-module

So vector space V is both a k-module and an $\mathrm{End}(V)$-module

$$\mathbb{Z} \times M \to M$$
$$(n, m) \mapsto nm = \underbrace{m + \cdots + m}_{n \text{ times}}$$

$\mathbb{Z}$-modules are the same as abelian groups.

Prop. Let M be an ab. gp. There is a one-to-one correspondence between R-module structures on M, and ring homomorphisms $R \to \mathrm{End}(M)$

Pf. Say $R \times M \xrightarrow{\alpha} M$ gives M the structure of a R-module. Define $\rho : R \to \mathrm{End}(M)$, $r \mapsto (m \mapsto rm)$. $(m \mapsto rm)$ is a ab. gp. homomorphism, so $\overset{\text{this is a}}{\text{well}}$ defined map $R \to \mathrm{End}(M)$

Conversely, given $\rho : R \to \operatorname{End}(M)$ a ring homomorphism.

Define $a : R \times M \to M$

$(r, m) \mapsto \rho(r)(m)$ this gives M the structure of a R-mod.

An R-module homomorphism $f : M \longrightarrow N$ is an ab. gp. homomorphism with $\forall\, r, m,\ f(r \cdot m) = r\, f(m)$

So $\underline{R\text{-Mod}}$ is a category. We just write $\operatorname{Hom}_{R\text{-mod}}(M,N)$ as $\operatorname{Hom}_R(M,N)$

(associative, unital)

An algebra is an R-mod A, which has a ring structure, with $r(ab) = (ra)b = a(rb)$

An algebra hom. is a module hom which is also a ring hom.

$\underline{R\text{-Alg}}$ is a category.

Ex. V a vector space over k, then $\operatorname{End}_k(V)$ is an algebra

Ex. M an ab. gp. $\operatorname{End}(M)$ is a $\mathbb{Z}$-algebra.

Prop. Suppose R, A are comm. rings, 1-1 correspondence

ring hom. $\phi : R \to A$ and

R-alg. structures on A

$r \cdot a = \phi(r)\, a$

$r(ab) = (ra)b = a(rb)$

$$\underline{\text{Rings}} \xrightarrow{G_a} \underline{\text{Groups}}$$

$R \longmapsto (R, +)$

$R \longmapsto R^\times$

Lecture 18 (2008-10-24)

$$\begin{tikzcd}A \arrow[r] & B \\ 0 \arrow[u] \arrow[r] & ? \arrow[u]\end{tikzcd}$$

10/24/08

Prop. In Rings, R-Mod, and R-Alg, products exist and are given by cartesian product.

$R_1 \times R_2 = \{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R_2\}$

Coproducts in R-mod; If $\forall i$, $M_i \xrightarrow{f_i} N$, then $\exists!$ map from $\bigoplus M_i \to N$

Functor $\mathbb{G}_a$: Ring $\to$ Ab

$R \longmapsto (R, +)$

$\mathbb{G}_M$: Ring $\to$ Ab

$R \longmapsto (R^\times, \cdot)$

Ring $\to$ Ring

$R \longmapsto R[x]$

$(R_1 \xrightarrow{f} R_2) \to R_1[x] \to R_2[x]$

$\sum r_i x^i \mapsto \sum f(r_i) x^i$

Note: if R commutative, $R[x]$ is naturally a R-algebra.

Universal property of $R[x]$

$\exists$ $R \to R[x]$

$r \mapsto r x^0$, x commutes with all elements of R,

$$r_1 x^i \cdot r_2 x^j = r_1 r_2 x^{i+j}$$

Ring $\times$ Group $\to$ Rings Exercise: this is a functor

$R, G \longmapsto R[G]$ or RG

R, G commutative $\Leftrightarrow$ RG is commutative, unless $R = \{0\}$ in which case RG is always commutative

$RG = \bigoplus_{g \in G} Rg$ and $\left(\sum_i r_i g_i\right)\left(\sum_j r_j' g_j'\right) = \sum r_i r_j' g_i g_j'$

If $R = \mathbb{Z}$, $G = \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}G = \{m[0] + n[1]\} \simeq \mathbb{Z}^2$

Exercise. If $G = \mathbb{Z}/2\mathbb{Z}$, R commutative.

describe $\mathbb{Z}G$ and show $\mathbb{Z}G \not\simeq \mathbb{Z} \times \mathbb{Z}$

If $2^{-1} \in R$, show $RG \simeq R \times R$

What is RG if $R = \{0\}$?

Similarly, Sets $\to$ R-Mod

$X \longmapsto R\langle X \rangle = \bigoplus_{x \in X} Rx$

We can have Sets $\to$ Ab

$X \longmapsto \mathbb{Z}\langle X \rangle = \bigoplus_{x \in X} \mathbb{Z}x$. Show this is a functor.

Lecture 19 (2008-10-27)

<u>Rings</u> $\longrightarrow$ <u>Rings</u>

$R \longmapsto M_n(R)$ even for non-commutative rings 10/27/08

If R is commutative, $M_n(R) \simeq \mathrm{End}_R(R^n)$

Exercise. What is $\mathrm{End}_R(R)$ for R non-comm? $\mathrm{End}_R(R^n)$?

If R a ring, $M \subset N$ are R-modules, we say M is a submodule and N/M is an abelian group.

Prop. N/M is an R-module such that $N \xrightarrow{q} N/M$ is an R-module homomorphism.

$r(n+m) = rn + M \quad \forall r \in R$. Verify, $1(n+m) = 1n + M = n + M$

$r((n+M)+(n'+M)) = r((n+n')+M) = r(n+n') + M$ ad

Def. A R-module M is said to be free is $M \simeq \bigoplus_{i \in I} R_i$ or equivalently $M = R\langle X\rangle$ where $X = I$

Exercise. $\mathbb{Q}$ is not a free $\mathbb{Z}$-module. $(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$ is not a free $\mathbb{Z}$-module.

Prop. Every module is the quotient of a free module.

Lemma. If $\phi: M \to N$ is an R-module homomorphism, $\mathrm{Ker}(\phi)$, $\mathrm{Im}(\phi)$ are R-modules.

Pf. If $m \in \mathrm{Ker}(\phi)$, $\phi(rm) = r\phi(m) = 0 \Rightarrow rm \in \mathrm{Ker}(\phi)$, similarly for $\mathrm{Im}(\phi)$

Pf. Given M, we want a free R-module F and a surjective $F \to M$. Take $F = R\langle M\rangle$, and $\bigoplus_{m \in M} Rm \longrightarrow M$ with $m \longmapsto m$.

<u>Rings</u>. If $\phi: R \to S$ is a ring hom, $\mathrm{Ker}(\phi)$ is an two-sided ideal.

Isomorphism Theorems for Modules. For an R-mod hom $\phi: M \to N$, $\mathrm{Im}(\phi) \simeq M/\mathrm{Ker}(\phi)$

$M \subset N \subset L$ R-mods, then $(L/M)/(N/M) \simeq L/N$

$M_1, M_2 \subset N \Rightarrow M_1 + M_2$ is a submodule, and $M_1+M_2/M_2 \simeq M_1/M_1 \cap M_2$

If $M \subset N$, $\exists$ a bijection $\{\text{submodules } \overline{K} \subset N/M\} \leftrightarrow \{K : M \subset K \subset N\}$

For Rings. If $\phi: R \to S$ is a ring hom, $\phi(R)$ is a subring of S, and $\phi(R) \simeq R/\mathrm{Ker}(\phi)$

$J \subset I \subset R$, J and I ideals, then I/J is an ideal in R/J and $(R/J)/(I/J) \simeq R/I$

If $J \subset R$, $\exists$ a bijection $\{\text{ideals of } R/J\} \leftrightarrow \{\text{ideals } I \text{ of } R : J \subset I \subset R\}$

Prop. R is a field iff R is a comm. ring with only ideals $I = \{0\}$ and $I = R$.

Use $I = R \Leftrightarrow 1 \in I$. $\Rightarrow$ is easy; for $\Leftarrow$, suppose $I \subset R$ is only $\{0\}$ or R. We want to show $r \neq 0$ is invertible. Consider $Rr \subset R$, an ideal; $r \neq 0 \Rightarrow Rr \neq \{0\}$, so Rr must be R, so $\exists\, s \in R : sr = 1 \Rightarrow$ invertible

Lecture 20 (2008-10-29)

10/29/08

P a prime ideal $\Leftrightarrow$ R/P an integral domain.

If P is prime, $\bar{a}, \bar{b} \in R/P$, with $\bar{a}\bar{b} = 0$,
let $a \in R$ be s.t. $a + P = \bar{a}$, $b \in R$ with $b + P = \bar{b}$ (representatives)
$ab \in P \Rightarrow$ either a or b in P $\Rightarrow$ either $\bar{a}$ or $\bar{b}$ is 0 (other way, reverse arrows)

Thm. If $f : R \to S$ a ring hom, $P \subset S$ prime, then $f^{-1}(P)$ is prime in R.

Pf.
$$\begin{tikzcd} R \arrow[r, "f"] \arrow[dr, "\phi"'] & S \arrow[d, "q"] \\ & S/P \end{tikzcd}$$
, $\ker(\phi) = f^{-1}(P)$ so $R/f^{-1}(P) \subset S/P$
but S/P is a domain, so $R/f^{-1}(P)$ is a subdomain, so $f^{-1}(P)$ is prime in R.

Thm. Let R be a ring, $I \subset R$ an ideal $\neq R$. $\exists M : I \subset M \subset R$ is maximal

Pf. Let $P = \{J : I \subset J \subsetneq R\}$, ordered by inclusion. Let $C \subset P$ be a totally ordered subset, i.e., $\forall J_1, J_2 \in C$, either $J_1 \subset J_2$ or $J_2 \subset J_1$.
Let $N = \bigcup_{J \subset C} J$. Need to show $N \in P$. N is an ideal since $\forall a \in J_1, b \in J_2$, either $a, b \in J_1$ or $a, b \in J_2$ since either $J_1 \subset J_2$ or $J_2 \subset J_1$, so $a + b \in J_1$ or J_2, so $a + b \in N$. Similarly with absorptiveness. Also, $N \neq R$, since if $N = R$, $1 \in N \Rightarrow 1 \in J_1 \Rightarrow J_1 \in R$. N is maximal by Zorn's Lemma.

LEARN MODULES OVER PIDS.

Rings of fractions. R a comm. ring, a subset $S \subset R$ is a multiplicative set if $1 \in S$, $\forall a, b \in S$, $ab \in S$.
Want $\left\{\frac{a}{s}\right\}_{\substack{a \in R \\ s \in S}}$, $\frac{a}{s} = \frac{b}{t}$ iff $at = sb$. This is not good enough if S has zero divisors.

Def. $S^{-1}R = \left\{\frac{a}{s} \,\middle|\, \substack{a \in R \\ s \in S}\right\} / \sim$ where $\left(\frac{a}{s}\right) \sim \left(\frac{b}{t}\right)$ iff $\exists u \in S : u(at - sb) = 0$,

Def. $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$, $\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$

If R a ring, $f \in R$, $S = \langle f \rangle$
$S^{-1}R$ is denoted R_f or $R[f^{-1}] = R[x]/(fx - 1)$

Thm. (a) $S^{-1}R$ is a ring
(b) the map $R \xrightarrow{\phi} S^{-1}R$, $a \mapsto a/1$ is a ring hom. which satisfies
(i) $\phi(s) \in (S^{-1}R)^\times$ $\forall s \in S$
(ii) If $\psi : R \to A$ a ring hom. has $\psi(S) \subset A^\times$,

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[dr, "\psi"'] & S^{-1}R \arrow[d, "\exists! h"] \\ & A \end{tikzcd}$$

Ex. R a domain, $S = R - \{0\}$
Ex. R a comm. ring $S =$ units (the $u \in S$ in the definition is unnecessary here)
$R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(a, b) : \substack{a \neq 0 \\ b \neq 0}\}$. $S^{-1}R \cong \mathbb{Q} \times \mathbb{Q}$

If $R = A \times B$, $S = A \times \{1\}$
$S^{-1}R \simeq B$

R a ring, P a prime ideal, $S = R - P$

Note: $1 \notin P$

$a, b \in S \Rightarrow a \cdot b \in S$ since P is prime So S is mult.

$S^{-1}R = R_P$, localization of R at P

Lecture 21 (2008-10-31)

$S^{-1}R = \left\{ \frac{a}{s} : \begin{array}{l} a \in R \\ s \in S \end{array} \right\} \Big/ \left\{ \frac{a}{s} = \frac{a'}{s'} \text{ iff } \begin{array}{l} \exists u \in S: \\ u(s'a - sa') = 0 \end{array} \right\}$ 10/31/08

Thm. $S^{-1}R$ is a ring

$R \xrightarrow{\phi} S^{-1}R$ is a ring hom
$a \mapsto \frac{a}{1}$

Note. The u in the definition is necessary for it being an equivalence relation, specifically for transitivity.

$\phi(S) \subset (S^{-1}R)^\times$

universal, in that

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[dr, "\psi"'] & S^{-1}R \arrow[d, "\exists! h"] \\ & A \end{tikzcd}$$

$\forall A: \psi(S) \subset A^\times$

Pf. We need to show the operations are well-defined. If $\frac{a}{s} = \frac{a'}{s'}$, $\frac{b}{t} = \frac{b'}{t'}$, we need that $\frac{a}{s} + \frac{b}{t} = \frac{a'}{s'} + \frac{b'}{t'} = \frac{dt' + b's'}{s't'}$. We know $\exists u: u(as' - sa') = 0$ and $v: v(bt' - tb') =$ and $uv(st(a't' + b's') - s't'(at + bs)) = 0$, so we're good. Comm, assoc, etc. as in second grade. $a \mapsto \frac{a}{1}$, $b \mapsto \frac{b}{1}$, $\frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$, $\frac{ab}{1} = \frac{a}{1}\frac{b}{1}$, and $\frac{1}{1}$ is the identity. Next, $\phi(s) = \frac{s}{1}$, then $\phi(s)^{-1} = \frac{1}{s}$. Finally, we want our $h: S^{-1}R \to A$ to have $\frac{a}{s} \mapsto \psi(a) \cdot \psi(s)^{-1}$. Check $\frac{a}{s} = \frac{a'}{s'} \Rightarrow \exists u: us'a - usa' = 0$, for it to be well defined.

$\psi(uss^{-1})(\psi(a)\psi(s)^{-1} - \psi(a')\psi(s)^{-1}) \Rightarrow \psi(u)\psi(s')\psi(a) - \psi(u)\psi(a')\psi(s) = \psi(us'a - usa') = 0$,

So well-defined. Then check that ψ is a homomorphism. Etc.

Thm. $\exists$ a 1-1 correspondence between $\{\text{prime ideals } Q \subset S^{-1}R\}$ and $\{\text{prime ideals } P \subset R \text{ with } P \cap S = \phi\}$

if $S = R - P_0$, P_0 a prime ideal, $\{\text{primes in } R_{P_0}\} \leftrightarrow \{\text{primes } P \subset R : P \subset P_0\}$

Pf. We know $\underset{Q \text{ prime}}{Q \subset S^{-1}R}, \longmapsto \phi^{-1}(Q) \subset R$ a prime ideal (inverse image of prime ideal is prime ideal)

and to any $P \subset R$, we can associate $\phi(P)S^{-1}R$ (the ideal generated by $\phi(P)$).

$PS^{-1}R = \left\{ \frac{p}{s} : \begin{array}{l} p \in P \\ s \in S \end{array} \right\} \leftarrow$ since this the ϕ from above, $\phi(P) = P$

Claim. $PS^{-1}R \neq (1)$.

suppose $1 \in PS^{-1}R$, i.e. $1 = \sum_{i=1}^{m} \frac{r_i}{s_i} p_i$, $\frac{r_i}{s_i} \in S^{-1}R$, $p_i \in P$. We can take common denominators, $1 = \frac{\sum_{i=1}^{m} r_i' p_i}{s} = \frac{p}{s}$ for some $p \in P$, $s \in S$, so $s = p'$, but $P \cap S = \phi$, contradiction. Thus $PS^{-1}R$ is a proper ideal.

Claim. $PS^{-1}R$ is prime.

Suppose $\frac{a}{s} \cdot \frac{b}{t} \in PS^{-1}R$, i.e. $\frac{a}{s} \cdot \frac{b}{t} = \frac{p}{u}$ for some $p \in P$. So $ab = pstu \in S^{-1}R$, so $abv = pstuv \in R$ for some $v \in S$, so $abv \in P$, $v \in S \Rightarrow v \notin P$ so $ab \in P$, so a or $b \in P$ and we are done.

Now given $Q \subset S^{-1}R$, prime, $(\phi^{-1}(Q))S^{-1}R \subset Q$, and if $q \in Q$, $q = \frac{a}{s}$ for some $a \in R$, $s \in S$, $qs = a \in R$, but also $qs \in Q$, so $a \in \phi^{-1}(Q)$, so $\frac{a}{1} \in (\phi^{-1}(Q))S^{-1}R$, so $q = \frac{1}{s}\frac{a}{1} \in (\phi^{-1}(Q))S^{-1}R$, so we get equality ✓

need to show: assume $P \subset R$ prime, $P \cap S = \phi$

$\phi^{-1}(PS^{-1}R) \supset P$, but $a \in \phi^{-1}(PS^{-1}R)$, i.e. $\frac{a}{1} \in PS^{-1}R$, i.e. $\frac{a}{1} = \frac{p}{s}$

so $usa = u1p = up \in P$, so $a \in P$.

Lecture 22 (2008-11-03)

(all rings are comm.)

11/3/08

Suppose $f: R \to T$ is a ring homomorphism, and N is a T-module.

N becomes an R-module by $R \times N \to N$ with $(r, n) \mapsto f(r)n$. This is labeled ${}_R N$.

This is a functor; $N_1 \longrightarrow N_2$ a T-mod hom.

${}_R N_1 \longrightarrow {}_R N_2$ an R-mod hom.

We have the ring hom. $R \to S^{-1}R$, so any $S^{-1}R$-mod is an R-mod; what about reverse? Let S be mult. set., M an R-mod.

$$S^{-1}M = \left\{ \frac{m}{s} : \begin{matrix} m \in M \\ s \in S \end{matrix} \right\} \Big/ \left\{ \frac{m}{s} \sim \frac{n}{t} \Leftrightarrow \exists u : utm = usn \right\}.$$

add. $\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st}$ (well defined, ab. group)

Mult by R. $r \cdot \left(\frac{m}{s}\right) = \frac{rm}{s}$, so $S^{-1}M$ is an R-module

<u>Mult by $S^{-1}R$.</u> $\left(\frac{r}{t}\right) \cdot \left(\frac{m}{s}\right) = \frac{rm}{ts}$

Proof that $S^{-1}M$ is an $S^{-1}R$ module is same as that $S^{-1}R$ is a ring

Def. Let $M \xrightarrow{f} M'$ be an R-mod hom. Then $S^{-1}M \xrightarrow{f_S} S^{-1}M'$ is an $S^{-1}R$-mod hom. with $f_S\left(\frac{m}{s}\right) = \frac{f(m)}{s}$. well-defined: if $\frac{m}{s} = \frac{m_1}{s_1}$, $\exists u : us_1 m = usm_1$,

$$\begin{matrix} us_1 f(m) = & usf(m) \\ \| & \| \\ f(us_1 m) & f(usm_1) \end{matrix}$$

, and $f_S\left(\frac{m}{s} + \frac{m_1}{s_1}\right) = f_S\left(\frac{m}{s}\right) + f_S\left(\frac{m_1}{s_1}\right)$, and $\frac{r}{t} f_S\left(\frac{m}{s}\right) = f_S\left(\frac{rm}{st}\right)$.

e.g. M an ab. gp. $S = \mathbb{Z} - \{0\}$, $S^{-1}M$ a $\mathbb{Q}$-vector space.

$M = \mathbb{Z}$, $S^{-1}M = \mathbb{Q}$, $M = \mathbb{Z}^2$, $S^{-1}M = \mathbb{Q}^2$, but $M = \mathbb{Z}/2\mathbb{Z}$, $S^{-1}M = 0$

Thm. (a) suppose $M \overset{f}{\subset} N$ an R-submodule, then $S^{-1}M \overset{f_S}{\subset} S^{-1}N$ a submodule.

(b) suppose $M \twoheadrightarrow N$ is surjective, then $S^{-1}M \twoheadrightarrow S^{-1}N$ surjective.

(c) Let $\phi : M \to N$ be an R-Mod hom. $\phi_S : S^{-1}M \to S^{-1}N$ is an $S^{-1}R$-mod hom, and $S^{-1}(\mathrm{Ker}(\phi)) = \mathrm{Ker}(\phi_S)$.

Remark. This means that $M \longrightarrow S^{-1}M$ is an exact functor, i.e. $0 \to K \to M \to N \to 0$ exact $\Rightarrow$ $0 \to S^{-1}K \to S^{-1}M \to S^{-1}N \to 0$ is also exact

Pf. Suppose $\frac{m}{s} \in S^{-1}M$, $f_S\left(\frac{m}{s}\right) = 0$. If $S^{-1}M$ is to be a submodule of $S^{-1}N$, we want f_S to be injective, i.e. $\frac{m}{s}$ must be 0. But $f_S\left(\frac{m}{s}\right) = \frac{1}{s} \cdot f(m)$. $\frac{1}{s} f(m) = 0 \Rightarrow f(m) = 0 \Rightarrow$ $\exists u : uf(m) = 0 \Rightarrow f(u \cdot m) = 0 \Rightarrow u \cdot m = 0 \Rightarrow \frac{m}{1} = 0 \Rightarrow \frac{m}{s} = 0$. This proves (a)

(b) Let $\frac{n}{s} \in S^{-1}N$, $n \in N \Rightarrow \exists m : n = f(m)$ so $f_S\left(\frac{m}{s}\right) = \frac{f(m)}{s} = \frac{n}{s}$. Thus f_S is surjective.

(c) Let $\frac{m}{s} \in S^{-1}\operatorname{Ker}(\phi)$, i.e. $m \in \operatorname{Ker}(\phi)$, $s \in S$. $f_S\left(\frac{m}{s}\right) = \frac{f(m)}{s} = \frac{0}{s} = 0$, so $S^{-1}\operatorname{Ker}(\phi) \subset \operatorname{Ker}(\phi_S)$. Let $\frac{m}{s}$ be : $\phi_S\left(\frac{m}{s}\right) = 0$, That is, $\frac{1}{s} \cdot \frac{\phi(m)}{1} = 0$ in $S^{-1}N$, so $\frac{\phi(m)}{1} = 0$ in $S^{-1}N$, so $\exists u : u\phi(m) = 0$ in N, so $\phi(um) = 0$, so $um \in \operatorname{Ker}(\phi)$.

Consider $\underbrace{\frac{um}{us}}_{\in S^{-1}\operatorname{Ker}(\phi)} = \frac{m}{s}$; we know $\phi_S\left(\frac{m}{s}\right) = 0$. So $\operatorname{Ker}(\phi_S) \subset S^{-1}\operatorname{Ker}(\phi)$

Examples. $0 \to \mathbb{Z} \to \mathbb{Z}^2 \to \mathbb{Z} \to 0$

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Q} \arrow[r] & S^{-1}\mathbb{Z}^2 \arrow[r] \arrow[d, phantom, "\wr"] & \mathbb{Q} \arrow[r, Rightarrow] & 0 \\
 & & \mathbb{Q}^2 & &
\end{tikzcd}$$

(since the kernel is a 1-dimensional $\mathbb{Q}$-vector space, and so is the image)

$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

$$0 \to \mathbb{Q} \xrightarrow{\cdot 2} \mathbb{Q} \to \mathbb{Q}/2\mathbb{Q} \to 0$$

Lecture 23 (2008-11-05)

11/5/08

Limits + Colimits

If I is a poset, I is called directed (or direct) if $\forall i, j \in I, \exists k \in I: k \geq i, k \geq j$

A a category, an I-system in A is (a) $\forall i \in I$, there is an $x_i \in Ob(A)$

(b) $\forall i \leq j$, an arrow $x_i \xrightarrow{\phi_{ij}} x_j$

if $i = j$, $\phi_{ij} = id\, x_i$

if $i \leq j \leq k$, then

$$\begin{tikzcd} x_i \arrow[r, "\phi_{ij}"] \arrow[rr, bend right, "\phi_{ik}"'] & x_j \arrow[r, "\phi_{jk}"] & x_k \end{tikzcd}$$

commutes

$\phi_{ik} = \phi_{jk} \circ \phi_{ij}$

Note: this is a $\overset{\text{covariant}}{\text{functor}}$

$Cat(I) \longrightarrow A$

An inverse I-system in A

(a) $\forall i \in I$, $x_i \in Ob(A)$

(b) $\forall i \leq j$, $x_i \xleftarrow{\phi_{ij}} x_j$

commutes, etc

Let $I \to A$ (we're dropping the "$Cat(I)$") be a diret I-system in A.

A <u>direct limit</u> of $I \to A$, $\varinjlim_I x_i$, is an element of $Ob(A)$ with a collection of

(this is really $\varinjlim_I (x_i, \phi_{ij})$)

arrows $\phi_i : x_i \to \varinjlim_I x_i$. Let's call $\varinjlim_I x_i = L$

such that

$$\begin{tikzcd} x_i \arrow[r, "\phi_i"] \arrow[d, "\phi_{ij}"'] & L \\ x_j \arrow[ur, "\phi_j"'] & \end{tikzcd}$$

commutes, and L is universal, so $\forall M \in Ob(A)$,

with maps $\psi_i : x_i \longrightarrow M$,

$$\begin{tikzcd} x_i \arrow[r, "\psi_i"] \arrow[d, "\phi_{ij}"'] & M \\ x_j \arrow[ur, "\psi_j"'] & \end{tikzcd}$$

commutes,

and $\exists ! h : L \to M$:

$$\begin{tikzcd} x_i \arrow[dr, "\phi_i"] \arrow[d, "\phi_{ij}"'] \arrow[drr, bend left, "\psi_i"] & & \\ x_j \arrow[r, "\phi_j"'] \arrow[rr, bend right, "\psi_j"'] & L \arrow[r, "h"] & M \end{tikzcd}$$

If $A = Ab$, $I = \{i_1, i_2\}$, no relation between 1 and 2,

$i \to x_1$

$i \longrightarrow x_2$,

limit is just coproduct, i.e. $x_1 \oplus x_2$.

If $A = \underline{Sets}$, $I = \{\mathbb{Z}, \geq\}$, $n \longrightarrow x_n$, $x_{-1} \subset x_0 \subset x_1 \subset \cdots$

limit is union

Inverse limit is same but with arrows all reversed, so in first example, invese limit is product (which in Ab is isomorphic to coproduct), but in the second example, inverse limit is intersection since

$x_1 \supset x_2 \supset x_3 \cdots$

Prop. Let A be a category, I a poset w/trivial ordering, so I looks like $\cdot\ \cdot\ \cdot\ \cdot\ \cdot$

then if $I \to A$ is a direct system, then $\varinjlim_{I} X_i$ exists iff $\coprod_{I} X_i$ exists, and they are isomorphic.

If $I \to A$ is an inverse system, $\varprojlim_{I} X_i$ exists iff $\prod_{I} X_i$ exists, and they are isomorphic.

Pf. Same diagrams.

Prop. (1) Direct limits (also called colimits) exist in Ab.

(2) Inverse limits (also called limits) exist in Sets, Groups, Ab, Top, –

Pf of (2). Need

$$\begin{tikzcd} L \arrow[r, "\phi_i"] \arrow[dr, "\phi_j"'] & X_i \\ & X_j \arrow[u] \end{tikzcd}$$

$\forall i<j$

Let $I' = I$ with trivial p.o.

$\varprojlim_{I'} = \prod X_i$, with $\xrightarrow{\pi_i} X_i$ maps to the X_i

$L = \varprojlim_{I}$, so

$$\begin{tikzcd} L \arrow[r, "h"] \arrow[dr, "\phi_i"'] & \prod X_i \arrow[d, "\pi_i"] \\ & X_i \end{tikzcd}$$

for $y \in L$, $h(y) = (x_i)$, a sequence

$x_i = \phi_i(y)$

$\phi_{ij}(x_j) = x_i$

Claim $L = \{ (x_i) \in \prod X_i : \forall i<j,\ \phi_{ij}(x_j) = x_i \}$ with the maps $\phi_i((x_i)) = x_i$ is a limit of the system

Lecture 24 (2008-11-07)

11/7/08

direct limits exist in <u>R-Mod</u>

pf. $I \longrightarrow$ <u>R-Mod</u> $(M_i,\ \phi_{ij} : M_i \to M_j \text{ for } i \leq j)$

need $L = \varinjlim_{I} (M_i, \phi_{ij})$ with

$$\begin{tikzcd} M_i \arrow[r, "\phi_i"] \arrow[d, "\phi_{ij}"'] & L \\ M_j \arrow[ur, "\phi_j"'] & \end{tikzcd}$$

$\forall i \leq j$

note that coproducts exist in R-mod, because $M_i \longrightarrow \oplus M_i$
$m \longmapsto (0, 0, \ldots m, 0, 0)$

so we have

$$\begin{tikzcd} M_i \arrow[r, "\widetilde{\phi}_i"] \arrow[d, "\phi_{ij}"'] \arrow[dr, "\phi_i" near start] & \oplus M_i \arrow[d, "\widetilde{h}"] \\ M_j \arrow[ur, "\widetilde{\phi}_j"' near end] \arrow[r, "\phi_j"'] & L \end{tikzcd}$$

$\phi_i(m) = \widetilde{h}(\widetilde{\phi}_i(m)) =$
$\widetilde{h}(0, 0, \ldots \underset{\nwarrow ith}{m}, 0)$

Claim $L = \oplus M_i / \langle \widetilde{\phi}_i(m) - \widetilde{\phi}_j(\phi_{ij}(m)) \mid \begin{smallmatrix} i<j \in I \\ m \in M_i \end{smallmatrix} \rangle$ with the maps $\phi_i = q \circ \widetilde{\phi}_i$ is a colimit

$\widetilde{\phi}_i(m) \nearrow (0, 0, \ldots \underset{ith \nearrow}{m}, 0)$ $\qquad \widetilde{\phi}_j(\phi_{ij}(m)) \nwarrow (0, 0, \ldots \underset{\nwarrow jth}{\phi_i(m)}, \ldots 0)$

Pf. need. $\phi_j \circ \phi_{ij}(m) = \phi_i(m)\ \forall i<j,\ m \in M_i$

if $q \circ \widetilde{\phi}_j \circ \phi_{ij}(m) = q(0\ 0 \cdots \underset{\nwarrow jth}{\phi_{ij}(m)}\ 0)$ and

$q \circ \widetilde{\phi}_i(m) = q(0\ 0 \cdots \underset{i \nearrow}{m}\ 0)$

$\widetilde{\phi}_j \circ \phi_{ij}(m) =$

Prove universal property.

fibered products.

$$\begin{tikzcd} & X_1 \times_S X_2 \arrow[dl] \arrow[dr] & \\ X_1 \arrow[dr] & \circlearrowleft & X_2 \arrow[dl] \\ & S & \end{tikzcd}$$

$I =$

• corresponds to S

$$\varprojlim_{\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z} = \mathbb{Z}_p \subset \prod \mathbb{Z}/p^i\mathbb{Z}$$

Lecture 25 (2008-11-10)

11/10/08

field has characteristic $< \begin{matrix} p & \forall x \in F,\ px = 0 \\ 0 & \text{if } \nexists \end{matrix}$

in other words, generates the annihilator of the $\mathbb{Z}$-mod $(F, +)$.

every field has a prime subfield, for char p it's $\mathbb{F}_p$, for char 0 it's $\mathbb{Q}$

also, the prime subfield is the subring generated by 1.

If $F_1 \xrightarrow{\phi} F_2$ is a ring hom; ϕ must be injective since only additive subgroups of F_1 are $\{0\}$ and F_1, so kernel must be one of them

$\deg K/F = [K:F] = \dim_F K$

We have a map

$$\begin{tikzcd} K[t] \arrow[r] \arrow[dr] & K[t]/(t^n) \arrow[d] \\ & K[t]/(t^m) \end{tikzcd}$$

if $n > m$

so letting $I = \mathbb{N}$ we have an inverse system, with $\varprojlim\limits_{\mathbb{N}} K[t]/(t^n) = (p_1, p_2, \dots) =$

$\{a_0 + a_1 t + \cdots\} = K[[t]]$, formal power series

Exercise. $K((t))$, the field of fractions of $K[[t]]$, is really the field of formal Laurent series in t, i.e. $\{a_{-n}t^{-n} + a_{-n+1}t^{-n+1} + \cdots\}$

Thm. Let F be a field, $p(x) \in F[x]$ an irreducible polynomial, then there exists an extension K/F and an element $\theta \in K$, such that $p(\theta) = 0$,

$$\begin{tikzcd} a \in F \arrow[r, "i"] \arrow[dr] & K \ni \theta \arrow[d, "\delta"] \\ & L \ni \eta \end{tikzcd}$$

and if L/F is another extension with $\eta \in L : p(\eta) = 0$, then $\exists!\ K \xrightarrow{\delta} L$ with $\forall a \in F$, $\delta(a) = a$, and $\delta(\theta) = \eta$

Pf. Let $K = F[x]/(p)$

Note! $p \neq 0$, irred. $\Rightarrow$ (p) is maximal. $\Rightarrow$ K is a field.

Define $i : F \to K$, such that $\underbrace{F \to F[x] \xrightarrow{q} K}_{i}$, define $\theta = q(x)$.

$p(\theta) = p(q(x)) = q(p(x)) = 0.$

(2).
$$\begin{tikzcd}
F \arrow[r, "i"] \arrow[dr, "\phi"'] & L \arrow[r, phantom, "\ni"] & \eta \\
 & F[x] \arrow[u, "h"] \arrow[r, phantom, "\ni"] & x \arrow[u, mapsto]
\end{tikzcd}$$

By the universal property of polynomial rings, if we want a ring hom. for F and a distinguished element, there is a map from the polynomial ring to it, so h exists.

But $p(\eta)=0$, so $p(h(x))=0$, so $h(p(x))=0$, so $p(x)\in \operatorname{Ker}(h)$, so $h: F[x]\to L$ factors through

$$\begin{tikzcd}
F[x] \arrow[r, "h"] \arrow[d, "q"'] & L \\
F[x]/(p(x)) \arrow[ur, "\exists!"', "\sigma"] &
\end{tikzcd}$$

Thm Let $p(x)\in F[x]$ be irred. of deg n,
Then K, the root θ from above, satisfy: $1, \theta, \cdots, \theta^{n-1}$ is a basis for K/F, and $[K:F]=n$

Pf. Need: $F[x]/(p(x))$ has a basis given by images of $1, x, \cdots, x^{n-1}$.

Given any $v(x)$, by Euclidean algorithm, $v(x)=q(x)\cdot p(x)+r(x)$ where $\deg r(x)<n$, so any element in $F[x]/(p(x))$ is uniquely represented by $r(x)\longmapsto r(\theta)=a_0+\cdots+a_{n-1}\theta^{n-1}$.

Lecture 26 (2008-11-12)

$p(x) \in F[x]$ 11/12/08

$K = F[x]/(p)$

$\theta = x + (p)$ what is θ^{-1}? Since $p(\theta) = 0 = a_0 + a_1\theta + \cdots + a_n\theta^n$,

$$1 = \theta\left(\frac{-(a_1 + a_2\theta + \cdots + a_n\theta^{n-1})}{a_0}\right)$$

Def. given K/F, $\{a_i\} \in K$,

$F(\{a_i\}) = \bigcap_{\substack{L \supset F \\ \{a_i\} \subset L}} L$. Claim. $F(\{\alpha_i\}) = \left\{ \frac{p(\alpha_i)}{q(a_i)} \mid q(a_i) \neq 0 \right\} \subset K$.

Pf. Clearly everything of this form must be there, and it itself is a field.

Def. K/F is simple if $\exists \alpha \in K : K = F(\alpha)$

Ex. $K(x)$ is simple, $K(x,y)$ is not simple.

Thm. suppose $\delta_0 : F \xrightarrow{\sim} F'$, $p(x) \in F[x]$ irred.

$K = F[x]/(p) = F(\theta)$

$\delta_0 : F[x] \xrightarrow{\sim} F'[x]$

$\sum a_i x^i \longmapsto \sum a_i' x^i$ $\quad p'(x) = \delta_0(p(x)) \in F'(x)$

$a_i = \delta_0(a_i)$

L'/F', $\eta \in L' : p'(\eta) = 0$.

then

$$\begin{tikzcd}
\theta \in K \arrow[r, "\exists!\delta"] \arrow[d, dash] & L \ni \eta \arrow[d, dash] \\
F \arrow[r, "\delta_0"] & F'
\end{tikzcd}$$

$\exists!\ \delta : K \to L$ such that

(a) $\delta(a) = \delta_0(a)\ \forall a \in F$

(b) $\delta(\theta) = \eta$

Pf. need to construct

$K \to L$

need $F[x] \xrightarrow{\tilde{\delta}} L$, ring hom, with $p(x) \in Ker(\tilde{\delta})$

To construct $\tilde{\delta}$, need $F \to L$ (given by δ_0) $\quad \tilde{\delta}(a) = \delta_0(a)\ \forall a \in F$

and $\eta \in L$, $\tilde{\delta}(x) = \eta$ $\quad \tilde{\delta}(x) = \eta$

So get (a), (b) by construction

uniqueness by universal property of polynomial rings.

let K/F be an extension

Def. $\alpha \in K$ is algebraic over F if $\exists p \in F[x]$, $p \neq 0$, s.t. $p(\alpha) = 0$.

α is transcendental over F if not algebraic.

K/F is algebraic when $\forall \alpha \in K$, α is algebraic.

Prop. $\alpha \in K/F$ alg. over F, then $\exists!$ irred, monic $M_{\alpha/F}(x) \in F[x]$ such that $M_{\alpha/F}(\alpha) = 0$, and if $f(x) \in F[x]$ has $f(\alpha) = 0$, then $M_{\alpha/F}(x) \mid f(x)$.

Pf.. $F[x] \longrightarrow K$

$\sum a_i x^i \longmapsto \sum a_i \alpha^i$ sends 1 to 1,

and since α is algebraic, $\text{Ker} \neq 0$. Since $F[x]$ is a PID, Ker, an ideal of $F[x]$, has a generator, i.e. $\text{Ker} = (m_{\alpha/F}(x))$, and since $\text{Ker} \neq 0$, $m_{\alpha/F}(x) \neq 0$, and this is chosen to be monic.

Further, since Ker is a prime ideal, $m_{\alpha/F}(x)$ is irreducible and $m_{\alpha/F}(\alpha) = 0$.

Cor. $F(\alpha) \simeq K[x]/(m_{\alpha/F}(x))$

Pf. $(m_{\alpha/F}(x))$ nonzero prime ideal $\Rightarrow$ field.

Cor. $[F(\alpha) : F] = \deg m_{\alpha/F}(x)$

Def. $\alpha \in K/F$ is algebraic of $\deg n = [F(\alpha) : F]$

Prop. $\alpha \in K/F$ is algebraic iff $\exists L \ni \alpha$, $K/L/F$, where $[L : F]$ is finite.

Pf. $\Leftarrow$ Say $\alpha \in L$, $K/L/F$, $[L:F] = n < \infty$, $\rightarrow$ (stupid)

$\Rightarrow$ $1, \alpha, \ldots, \alpha^n$ are linearly dependent over F, so $\exists a_i \in F$ with $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, not all $a_i = 0$, so if $f(x) = \sum a_i x^i \in F[x]$, $f \neq 0$, $f(\alpha) = 0$, α is algebraic.

Cor. K/F finite $\Rightarrow$ K is algebraic $/F$

Thm. If $K/L/F$, $[K:F] = [K:L][L:F]$

finite case: Suppose $\alpha_1, \ldots, \alpha_m$ is basis for K/L, $\beta_1, \ldots, \beta_n$ for L/F. Claim that $\{\alpha_i \beta_j\}$ is a basis for K/F. Pf. let $\gamma \in K$. $\gamma = \sum a_i \alpha_i$, $a_i \in L$, and $a_i = \sum b_{ij} \beta_j$, so $\gamma = \sum b_{ij} \alpha_i \beta_j$, so spans. Suppose $\sum b_{ij} \alpha_i \beta_j = 0$. Then $\sum_i \left(\sum_j b_{ij} \beta_j\right) \alpha_i = 0$,

So $\sum_i \underbrace{b_{ij}}_{\in F} \beta_j = 0 \ \forall i$, so $b_{ij} = 0 \ \forall_{ij} = 0$.

Lecture 27 (2008-11-14)

11/14/08

If $K/L/F$, $[K:F] = [K:L][L:F]$

Useful example: $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$ since $\mathbb{Q}(\sqrt{2})$ has degree 2, $\mathbb{Q}(\sqrt[3]{2})$ has degree 3.

Prop. If

$$\begin{tikzcd}
& M = K(\alpha) \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & L = F(\alpha) \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

, $[M:K] \leq [L:F]$

Lemma. For algebraic $\alpha \in L/F$, and $f \in F[x]$ has $f(\alpha) = 0$, then $m_{\alpha/F}(x) \mid f(x)$

Pf. $f(x) = q(x)\, m_{\alpha/F}(x) + r(x)$

$0 = f(\alpha) = q(\alpha)\, m_{\alpha/F}(\alpha) + r(\alpha)$, so $r(\alpha) = 0$, but $\deg r < \deg m_{\alpha/F}$, so $r = 0$

Pf. Since $K[x] \ni m_{\alpha/K}(x) \mid m_{\alpha/F}(x) \in F[x] \subset K[x]$, $\deg(m_{\alpha/K}) \leq \deg(m_{\alpha/F})$.

Ex. If $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$, $\alpha = \sqrt[3]{2}\,\zeta_3$, $[K(\alpha):K] = [K(\zeta_3):K] = 2 \leq 3 = [F(\alpha):F]$

Def. K/F is finitely generated if $\exists \alpha_1, \dots, \alpha_n \in K$: $K = F(\alpha_1, \dots, \alpha_n)$.

Since $K = F(\alpha_1, \dots, \alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$, and defining $F_i = F(\alpha_1, \dots, \alpha_i)$,

$[F_i : F_{i-1}] \leq [F(\alpha_i):F]$, so $[F(\alpha_1, \dots, \alpha_n):F] \leq \prod [F(\alpha_i):F]$

Thm. K/F is finite $\Leftrightarrow$ $F(\alpha_1, \dots, \alpha_n)$, α_i algebraic over F.

Pf. $\Leftarrow$ $[K:F] \leq \prod \deg(\alpha_i) < \infty$

$\Rightarrow$ K/F is finite, i.e. K is a finite dimensional F-vector space, so let $\alpha_1, \dots, \alpha_n$ be a basis for K. Clearly, $K = F(\alpha_1, \dots, \alpha_n)$, and

Recall $\alpha \in K/F$ is algebraic iff. $\exists$ intermediate field L, $K/L/F$, with $\alpha \in L$, such that $[L:F] < \infty$. Hence the α_i are algebraic.

Cor. L/F, $K = \{\alpha \in L : \alpha \text{ is algebraic over } F\} \subset L$ is a subfield.

Pf. Let $\alpha_1, \alpha_2 \in K$. Consider $F(\alpha_1, \alpha_2)/F$, finite by above, so $F(\alpha_1, \alpha_2) \subset K$. This subfield is closed under operations, so so is K.
for any α_1, α_2

Thm. $K/L/F$, if K/L and L/F are algebraic, K/F is algebraic.

Pf. Exercise.

Def. If

$$\begin{tikzcd}
& K \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[r, dash] \arrow[dr, dash] & K_1K_2 \arrow[r, dash] & K_2 \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

, $K_1K_2 = \{k_1 k_2\} \subset K$ is a subfield.

In this situation, $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$; since if α_i is a basis of K_1/F, β_i a basis of K_2/F,

$$K_1K_2 = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_{m_2}) = K_1(\beta_1, \ldots, \beta_{m_2})$$

Lecture 28 (2008-11-17)

11/17/08

Def. An extension K/F is a splitting field for $f(x)$ over F if $f(x) = c\prod(x-\alpha_i)$, $\alpha_i \in K$, and this is not true for any L with $K/L/F$

Thm. $\forall f(x) \in F[x]$, $\exists E/F$: $f(x) = c\prod(x-\alpha_i)$, $\alpha_i \in E$, and $\forall E$ thus described, $\exists K$ with $E/K/F$ such that K is a splitting field.

Pf. induction on degree, then check $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ must be in every splitting field, and worksitself.

Thm. K a splitting field for $f \in F[x]$, $\deg(f) = n$, then $[K:F] \leq n!$

Pf. induction on degree

Thm. If $F \xrightarrow[\phi]{\sim} F'$ is an isom, $f \in F[x]$, $f' = \phi(f)$, E splitting field of f over F, E' splitting field of f' over F', $\exists\, \sigma$:

$$\begin{tikzcd} E \arrow[r, "\sigma", "\sim"'] \arrow[d, dash] & E' \arrow[d, dash] \\ F \arrow[r, "\phi", "\sim"'] & F' \end{tikzcd}$$

Cor. Any two splitting fields of $f(x)$ are isomorphic.

Pf. Let ϕ be <u>id</u>.

Pf.

$$\begin{tikzcd} E \arrow[dr, dash] & & & E' \\ & F[\alpha] \arrow[r, "\sigma"] \arrow[d, dash] & F'[\beta] \arrow[ur, dash] \arrow[d, dash] & \\ & F \arrow[r, "\phi", "\sim"'] & F' & \end{tikzcd}$$

, zip up by induction on degree

Def. $\bar{F}/F$ is an algebraic closure if (a) $\bar{F}/F$ algebraic, (b) $\forall f \in F[x]$, $f(x)$ splits completely in $\bar{F}$

Def. A field K is algebraically closed if $\forall f \in K[x]$, $\deg(f) > 0$, has a root in K, $\exists \alpha \in K$: $f(\alpha) = 0$

Prop. An algebraic closure is algebraically closed

Thm. $\exists \bar{F}/F$ an algebraic closure

Pf. Lemma. $\exists K/F$ which is algebraically closed

Pf. Let $R = F[\{x_f\}_{f \in F[x],\ \text{monic, irred, non constant}}]$, $I = (\{f(x_f)\}_{f \in F[x],\ \text{monic, irred, non constant}})$,

Claim. $I \neq R$, i.e. $1 \notin I$, since if $1 \in I$, $1 = \sum_{i=1}^{n} g_i(x_{f_1}, \dots, x_{f_m}) f_i(x_{f_i})$, $m \geq n$.

But if this is the case, no matter what we plug in for the x's, it is true; let $x_{n+1}, \dots, x_m = 0$, plug in α_i, a root of f_i, for x_{f_i}. $1 \neq 0$, oops. So

By AC, I is contained in a maximal ideal M, $K_1 = R/M$ is a field, and over K_1 any $f \in F[x]$ has a root, α_f = the image of x_f. Let $K = F \cup K_1 \cup K_2 \cup \dots$ K_2 = same process applied to K_1. finally $\bar{F} = \{\alpha \in K : \alpha \text{ is algebraic over } F\}$

Lecture 29 (2008-11-19)

11/19/08

<u>Thm</u>. F field, E/F algebraic, $\sigma : F \to L$, then L algebraically closed field

$\exists \tilde{\sigma}$:

$$\begin{tikzcd} E \arrow[r, dash, "\tilde{\sigma}"] & L \\ F \arrow[u, dash] \arrow[ur, dash, "\sigma"'] & \end{tikzcd}$$

Pf. (K, γ), $F \subset K \subset E$,

$$\begin{tikzcd} K \arrow[r, dash, "\gamma"] & L \\ F \arrow[u, dash] \arrow[ur, dash, "\sigma"'] & \end{tikzcd}$$

$S = \{(K, \gamma)\}$

$(K, \gamma) < (K', \gamma')$ if $K \subset K'$, $\gamma'|_K = \gamma$

S a poset.

$C \subset S$ a chain, consider $K_C = \bigcup_{(K,\gamma) \in C} K$

$\gamma_C : K_C \to L$

$a \in K_C \Rightarrow a \in K$ with $(K, \gamma) \in C$

define $\gamma_C(a)$

exists a maximal element (K_m, γ_m)

Claim. $K_m \overset{?}{=} E$

Cor. Any two algebraic closures of F are isomorphic.

$$\begin{tikzcd} \bar{F}' \arrow[r] & \bar{F} \\ F \arrow[u] \arrow[ur] & \end{tikzcd}$$

Lemma. any endomorphism of an alg. extension is an automorphism

Def. $f(x) \in F[x]$ is separable if it has no multiple roots in $\bar{F}$, α is separable if $m_{\alpha/F}$ is separable.

Prop. α is a multiple root of f iff $f(\alpha) = f'(\alpha) = 0$

Cor. $\text{char}(F) = 0$, f irred. $\Rightarrow$ f separable

$\text{char}(F) = p$, f irred. $\Rightarrow$ every root has mult. p^e for some $e \geq 0$.

Pf. $\gcd(f(x), f'(x)) \mid f(x)$, but $\deg(f'(x)) < \deg(f(x))$, so $\deg \gcd(f', f) < \deg(f)$, so $\gcd(f, f') = 1$ since f is irred.

F is perfect if either char $= 0$, or char $= p$ and F^p, the image of the Frobenius map, is F.

Every finite field is perfect.

Frob: $F \to F$ injective hence bijective

Prop. F is perfect $\Longleftrightarrow$ every $f(x)$ irred $\in F[x]$ is separable

every alg. extn. of a perfect field is separable + perfect.

Pf. OK in char 0, suppose char $= p$. Then $F = F^p$, $f(x)$ suppose irred but not separable $\Rightarrow f(x) = g(x^p)$, $f(x) = \sum a_i x^i$, $a_i \in F$

$a_i = b_i^p$, $b_i \in F$ each a jp

$f(x) = \sum a_i x^i$

$= \left(\sum b_{jp} x^j\right)^p \Rightarrow f(x)$ not irred.

$\Leftarrow$ $a \in F$, $f(x) = x^p - a$ not separable $\Rightarrow$ not irred. $\Rightarrow$ has a root b, so $b^p = a$ so $a \in F^p$

Lecture 30 (2008-11-24)

11/24/08

Prop. $f \in F[x]$, $E =$ spf of $f \Rightarrow |\mathrm{Aut}(E/F)| \leq [E:F]$
with equality when f is separable

Lemma. Given $\tau : F \xrightarrow{\sim} F'$ $\quad$ f with no repeated factors
$f(x) \mapsto f'(x)$
$E =$ spf of f $\quad$ $E' =$ spf of f'

then $\#\{\sigma : E \xrightarrow{\sim} E'$ with $\sigma|_F = \tau\} \leq [E:F]$ and
equality if $f(x)$ is separable

Proof. $[E:F] = 1$, trivial. Otherwise, $p(x) | f(x)$ irred, $\alpha \in E$ with $p(\alpha) = 0$.
Consider $\sigma : E \to E'$, $\sigma(\alpha) = \beta$, $p'(\beta) = 0$.

$\forall \beta$, $\exists!$.

$$\begin{tikzcd}
F(\alpha) \arrow[r, "\tilde{\tau}"] & F'(\beta) \\
F \arrow[u, dash] \arrow[r, "\tau"] & F \arrow[u, dash]
\end{tikzcd}$$

\# of choices of β for where to send $\alpha =$
\# of distinct roots of $p'(\beta) \leq dg(p) = [F(\alpha):F]$,
with equality if p is separable

Then

$$\begin{tikzcd}
E & E' \\
F(\alpha) \arrow[u, dash] \arrow[r, "\tilde{\tau}"] & F'(\beta) \arrow[u, dash] \\
F \arrow[u, dash] \arrow[r, "\tau"] & F' \arrow[u, dash]
\end{tikzcd}$$

Def E/F is Galois if separable + normal $\rightarrow \exists S \subset F[x] : E = spf(S)$

Note: E/F is finite Galois $\Rightarrow$ splitting field of a separable polynomial

Artin's Theorem: If $G < \mathrm{Aut}(K)$, $|G|$ finite, then $[K:K^G] = |G|$,
i.e. $\mathrm{Aut}(K/K^G) = G$, and K/K^G is Galois.

Proof will show K/K^G is sp. field of sep. poly. Denote $F = K^G$.
$\alpha \in K$, $G\alpha = \{\sigma_1\alpha, \sigma_2\alpha, \dots, \sigma_r\alpha\} = \{\alpha_1, \dots, \alpha_r\}$ is orbit of α under G,
the distinct places α can be sent, so $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ if $i \neq j$, so $\tau \in G$,
$\tau\sigma_i(\alpha) \in G\alpha = \sigma_j$ for some j. So τ gives permutation of
$\{\alpha_1, \dots, \alpha_r\}$, so α is a root of $f(x) = \prod(x - \alpha_i)$, so every
element of K is root of separable poly, so K/F is finite.
$K = F(\beta_1, \dots, \beta_n)$, $f_i = m_{\beta_i/F}(x)$, separable; $f =$ prod of distinct f_i,
$K =$ sp. field of separable f, $[K:F] = |\mathrm{Aut}(K/F)| \geq G$

$|G| \geq [K:F]$, $G = \{\sigma_1, \ldots, \sigma_n\}$, $n = |G|$,
$\omega_1, \ldots, \omega_m \in K$ indep. over F

$A = (\sigma_i(\omega_j))_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}}$ Suppose $m > n$, then non-zero solution to

$$A^T \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = 0, \qquad A^T = \begin{pmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_m) \\ \vdots & & \vdots \\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_m) \end{pmatrix}$$

take one with minimal # of non-zero elements may assume
the least is 1, and is last in the vector

$$\begin{pmatrix} 0 \\ \beta_i \\ \vdots \\ 1 \\ \hline \vdots \\ 0 \end{pmatrix}$$

$$\sum_{j=1}^{r-1} \sigma_i(\omega_j)\beta_j + \sigma_i(\omega_r) = 0$$

Claim: not all β_i in F since independent ω_j

some $\beta_i \notin F$

Lecture 31 (2008-12-03)

12/3/08

Roots of unity

k field, $k \hookrightarrow \bar{k}$ an alg. closure of k.

$x^n - 1 \in k[x]$, study roots of this

if char $k = p > 0$, and $n = p^r$, $x^{p^r} - 1 = (x-1)^{p^r}$ has only one root.

Now assume char$(k) \nmid n$. Then $x^n - 1$ is separable : $(x^n-1)' = nx^{n-1}$, only root of this is 0. $\Rightarrow x^n - 1$ has n distinct roots in $\bar{k}$. These form a finite subgroup of $\bar{k}^\times$, called μ_n, which is therefore cyclic. Let ζ be a generator of μ_n.

Prop. $k(\zeta)/k$ is Galois with $\mathrm{Gal}(k(\zeta)/k)$ a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Pf. To see that $k(\zeta)/k$ is normal, we must prove any $\sigma : k(\zeta) \to \bar{k}$ induces an automorphism of $k(\zeta)$. Since $(\sigma(\zeta))^n = \sigma(\zeta^n) = 1$, $\sigma(\zeta)$ is another primitive n^{th} root of unity. Any automorphism $k(\zeta) \xrightarrow{f} k(\zeta)$ over k is determined by $f(\zeta)$ so $f(\zeta) = \zeta^i$ for some $i \in (\mathbb{Z}/n\mathbb{Z})^\times$

We have a monomorphism of $\mathrm{Gal}(k(\zeta)/k)$ into $(\mathbb{Z}/n\mathbb{Z})^\times$ (since the $\zeta \to \zeta^i$ for each $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ may be counting automorphisms twice, of if $\zeta \in k$ to begin with).

Prop. If $k = \mathbb{Q}$, then $\mathrm{Gal}(k(\zeta)/k) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Pf. Since we have a monomorphism, suffices to prove $[k(\zeta):k] = \#(\mathbb{Z}/n\mathbb{Z})^\times = \phi(n)$. Let $f(x)$ be the min poly of ζ. Thus $f(x)g(x) = x^n - 1$ for some g. By Gauss' lemma, $f(x), g(x) \in \mathbb{Z}[x]$.

$$x^n - 1 = \prod_{d \mid n} \phi_d(x)$$

By Gauss's lemma, $\phi_d(x)$ has integer coefficients

$\phi_n(x) \in \mathbb{Z}[x]$ is irreducible of degree $\phi(n)$

Corollary. If $\gcd(n,m)=1$, $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$

Pf. Suffices to show the compostum has largest possible degree,

$$\underset{\substack{\downarrow \\ \text{primitive } mn^{th} \text{ root of unity} \\ \text{so this is } \phi(mn)}}{[\mathbb{Q}[\zeta_n, \zeta_m] : \mathbb{Q}]} = \underset{\substack{\| \\ \phi(m)}}{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]}\ \underset{\substack{\| \\ \phi(n)}}{[\mathbb{Q}(\zeta_m) : \mathbb{Q}]}$$

$$\phi(mn) = \phi(m)\phi(n) \checkmark$$

~~Kummer's Theorem, Suppose k contains a primitive roo+~~

Kummer's Theory, Artin-Schrier Theory

Let K/k be Galois,

$$N : K \longrightarrow k \qquad N(\alpha) = \prod_{\sigma \in \text{Gal}} \sigma(\alpha) \quad \in k$$

$$Tr : K \longrightarrow k \qquad Tr(\alpha) = \sum_{\sigma \in \text{Gal}} \sigma(\alpha) \quad \in k$$

Lecture 32 (2008-12-08)

12/8/08

$n \geq 1$; $[\mathbb{Q}[\zeta_n):\mathbb{Q}] = \phi(n)$

$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

$\sigma_a(\zeta_n) = \zeta_n^a \longleftrightarrow \bar{a}$

$$\begin{tikzcd}
\mathbb{Q}(\zeta_m) \arrow[d, dash] \arrow[dd, dash, bend left=60, "G_m"] \\
\mathbb{Q}(\zeta_n) \arrow[d, dash] \arrow[d, dash, bend right=60, "G_n"'] \\
\mathbb{Q}
\end{tikzcd}$$

If $n|m$, $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_m)$ since $\zeta_m^{m/n} = \zeta_n$

$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longleftarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$

$$\begin{tikzcd}
G_m \arrow[r] \arrow[d, equal] & G_n \arrow[d, equal] \\
(\mathbb{Z}/m\mathbb{Z})^\times \arrow[r] & (\mathbb{Z}/n\mathbb{Z})^\times \\
\bar{a} \arrow[r, mapsto] & \bar{a} \bmod n
\end{tikzcd}$$

So $G_1, G_2, \ldots$ is an inverse system parametrized by $I = \mathbb{N}$, with maps $\phi_{mn}: G_m \to G_n$ when $n|m$.

$$\varprojlim_{n\in I} G_n = \varprojlim_{n\in I} (\mathbb{Z}/n\mathbb{Z})^\times \subset \varprojlim_{n \in I} (\mathbb{Z}/n\mathbb{Z}) = \hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$$

Exercise: $\varprojlim_{n\in I} G_n = \hat{\mathbb{Z}}^\times$

$n \geq 1$, $n|m$, $\exists!\ \mathbb{F}_{p^n}$. $\phi: \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$, $x \longmapsto x^p$ is an automorphism of $\mathbb{F}_{p^n}$

$\phi^n(x)$ $x \longmapsto x^{p^n} = x$ so $\mathrm{ord}(\phi) / n$. But if $\mathrm{ord}(\phi) = d < n$, $x^{p^d} - x = 0$ $\forall x \in \mathbb{F}_{p^n}$; impossible, can only be p^d solutions. Thus $\mathrm{ord}(\phi) = n$. So $\langle\phi\rangle \subset \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. But $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, so $\langle\phi\rangle$ must be entire thing.

Subfields of $\mathbb{F}_{p^n}$ $\longleftrightarrow$ subgroups of $\mathbb{Z}/n\mathbb{Z}$

Primitive element theorem: $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$ for some θ (e.g., θ a generator of $\mathbb{F}_{p^n}^\times$) $\Rightarrow$ $\exists$ an irred. $f(x) \in \mathbb{F}_p[x]$ of deg n. Suppose $f(x) \in \mathbb{F}_p[x]$ is irreducible of deg d/n. Spfield $= \mathbb{F}_{p^d} \Rightarrow f / x^{p^n} - x$

Prop. $x^{p^n} - x = \prod f$ of f irred. $\in \mathbb{F}_p[x]$ of deg. $/n$.

Let $\#$ irred. poly of deg $n = \Psi(n)$. $p^n = \sum_{d/n} d\,\Psi(d)$, so by Mobius inversion $\Psi(n) = \frac{1}{n} \sum_{d/n} \mu(d) p^{n/d}$

If E/F Galois (splitting field of $S \subset \mathbb{F}[x]$, set of sep. poly)

$G = \mathrm{Aut}(E/F)$

Let $G' = \varprojlim_{I} G_K$, for $G_K = \mathrm{Gal}(K/F)$ $I = \left\{ \text{all finite } \begin{tikzcd}[row sep=small, column sep=small] & E \arrow[dl, dash] \arrow[dd, dash] \\ K \arrow[dr, dash] & \\ & F \end{tikzcd} \right\}$

$\phi : G \longrightarrow G'$

$\sigma \longmapsto (\sigma|_K)_{K \in I}$ ordered by inclusion since if $K \subset K'$, $(\sigma|_{K'})|_K = \sigma|_K$

Theorem. ϕ is an isomorphism

Note: G' is a topological group (compact Hausdorff)

1-1 correspondence

$$\left\{ \text{subfields } \begin{tikzcd}[row sep=small, column sep=small] & E \arrow[dl, dash] \arrow[dd, dash] \\ L \arrow[dr, dash] & \\ & F \end{tikzcd} \right\} \longleftrightarrow \{ \text{closed subgroups } H < G \}$$

1:1 correspondence

$$\left\{ \begin{tikzcd}[row sep=small, column sep=small] & E \arrow[dl, dash] \arrow[dd, dash] \\ L \arrow[dr, dash] & \\ & F \end{tikzcd} [L:F] \text{ finite} \right\} \longleftrightarrow \{ \text{open subgroups} \}$$

Lecture 33 (2008-12-10)

12/10/08

$$\begin{tikzcd} E \arrow[dd, dash, "G"'] \arrow[dr, dash] & \\ & K \arrow[dl, dash] \\ F & \end{tikzcd}$$

$G = \mathrm{Aut}(E/F)$, E/F Galois

$I = \{K : F \subset K \subset E,\ K/F \text{ finite Galois}\}$

I a poset by inclusion

$K \subset K'$,
$$\begin{tikzcd} G_K & G_{K'} \arrow[l, "\phi_{K'K}"'] \\ \sigma|_K \arrow[u, phantom, sloped, "\in"] & \sigma \arrow[l, mapsto] \arrow[u, phantom, sloped, "\in"] \end{tikzcd}$$
$G_K = \mathrm{Gal}(K/F)$

Let $G' = \varprojlim_I G_K$. $G' \subset \prod_K \mathrm{Gal}(K/F)$

$$\begin{tikzcd} {} \arrow[drr, "\pi_{K'}"'] & & \prod_K \mathrm{Gal}(K/F) \arrow[ll, "\phi_{K'K}"'] \arrow[d, "\pi_K"] \\ & & G_K \end{tikzcd}$$

$\phi_{K'K} \circ \pi_{K'} = \pi_K$

Construction: $\phi : G \to G'$

$\sigma \longmapsto (\sigma|_K)_{K \in I}$

well-defined since $(\sigma|_{K'})|_K = \sigma|_K$

Thm. ϕ is an isomorphism

Pf. (injective) Let $\sigma \in G$ with $\sigma(\alpha) \neq \alpha$ for some $\alpha \in E$

Let K_α = spf of $m_{\alpha/F}(x)$

$\sigma|_{K_\alpha}(\alpha) \neq \alpha \Rightarrow \sigma|_{K_\alpha} \neq id \Rightarrow \phi(\sigma) \neq id \Rightarrow \phi$ is injective

(surjective) $\psi : G' \to G$

$$(\sigma|_K)_{K \in I} \longmapsto (\alpha \mapsto \sigma_{K_\alpha}(\alpha))$$

This is an automorphism: $\psi(\sigma)(\alpha+\beta)$

$$\begin{tikzcd} K_{\alpha,\beta} \arrow[d, dash] \\ K_{\alpha+\beta} \arrow[d, dash] \\ F \end{tikzcd}$$

$$\begin{aligned} &= \sigma_{K_{\alpha+\beta}}(\alpha+\beta) = \sigma_{K_{\alpha,\beta}}(\alpha+\beta) \\ &= \sigma_{K_{\alpha,\beta}}(\alpha) + \sigma_{K_{\alpha,\beta}}(\beta) \\ &= \sigma_{K_\alpha}(\alpha) + \sigma_{K_\beta}(\beta) = \psi(\sigma)(\alpha) + \psi(\sigma)(\beta) \end{aligned}$$

(Same proof for multiplicatio)

Claim: $\phi \circ \psi = id$ (i.e. $\forall K \in I$, $(\sigma_K)_{K \in I}|K = \sigma_K$)

Since has a right inverse, surjective.

G' is a topological group since

$G' \subset \prod_{K \in I} G_K$, and G_K has finite discrete top

so has Tychonoff top.

Prop: G' is closed

Cor: G' is compact (since closed subset of compact is compact) and Hausdorff (since ambient space is Hausdorff)

Pf. $G' = \{ (G_K) \in \prod_K G_K \mid \phi_{K'K} \sigma_{K'} = \sigma_K \}$

$$= \bigcap \{ (\sigma_{K'}) \mid \sigma_{K'}|_K = \sigma_K \}$$

$$= \bigcap \underset{\substack{\uparrow \\ \text{continuous}}}{\pi_{K',K}} \Big(\underbrace{\{(\sigma_{K'}, \sigma_K) \mid \sigma_{K'}|_K = \sigma_K\}}_{\text{closed}} \Big)$$

$=$ closed

Lemma. $H < G$ is open iff $\exists K \in I$ and $H_K < G_K$: $H = \pi_K^{-1}(H_K)$

Pf. $H = \bigcup_i U_i$, $U_i = \pi_{K_i}^{-1}(V_i)$, $V_i \subset G_K$ any subset
inv. lim. of directed system (automatically open)

$$H \supset U_i \Rightarrow H \supset \langle U_i \rangle = \pi_{K_i}^{-1}(\langle V_i \rangle)$$

$$\Rightarrow H \supset \operatorname{Ker}(\pi_{K_i}) = \pi_{K_i}^{-1}(\{1\})$$

$$0 \longrightarrow \operatorname{Ker}(\pi_{K_i}) \longrightarrow G \xrightarrow{\pi_{K_i}} G_{K_i} \longrightarrow 0$$

$H \supset \operatorname{Ker}(\pi_{K_i}) \longleftrightarrow G_{K_i} \supset H_{K_i}$ } since subgroups containing kernel have 1:1 correspondence to intermediate subgroups, by 4th iso thm.

Cor. any open subgroup is closed

Thm. 1:1 correspondence

$$\{L \mid F \subset L \subset E,\ [L:F] \text{ finite}\} \longleftrightarrow \{H < G \text{ open}\}$$

$$L \longmapsto \operatorname{Aut}(E/L)$$

$$E^H \longleftarrow\!\shortmid\ H$$

inclusion reversing, and L/F Galois $\Leftrightarrow H \trianglelefteq G$

12/10/08

Pf. Given L, let $H = \mathrm{Aut}(E/L) \subset G$

Claim. H is open in G

Let $K \supset L$ be such that K/F finite Galois

$G \to G_K$

When will $\sigma \in G$ fix L?

$\sigma|_L = \mathrm{id} \Leftrightarrow \sigma|_K(\alpha) = \alpha \quad \forall \alpha \in L$

$$\begin{tikzcd}[row sep=small] H_{K/L} \subset G_K \arrow[d, phantom, "\shortparallel"] & \leftrightarrow & \sigma|_K \in H_{K/L} \\ \mathrm{Gal}(K/L) & \longleftrightarrow & \sigma \in \pi_K^{-1}(H_{K/L}) \end{tikzcd}$$

so H is open. Conversely, $H \subset G$ is open $\Rightarrow H = \pi_K^{-1}(H_K)$, $H_K \leq G_K \Rightarrow H_K = \mathrm{Gal}(K/L)$ for some $L \subset K$, so $E^H : F$ finite

inverse to each other due to finite Gal correspondence

Prop. Let $F \subset L \subset E$ be any intermediate extension. Then $\mathrm{Gal}(E/L)$ is closed.

Pf. $G(E/L) = \cap\, G(E/F(\alpha))$, $\alpha \in L$

$\boxed{H \subset G \text{ closed} \Leftrightarrow H = \cap\, \pi_K^{-1}\pi_K(H)}$,

and we have $G(E/F(\alpha)) = \pi_{K_\alpha}^{-1}\, G(K_\alpha/F(\alpha))$

Claim: $E^{G(E/L)} = L$

Pf: $\supset$ (obvious from definitions)

For other direction, if $\alpha \notin L$, then $\exists\, \sigma : E \to E$ with $\sigma|_L = \mathrm{id}$ but $\sigma(\alpha) \neq \alpha$.

$$\begin{tikzcd} E \arrow[d, dash] \arrow[dr, dash] & \\ L \arrow[r, dash] \arrow[d, dash, "\}\text{ forgot about}"] & L(\alpha) \\ F & \end{tikzcd}$$

β, another root, $\sigma(\alpha) = \beta$

E is Galois over F, so it is spf of some polynomials, but E is Galois over L as well by taking some polynomials considered over L

Claim. $\mathrm{Gal}(E/E^H) = \overline{H}$ (top. closure)

Pf. $\mathrm{Gal}(E/E^H) = H'$, closed $\Rightarrow H' = \bigcap_K \pi_K^{-1}\underbrace{\pi_K(H')}_{H_K = \mathrm{Gal}(K/L_K)}$

$H' = \bigcap_K \pi_K^{-1}(\mathrm{Gal}(K/L_K)) = \bigcap_K \{\sigma \mid \sigma|_K(\alpha) = \alpha \ \forall \alpha \in E^H \cap K\}$

$L_K = K^{H_K} = K^{H'} = K \cap E^{H'}$

$\overline{H} = \{\sigma \mid \sigma(\alpha) = \alpha \ \forall \alpha \in E^H\}$

$H \subset G$

$\overline{H} = \cap\, \pi_K^{-1}\pi_K(H)$

So $H \subset G$

$$\bar{H} = \bigcap \pi_K^{-1} \pi_K(H)$$

$$L \longrightarrow \text{closed subgroup}$$

$$E^H \longleftarrow H, \text{closed}$$

Exaple. $E = \mathbb{Q}(\mu_\infty) = \mathbb{Q}(\zeta_3, \zeta_4, \zeta_5, \ldots)$

$$\begin{tikzcd}
E \arrow[d, dash] & \\
\mathbb{Q}(\zeta_n) \arrow[d, dash] & \\
\mathbb{Q} \arrow[r] & (\mathbb{Z}/n\mathbb{Z})^\times
\end{tikzcd}$$

$$\varprojlim (\mathbb{Z}/n\mathbb{Z})^\times$$
$$\parallel$$
$$(\mathbb{Z})^\times$$
$$\cup$$
$$\prod_{p \neq q} \mathbb{Z}_p^\times = \operatorname{Gal}(\mathbb{Q}(\zeta_{q^\infty}))$$

$$\begin{tikzcd}
\overline{\mathbb{F}_p} \arrow[dd, dash, "{\varprojlim(\mathbb{Z}/n\mathbb{Z}) = \hat{\mathbb{Z}}}"'] \arrow[dr, dash] & & \\
& \mathbb{F}_{p^n} & \\
\mathbb{F}_p \arrow[ur, dash] & & (\mathbb{Z}/n\mathbb{Z}) \arrow[ll]
\end{tikzcd}
\qquad
\begin{tikzcd}
\overline{\mathbb{Q}} \arrow[dd, dash, "?"'] \arrow[dr, dash] & \\
& \mathbb{Q}(\alpha) \\
\mathbb{Q} \arrow[ur, dash] &
\end{tikzcd}$$