Last revised: May 16, 2014

A.Miller M542
www.math.wisc.edu/∼miller/

# 1 Finite abelian groups

**Theorem 1.1** *(Chinese remainder theorem) Given $n, m$ relatively prime integers for every $i, j \in \mathbb{Z}$ there is an $x \in \mathbb{Z}$ such that $x = i$ mod $n$ and $x = j$ mod $m$.*

**Theorem 1.2** *$\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ iff $n, m$ are relatively prime.*

**Lemma 1.3** *Suppose $n, m$ are relatively prime, $G$ is a finite abelian group such that $x^{nm} = e$ for every $x \in G$. Let $G_n = \{x \in G : x^n = e\}$ and $G_m = \{x \in G : x^m = e\}$. Then*

- *$G_n$ and $G_m$ are subgroups of $G$,*
- *$G_n \cap G_m = \{e\}$,*
- *$G_n G_m = G$, and therefore*
- *$G \simeq G_n \times G_m$*

**Corollary 1.4** *(Decomposition into p-groups) Suppose $G$ is an abelian group and $|G| = p_1^{i_1} \cdot p_2^{i_2} \cdots p_n^{i_n}$ where $p_1 < p_2 < \cdots < p_n$ are primes. Then*

$$G \simeq G_1 \times G_2 \times \cdots \times G_n$$

*where for each $j$ if $x \in G_j$ then $x^{n_j} = e$ where $n_j = p_j^{i_j}$.*

**Lemma 1.5** *Suppose $G$ is a finite abelian $p$-group and $a \in G$ has maximum order, then there exists a subgroup $K \subseteq G$ such that*

- *$\langle a \rangle \cdot K = G$ and*
- *$\langle a \rangle \cap K = \{e\}$.*

The proof given in class is like the one in Gallian or Judson.

**Theorem 1.6** *Any finite abelian group is isomorphic to a product of cyclic groups each of which has prime-power order.*

**Theorem 1.7** *(Uniqueness) Suppose*

$$C_{p^{n_1}} \times C_{p^{n_1}} \times \cdots \times C_{p^{n_k}} \simeq C_{p^{m_1}} \times C_{p^{m_1}} \times \cdots \times C_{p^{m_l}}$$

*where* $n_1 \geq n_2 \geq \cdots n_k \geq 1$ *and* $m_1 \geq m_2 \geq \cdots m_l \geq 1$*. Then* $k = l$ *and* $n_i = m_i$ *for all* $i$*.*

# 2 Group Actions and Sylow Theorems

For the group $G$ acting on the set $X$ the orbit of $a \in X$ is

$$orb(a) =^{def} \{ga \ : \ g \in G\} \subseteq X.$$

**Proposition 2.1** *Orbits are either disjoint or the same.*

For a given group action of group $G$ on set $X$, define $Stab(a) = \{g \in G \ : \ ga = a\}$ for each $a \in X$. Called stabilizer or fixed subgroup.

**Proposition 2.2** $Stab(a)$ *is a subgroup of* $G$*.*

For $H \subseteq G$ a subgroup the index of $H$, $[G : H]$ is the number of $H$-cosets, $|\{gH \ : \ g \in G\}|$. Lagrange's Theorem says $|G| = [G : H] \cdot |H|$.

**Proposition 2.3** *(Orbit-stabilizer formula)* $|orb(a)| = [G : Stab(a)]$*.*

The conjugacy action of $G$ on $G$ is given by $(g, h) \to ghg^{-1}$. Under this action the orbits are called the conjugacy classes. $Z(G)$ the center of $G$ is the subgroup of all elements of $G$ which commute with every other element of $g$. Equivalently it is the set of elements of $G$ with orbits (conjugacy classes) of size one. $C(g) = Stab(g)$ is called the centralizer subgroup of $g$.

**Theorem 2.4** *(Class formula) If* $conj(g_1), \cdots, conj(g_n)$ *are the conjugacy classes of size greater than one, then*

$$|G| = |Z(G)| + \sum_{k=1}^{n} [G : C(g_k)]$$

**Theorem 2.5** *(Cauchy) If $p$ is a prime which divides $|G|$, then $G$ has an element of order $p$.*

**Corollary 2.6** *Groups of order $p^2$ are abelian.*

**Theorem 2.7** *(Sylow 1) If $G$ is a finite group and $p^n$ divides $|G|$, then there exists a subgroup $H \subseteq G$ with $|H| = p^n$.*

**Proposition 2.8** *Any two n-cycles in $S_N$ are conjugates. If $\tau = c_1 c_2 \cdots c_n$ and $\rho = c'_1 c'_2 \cdots c'_n$ are disjoint cycle decomposition with $|c_i| = |c'_i|$ all $i$, then $\tau$ and $\rho$ are conjugates. Similarly for the converse.*

**Definition 2.9** *$H \subseteq G$ is a p-subgroup iff its order is a power of $p$. $P \subseteq G$ is a p-Sylow subgroup of $G$ iff $|P| = p^n$ where $|G| = p^n m$ and $p$ does not divide $m$.*

**Lemma 2.10** *Suppose $P$ is a p-Sylow subgroup of $G$, $g \in G$ has order a power of $p$, and $gPg^{-1} = P$. Then $g \in P$.*

**Theorem 2.11** *(Sylow 2) If $G$ is a finite group, $H$ a p-subgroup of $G$, and $P$ a p-Sylow subgroup of $G$, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$.*

**Corollary 2.12** *Let $G$ be a finite group such that $p$ divides $|G|$.*
*(a) Any p-subgroup of $G$ is contained in a p-Sylow subgroup of $G$.*
*(b) Any two p-Sylow subgroups of $G$ are conjugates.*
*(c) Any two p-Sylow subgroups of $G$ are isomorphic.*
*(d) A p-Sylow subgroup of $G$ is normal iff it is the only p-Sylow subgroup of $G$.*

**Theorem 2.13** *(Sylow 3) If $|G| = p^n m$ where $p$ does not divide $m$ and $n(p)$ is the number of p-Sylow subgroups of $G$, then:*
*(a) $n(p) = [G : N(P)]$ for any $P$ a p-Sylow subgroup of $G$,*
*(b) $n(p)$ divides $m$, and*
*(c) $n(p) = 1 \bmod p$*

**Theorem 2.14** *If $p < q$ are primes and $q$ is not $1 \bmod p$, then every group of order $pq$ is abelian.*

**Theorem 2.15** *$aut(\mathbb{Z}_p, +_p)$ is isomorphic to $(\mathbb{Z}_p \backslash \{0\}, \times_p)$ the multiplicative group of nonzero elements.*

**Example 2.16** *If $p < q$ are primes and $q = 1$ mod $p$, then there is a twisted product of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ which has order $pq$ and is not abelian.*

**Theorem 2.17** *If $p < q$ are primes and $q = 1$ mod $p$, then up to isomorphism there is a unique nonabelian group of order $pq$.*

# 3 Polynomials and finite field extensions

**Theorem 3.1** *Suppose that $p(x)$ is a polynomial over the field $F$ and for some $\alpha \in F$ $p(\alpha) = 0$. Then $p(x) = (x - \alpha)q(x)$ for some polynomial $q(x)$.*

**Corollary 3.2** *Any polynomial $p \in F[x]$ of degree $\leq n$ with more than $n$ roots must be identically zero.*

**Theorem 3.3** *Let the exponent of $G$ be the least $n$ such that $x^n = e$ for every $x \in G$. If $G$ is finite abelian group then $G$ is cyclic iff $exp(G) = |G|$.*

**Corollary 3.4** *The multiplicative group of a finite field is cyclic.*

# 4 Vector spaces over an abstract field

Before taking up finite field extensions we review some elementary results on vector spaces. See:

`http://www.math.wisc.edu/~miller/old/m542-00/vector.pdf`

**Lemma 4.1** *(Exchange Lemma) Suppose* $\mathrm{span}(A \cup B) = V$ *and $a$ is not in* $\mathrm{span}(A)$. *Then there exists $b \in B$ such that* $\mathrm{span}(A \cup \{a\} \cup (B \setminus \{b\})) = V$.

**Theorem 4.2** *Every vector space has a basis. Any two bases have the same cardinality. Any set of $n + 1$ vectors in a vector space of dimension $n$ is linearly dependent.*

**Corollary 4.3** *Any finite field $F$ of characteristic $p$ has cardinality $p^n$ for some integer $n$.*

## 5 Extension fields

**Theorem 5.1** *(Kronecker) If $p(x) \in F[x]$ is a non-constant polynomial, then there exists a field $E \supseteq F$ and $\alpha \in E$ with $p(\alpha) = 0$.*

**Corollary 5.2** *(Kronecker) If $p(x) \in F[x]$ is a polynomial of degree $n$, then there exists a field $E \supseteq F$ and $\alpha_i \in E$ such that*

$$p(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

**Theorem 5.3** *If $p(x) \in F[x]$ is irreducible and $\alpha, \beta$ are roots in some extension fields of $F$ then $F(\alpha)$ and $F(\beta)$ are isomorphic via an isomorphism which fixes $F$.*

**Corollary 5.4** *If $p(x) \in F[x]$ is irreducible and splits in an extension field $E$ of $F$ then the multiplicity of each root of $p$ is the same.*

**Theorem 5.5** *The formal derivative for an abstract polynomial $f(x) \in F[x]$ satisfies the usual derivative laws:*

(a) *If $a \in F$ and $f \in F[x]$, then $(af)' = af'$.*

(b) *If $f, g \in F[x]$, then $(f + g)' = f' + g'$.*

(c) *If $f, g \in F[x]$, then $(fg)' = f'g + fg'$.*

**Theorem 5.6** *For any $\alpha \in F$ and $f \in F[x]$*
*$\alpha$ is repeated root of $f$ iff it is a root of $f'$.*

**Corollary 5.7** *The roots of an irreducible polynomial in a field of characteristic zero, are always distinct.*

**Lemma 5.8** *If $E$ is any field of characteristic $p$, then for any $\alpha, \beta \in E$*

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$$

**Theorem 5.9** *For any $p^n$ and there is a field $F$ with $|F| = p^n$.*

**Definition 5.10** *For fields $F \subseteq E$ define $[E : F]$ to be the dimension of $E$ viewed as a vector space over $F$.*

**Theorem 5.11** *For fields $F \subseteq K \subseteq E$*

$$[E:F] = [E:K] \cdot [K:F]$$

**Theorem 5.12** *For $p(x) \in F[x]$ irreducible and $\alpha$ a root of $p$ in some extension field, $[F[\alpha]:F]$ is the degree of $p$.*

**Theorem 5.13** *If $E \supseteq F$ is the splitting field of some polynomial in $F[x]$, then $[E:F]$ is finite.*

**Theorem 5.14** *If $[E:F]$ is finite and $\alpha \in E$, then there is an irreducible polynomial $p \in F[x]$ with $p(\alpha) = 0$.*

# 6 Algebraic closure

**Definition 6.1** *$\alpha$ is algebraic over $F$ iff it is the root of a nontrivial polynomial in $F[x]$. A field $K$ is algebraically closed iff every nonconstant polynomial $f \in K[x]$ has a root in $K$.*

**Theorem 6.2** *If $F \subseteq E$ are fields define*

$$K = \{\alpha \in E \ : \ \alpha \text{ is algebraic over } F\}$$

*Then $K$ is a field and $F \subseteq K \subseteq F$.*

Steinitz proved that every field $F$ is a subfield of an algebraically closed field $K$. This requires the Axiom of Choice.

**Theorem 6.3** *Suppose $F \subseteq K$ and $K$ is algebraically closed. Let $E$ be the elements of $K$ which are algebraic over $F$. Then $E$ is algebraically closed.*

# 7 Compass and straight-edge

**Theorem 7.1** *(Wantzel 1837) Let $\mathcal{C} \subseteq \mathbb{R} \times \mathbb{R}$ be the smallest set containing $(0,0)$ and $(1,0)$ and closed under constructions using straight edge and compass. Then $\mathcal{C} = F_c \times F_c$ where $F_c$ is the smallest subfield of $\mathbb{R}$ which closed under square roots.*

**Lemma 7.2** *For any $\alpha$*

*$\alpha \in F_c$ iff for some $n$ there are fields $F_k$ for $k = 0, 1, \ldots, n$ with $\alpha \in F_n$ and such that $F_0 = \mathbb{Q}$ and for each $k < n \quad F_{k+1} = F_k[\sqrt{a_k}]$ for some $a_k \in F_k$.*

**Theorem 7.3** *For any $\alpha \in F_c$*

$$[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2^n \quad \text{for some integer } n.$$

**Corollary 7.4** $\sqrt[3]{2} \notin F_c$ *so it is impossible to "double the cube".*

**Corollary 7.5** $\cos(20^\circ) \notin F_c$ *so it is impossible to trisect every angle.*

**Corollary 7.6** *Since $\pi$ is transcendental and every element of $F_c$ is algebraic, it is impossible to "square the circle".*

# 8 Irreducibility criterion

**Lemma 8.1** *(Gauss's Lemma) Suppose $f \in \mathbb{Z}[x]$, then*

*$f$ is irreducible in $\mathbb{Q}[x]$ iff $f$ is irreducible in $\mathbb{Z}[x]$.*

**Lemma 8.2** *(Eisenstein's Criterion) Suppose $f \in \mathbb{Z}[x]$ has degree $n$*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

*and for some prime $p$*

*(a) $p$ does not divide $a_n$,*

*(b) $p$ divides $a_k$ for all $k = 0, 1, \ldots, n-1$, and*

*(c) $p^2$ does not divide $a_0$.*

*Then $f$ is irreducible in $\mathbb{Z}[x]$.*

**Theorem 8.3** *For any prime $p$ the polynomial $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is irreducible in $\mathbb{Q}[x]$.*

**Proposition 8.4** *If $2^m + 1$ is prime, then $m$ is a power of 2.*

**Theorem 8.5** *(Gauss) If the regular $p$-gon is constructible with straight edge and compass, then $p = 2^{2^n} + 1$ for some integer $n$.*

# 9 Solvability by radicals

For Tartaglia method of solving a cubic polynomial see
`https://www.math.wisc.edu/~miller/old/m542-00/galois.pdf`
For a brief history see:
`www.dwick.org/pages/cubicquartic.pdf`

**Theorem 9.1** *(Steinitz 1910) Suppose $F \subseteq E$ are fields of characteristic 0 and $[E : F]$ is finite. Then there exists $\alpha \in E$ such that $E = F[\alpha]$. The same is true if $E$ is a finite field.*

**Example 9.2** *There is a field $F$ and $\alpha, \beta$ with $[F[\alpha, \beta] : F]$ finite but there is no $\gamma$ with $F[\alpha, \beta] = F[\gamma]$.*

See
`http://www.math.wisc.edu/~miller/old/m542-00/examp.pdf`

# 10 Galois Theory

Proofs and definitions can be found in galois.pdf see:
`https://www.math.wisc.edu/~miller/old/m542-00/galois.pdf`

**Proposition 10.1** *(2.4 galois.pdf)* $\mathrm{aut}(E|F)$ *is a group. Furthermore, if $F \subseteq E \subseteq K$ are fields, then* $\mathrm{aut}(K|E)$ *is a subgroup of* $\mathrm{aut}(K|F)$.

**Lemma 10.2** *(2.5 galois.pdf) Suppose $\sigma, \rho \in \mathrm{aut}(F(\alpha)|F)$. Then $\sigma = \rho$ iff $\sigma(\alpha) = \rho(\alpha)$. Similarly, if $\sigma, \rho \in \mathrm{aut}(F(\alpha_1, \alpha_2, \ldots, \alpha_n)|F)$ then $\sigma = \rho$ iff $\sigma(\alpha_k) = \rho(\alpha_k)$ for all $k = 1, 2, \ldots, n$.*

**Theorem 10.3** *(2.6 galois.pdf) Suppose that $K$ is the splitting field of a polynomial in $F[x]$ of degree $n$. Then* $\mathrm{aut}(K|F)$ *is isomorphic to a subgroup of $S_n$.*

**Definition 10.4** *For fields $F \subseteq K$ we say that $K$ is a splitting field over $F$ iff $K$ is the splitting field of some polynomial in $F[x]$.*

Every polynomial in $\mathbb{Q}[x]$ splits in $\mathbb{C}$ but $\mathbb{C}$ is not a splitting field over $\mathbb{Q}$.

**Lemma 10.5** *(Extension Lemma 2.9 galois.pdf) Suppose that* $F \subseteq F_1 \subseteq K$ *and* $F \subseteq F_2 \subseteq K$ *are fields,* $K$ *is a splitting field over* $F$*, and* $\sigma : F_1 \to F_2$ *is an isomorphism which fixes* $F$*. Then there exists* $\rho : K \to K$ *an automorphism which extends* $\sigma$*.*

**Theorem 10.6** *(3.1 galois.pdf) Suppose* $F \subseteq K$*,* $K$ *is a splitting field over* $F$*,* $p \in F[x]$ *is irreducible, and there is* $\alpha \in K$ *such that* $p(\alpha) = 0$*. Then* $p$ *splits in* $K$*.*

**Theorem 10.7** *(2.8 galois.pdf) Suppose* $F \subseteq K$*,* $K$ *is a splitting field over* $F$*, and these fields have characteristic zero. Then* $|\mathrm{aut}(K, F)| = [K : F]$*.*

**Theorem 10.8** *(2.10 galois.pdf) Suppose* $F \subseteq K \subseteq E$*,* $K$ *and* $E$ *are splitting fields over* $F$*. Then* $\mathrm{aut}(E|K) \triangleleft \mathrm{aut}(E|F)$ *and*

$$\frac{\mathrm{aut}(E|F)}{\mathrm{aut}(E|K)} \simeq \mathrm{aut}(K|F)$$

**Proposition 10.9** *Suppose* $F \subseteq K \subseteq E$*,* $E$ *is a splitting fields over* $F$*, and* $\mathrm{aut}(E|K) \triangleleft \mathrm{aut}(E|F)$*. Then* $K$ *is a splitting field over* $F$*.*

**Theorem 10.10** *(5.3 galois.pdf) Suppose* $F \subseteq E$ *is a radical Galois extension, then* $\mathrm{aut}(E|F)$ *is a solvable group.*

**Example 10.11** *If* $2$ *generates the multiplicative group of* $\mathbb{Z}_p$*, then*

$$f(x) = 1 + x + x^2 + \cdots + x^{p-1}$$

*is irreducible over* $\mathbb{Z}_2$*.*

See Gurrier 1968
`http://www.jstor.org/stable/2315109`
See also Artin's conjecture on primitive roots
`http://en.wikipedia.org/wiki/Artin_conjecture`

**Theorem 10.12** *(5.4 galois.pdf) Subgroups of solvable groups are solvable and homomorphic images of solvable groups are solvable.*

**Theorem 10.13** *Suppose* $K$ *is the splitting field of a polynomial in* $F_1[x]$ *and* $F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m$ *satisfies* $F_1 \subseteq K \subseteq F_m$ *and* $F_{k+1}$ *is a radical Galois extension of* $F_k$ *for each* $k < m$*. Then* $\mathrm{aut}(K|F_1)$ *is a solvable group.*

**Lemma 10.14** .

*(a)* $\{(i, i+1) : 1 \leq i < n\}$ *generates* $S_n$. *(adjacent swaps)*

*(b)* $\{(1,2),(1,2,3,\ldots,n)\}$ *generates* $S_n$.

*(c)* $\{(1,i),(1,2,3,\ldots,n)\}$ *generates* $S_n$ *if* $n$ *is prime.*

*(d) If* $n$ *is prime, then any subgroup of* $S_n$ *which contains an* $n$*-cycle and at least one transposition must be* $S_n$.

**Theorem 10.15** *Suppose* $f(x) \in \mathbb{Q}[x]$ *is an irreducible polynomial of prime degree* $p$ *such that* $f$ *has exactly* $p-2$ *real roots. If* $K$ *is the splitting field of* $f$*, then* $\mathrm{aut}(K, \mathbb{Q})$ *is isomorphic to* $S_p$.

**Example 10.16** *If* $f(x) = x^5 - 5x + \frac{5}{2}$ *then* $f$ *is irreducible and has exactly three real roots.*

**Theorem 10.17** *The alternating group* $A_5$ *is simple. Hence* $S_5$ *is not solvable.*

**Corollary 10.18** *There is polynomial in* $\mathbb{Q}[x]$ *of degree 5 which cannot be solved by radicals.*

**Theorem 10.19** *For any* $n$ *there are fields* $E \subseteq K$ *such that* $K$ *is the splitting field of a polynomial in* $E[x]$ *and* $\mathrm{aut}(K|E)$ *is isomorphic to* $S_n$.

**Theorem 10.20** *(char 0) Suppose* $F \subseteq K$ *and* $K$ *is the splitting field of a polynomial in* $F[x]$ *and* $H \subseteq \mathrm{aut}(K|F)$ *is a subgroup. Then there exists a field* $E$ *with* $F \subseteq E \subseteq K$ *and* $\mathrm{aut}(K|E) = H$.

**Corollary 10.21** *Every finite group is a Galois group.*

Proof of the fundamental theorem of algebra using Galois theory:
`http://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra`

**Definition 10.22** *A polynomial* $f(x) \in \mathbb{Q}[x]$ *is solvable by real radicals iff its roots are in the smallest subfield* $S \subseteq \mathbb{R}$ *which is closed under taking real roots, i.e., if* $a \in S$, $a > 0$ *and* $n \in \mathbb{N}$ *then* $\sqrt[n]{a} \in S$.

**Lemma 10.23** *Suppose* $F \subseteq \mathbb{C}$ *is a subfield,* $p$ *a prime, and* $a \in F$. *Then* $f(x) = x^p - a$ *is reducible in* $F$ *iff it has a root in* $F$.

**Theorem 10.24** *Suppose* $f(x) \in \mathbb{Q}[x]$ *is an irreducible cubic with three real roots. Then* $f(x)$ *is not solvable by real radicals.*

# 11 Similar Matrices

For this material see
`http://www.math.wisc.edu/~miller/old/m542-00/similar.pdf`

**Theorem 11.1** *Suppose $F$ is an infinite field, $A$ and $B$ are $F$-matrices, and for some field extension $E \supseteq F$ there is an $E$-matrix $P$ such that $A = PBP^{-1}$. Then there is an $F$-matrix $P$ such that $A = PBP^{-1}$.*

For algebraically closed fields $A$ and $B$ are similar iff they have the same Jordan Normal forms up to a permutation of the Jordan blocks. So without loss we may as well assume that $E$ is the algebraic closure of $F$. By adding one new element at a time it suffices to prove the Theorem for $E = F[\alpha]$ with $[E : F]$ finite. Let $p(x) \in F[x]$ be the minimal polynomial for $\alpha$. Consider the vector space

$$\mathcal{M} = \{P \ : \ AP = PB\}$$

where the $P$ are $E$-matrix. Note that any such $P$ has entries which are a polnomial in $\alpha$. So we can write

$$P = P_0 + \alpha P_1 + \ldots + \alpha^n P_n$$

where the $P_i$ are $F$-matrices. Let $f(x) \in F[x]$ be the determinate of

$$P_0 + xP_1 + \ldots + x^n P_n$$

Since $f(\alpha) \neq 0$ and $F$ is an infinite field there is an $\beta \in F$ such that $f(\beta) \neq 0$. The $F$-matrix

$$P' = P_0 + \beta P_1 + \ldots + \beta^n P_n$$

is invertible and witnesses the similarity of $A$ and $B$.